

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, 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 either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, 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 photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**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**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-3410-5

**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.....	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms, acronyms, conventions and symbols.....	8
4 Assessment approach.....	8
5 Assessment method.....	9
5.1 Overview.....	9
5.1.1 General.....	9
5.1.2 Phases.....	9
5.2 Defining the objectives of the assessment.....	10
5.3 Design and layout of the assessment.....	11
5.3.1 Defining the scope of assessment.....	11
5.3.2 System properties and influencing factors.....	11
5.3.3 Collation of documented information.....	13
5.3.4 Documenting collated information.....	14
5.3.5 Selecting assessment items.....	14
5.3.6 Assessment specification.....	14
5.4 Planning of the assessment program.....	14
5.4.1 Overview.....	14
5.4.2 Developing assessment activities.....	15
5.4.3 Assessment program.....	16
5.5 Execution of the assessment.....	16
5.6 Reporting of the assessment.....	16
6 Evaluation techniques.....	17
Annex A (informative) System Requirements Document (SRD).....	18
A.1 Overview.....	18
A.2 Analysis of system mission.....	18
A.2.1 General.....	18
A.2.2 Formulation of system mission.....	18
A.2.3 Analysis of system mission into tasks.....	18
A.2.4 Assignment of relative importance to tasks.....	19
A.2.5 Defining influencing factors.....	19
A.3 Review of system requirements document (SRD).....	19
Annex B (informative) System Specification Document (SSD).....	20
B.1 Overview.....	20
B.2 Development of system specification document.....	20
B.2.1 General.....	20
B.2.2 System overview.....	20
B.2.3 Defining system boundaries.....	21
B.2.4 Specification of system.....	21
B.2.5 Description of system operation.....	21
B.2.6 Statement of system implementation rationale.....	22

B.2.7	Statement of compliance with system requirements.....	22
Annex C	(informative) Examples of collation documentation.....	23
C.1	Overview.....	23
C.2	Example of furnace control documentation.....	23
C.2.1	Schematic of task.....	23
C.2.2	Task definition	23
C.2.3	Input characteristics	23
C.2.4	Output characteristics	24
C.2.5	Operational functions	25
C.2.6	Monitoring functions.....	25
C.2.7	Configuration	25
C.2.8	Flexibility	25
C.2.9	Functionality collation tables	26
C.3	Example of simple control loop task documentation.....	32
C.3.1	Overview	32
C.3.2	Schematic of task.....	32
C.3.3	Information flows.....	32
C.3.4	Performance tables	32
C.3.5	Performance collation tables	33
C.4	Example of collation documentation (from SRD of a master-slave control task)	35
C.4.1	Overview	35
C.4.2	Schematic of task.....	35
C.4.3	Boundary states	35
C.5	Example of collation documentation (from SSD of a master-slave control task)	36
Bibliography		38
Figure 1	– General layout of IEC 61069.....	7
Figure 2	– Assessment matrix	12
Figure C.1	– Control block	23
Figure C.2	– Task schematic.....	32
Figure C.3	– Schematic of task	35
Table 1	– Assessment phases, inputs and outputs.....	10
Table C.1	– SRD coverage analysis	26
Table C.2	– SRD configurability analysis	28
Table C.3	– SRD flexibility analysis	30
Table C.4	– Performance for information flow	32
Table C.5	– Information translation.....	33
Table C.6	– Performance collation.....	34
Table C.7	– Failure states of task input and output	36
Table C.8	– Dependability	37

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 2: Assessment methodology

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 61069-2 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 1993. 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 61069-2:1993 to make the overall set of standards more organized and consistent;
- b) IEC TS 62603-1:2014 has been incorporated into this edition.

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

FDIS	Report on voting
65A/790/FDIS	65A/799/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 61069 series, published under the general title *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

IEC 61069 deals with the method which should be used to assess system properties of a basic control system (BCS). IEC 61069 consists of the following parts:

- Part 1: Terminology and basic concepts
- Part 2: Assessment methodology
- Part 3: Assessment of system functionality
- Part 4: Assessment of system performance
- Part 5: Assessment of system dependability
- Part 6: Assessment of system operability
- Part 7: Assessment of system safety
- Part 8: Assessment of other system properties

Assessment of a system is the judgement, based on evidence, of the suitability of the system for a specific mission or class of missions.

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the particular 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 the standard 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 may 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, e.g., 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 part structure and the relationship among the parts of IEC 61069 are shown in Figure 1.

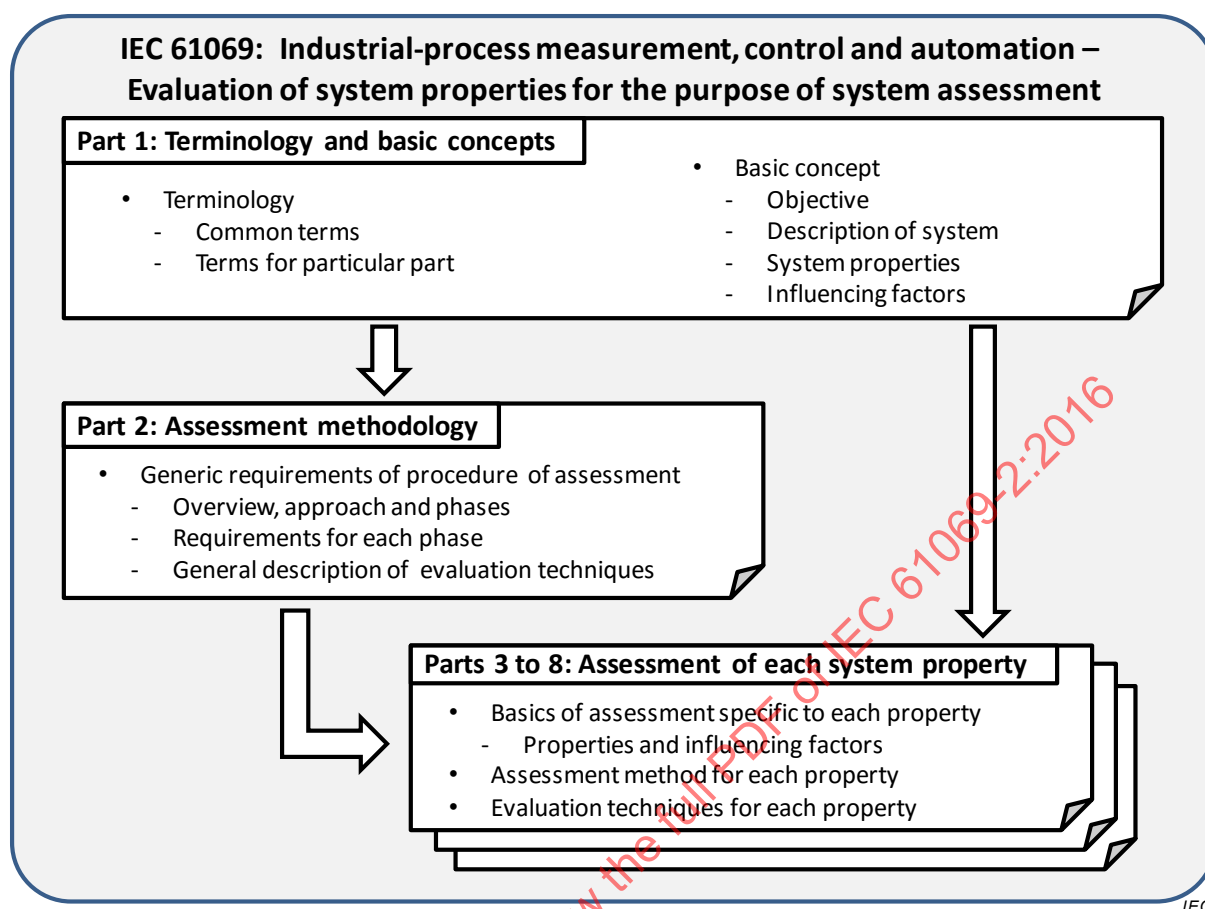


Figure 1 – General layout of IEC 61069

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

Part 2: Assessment methodology

1 Scope

This part of IEC 61069 specifies the methodology in the assessment of a basic control system (BCS) based on the basic concepts of IEC 61069-1.

It describes the method for analysing, weighing the relative importance of the various system properties and influencing factors, and determining an assessment program.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61069-1:—1, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 1: Terminology and basic concepts*

3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61069-1 apply.

3.2 Abbreviated terms, acronyms, conventions and symbols

For the purposes of this document, the abbreviated terms, acronyms, conventions and symbols given in IEC 61069-1 apply.

4 Assessment approach

BCSs are sufficiently complex, so that a totally comprehensive assessment inevitably requires an expenditure of effort and time that is neither practical nor cost-effective. It is therefore important to analyse and specify the objectives of the assessment carefully, before an assessment program is planned.

The mission of the system or class of missions is broken down into tasks.

The task(s) which the system needs to perform should be defined in terms of the selected BCS, its system properties, and the required functions. This enables the functions required for the system to fulfil its mission(s) to be specified precisely.

¹ Second edition to be published simultaneously with this part of IEC 61069.

Missions of the system usually require some characteristics of the system which are not directly related to the tasks of the system. Such characteristics include documentation and support services.

The assessment program shall be designed with the assessment objectives, the system requirements and the system specifications. It should be prepared in advance.

NOTE In certain cases, e.g. a regulated application, it may be necessary that the assessment be designed and performed by an independent party.

In the absence of a mission, no assessment can be made; however, examination of the system to gather and organize data for a later assessment is possible.

5 Assessment method

5.1 Overview

5.1.1 General

The details of the assessment program shall be derived from consideration of the assessment objectives (as stated in 5.2) and the following inputs:

- System Requirements Document (SRD), and
- System Specification Document (SSD).

NOTE 1 Systems Requirements Document is explained in Annex A.

NOTE 2 System Specification Document is explained in Annex B.

The assessment correlates items of the system requirements document with the system specification document guided by the assessment objective.

If at any phase of the assessment information from the SRD or SSD is missing or incomplete, the originators of the SRD or SSD should be consulted with specific questions to obtain the required further information.

The assessment method is a tool to be utilized during the life cycle of BCS. Yet the life cycle is out of scope of IEC 61069-2. Still during the development of a BCS and defining its assessment, the overall BCS life cycle should be taken into account.

Assessments for every relevant stages of the life cycle should be planned, e.g. commissioning.

5.1.2 Phases

The assessment consists of the following phases:

- Defining the objectives of the assessment;
- Design and layout of the assessment;
- Planning of the assessment program;
- Execution of the assessment;
- Reporting of the results.

The phases and their respective inputs and outputs are shown in Table 1.

Table 1 – Assessment phases, inputs and outputs

Phase	Input	Output
Defining the objectives of the assessment	SRD and SSD	(Documented) Objective of the assessment Assessment protocol
Design and layout of the assessment	Objective of the assessment SRD SSD	Assessment specification
Planning of the assessment program	Assessment specification	Assessment program
Execution of the assessment	Assessment program	Result of the evaluations
Reporting of the results	Result of the evaluations	Report of the assessment

5.2 Defining the objectives of the assessment

The objectives of the assessment shall be stated and documented prior to the start of the assessment as a foundation for planning and preparation of the assessment program. They should be stated clearly and carefully.

These objectives form the basis of the guiding principles throughout the assessment by:

- determining the scope,
- the nature of the evaluation,
- the depth of the evaluation to be carried out,
- the measurements and observations to be made,
- the type of reports to be produced.

The objectives govern the cost of the assessment and the resources required to conduct the assessment.

It is therefore of utmost importance that the objectives and the scope of the assessment are well-documented and agreed upon before the assessment program is further developed.

Description of the magnitude of BCS change requiring a reassessment should be defined, e.g. BCS expansion.

Updates of the assessment, during the BCS life cycle, regardless of changes/expansion, should be defined/scheduled, e.g. after 10 years of operation.

The authority(ies) who may require an assessment or re-assessment should be defined.

Additionally the authority(ies) who approve assessments or re-assessments should be defined.

During the assessment, reviews should be carried out at planned review points or at pre-determined intervals. Such reviews should at least be held at the end of each phase.

The objectives of the assessment may be, for example:

- to assess a specific system for a particular mission;
- to assess a variety of configurations of a single system for a particular mission;
- to compare several systems for a particular mission;
- to obtain an assessment of a particular system for general use in a variety of missions;

- to establish the suitability of a system for a particular mission;
- to establish the suitability of a system for a defined class of missions.

The assessment protocol shall be defined including:

- the assessment authorities for change and release of the assessment program,
- the assessment specifications and the assessment reports,
- the procedures to be followed,
- the contingency actions that are permissible without seeking prior authorization in the event that the assessment cannot be conducted as planned.

5.3 Design and layout of the assessment

5.3.1 Defining the scope of assessment

5.3.1.1 System boundary

The boundary of the system shall be carefully defined by identifying "what does and what does not" belong to the system to be assessed.

The boundary of the system to be assessed shall be defined by taking into account all aspects of influencing factors described in IEC 61069-1; — ,5.3 . It shall be documented in the assessment specification.

The system boundary can be physical (e.g. equipment, geography) and/or virtual (e.g. information, communication).

The objectives of the assessment are translated into a scope of the assessment. In order to develop the scope, the system properties described in IEC 61069-1; — , 5.2.2 to 5.2.7 shall be taken into consideration.

5.3.1.2 System configuration

The configuration(s) of the system to be assessed shall be specified in the assessment specification. Since the configurability of the system itself can be a system property to be assessed, the configuration of the system where the assessment items are evaluated should be carefully specified.

If the assessment objective is to assess a specific system for a particular mission, the assessment shall be carried out on a specific system configuration and this configuration shall be documented in the assessment specification.

If the assessment objective is to assess the flexibility of a system to meet a broad range of typical requirements encountered in a specific sector of industry, the assessment shall be carried out on a range of defined modules that can be configured in a variety of alternative ways. The range of modules and the variety of configurations shall be documented in the assessment specification.

A system is sometimes so complex that comprehensive evaluations of all system properties would not be cost-effective, or even feasible. By careful consideration of the objectives, the system configuration and the influencing factors, the evaluations can be reduced to include only those assessment items which are most sensitive for the mission of the system.

5.3.2 System properties and influencing factors

The assessment items required for the assessment shall be specified. The required value or range of value of each system property and influencing factor shall also be specified.

Additionally, as far as applicable, influencing factors as described in IEC 61069-1 should be included.

Each assessment item should be scrutinized to determine whether it influences or degrades the system in such a way that it hampers or prohibits the correct conduct of other assessment items.

These considerations shall be documented as an assessment specification to show the constraints upon the sequencing of the assessment activities.

A convenient way to document the system properties and the influencing factors is in the form of a matrix, where the cells correspond to the assessment items.

A generic matrix to summarize an assessment is given in Figure 2.

System Properties	Functionality			Performance			Dependability			Operability			System Safety			Other properties		
Influencing Factors																		
Mission / Task																		
Personnel																		
Process																		
Infrastructure																		
Environment																		
External systems																		

IEC

Figure 2 – Assessment matrix

The assessment items required to be included in the assessment shall be selected and their relative priorities shall be determined. It can be done using this matrix as a means for considering each system property and each influencing factor and taking into consideration the objective of the assessment.

An assessment item can be progressively further detailed by using e.g. groups or sub-groups of properties, in which the headings of the generic matrix are further expanded into more detailed system properties and influencing factors.

Assessment items, not relevant for the particular assessment, should also be identified for later reference, and the reasons for the exclusion should be documented.

5.3.3 Collation of documented information

The collation is a step of this phase to extract the information which is required to determine potential candidates of the assessment items. The information provided by this process is used for design and layout of the assessment.

For the purpose of the collation, the necessary information shall be extracted from the SRD and the SSD.

The SRD and SSD shall be carefully scrutinized to compile precise and concise statements of the topics. Example topics include:

- the boundaries of the system,
- the areas of non-compliance between system requirements and system specification,
- the list of required and future tasks,
- the list of functions provided to perform each of the required and future tasks,
- the list of alternative data paths linking the functions to support the required task(s),
- the allocation of the functions to the modules and elements,
- the number of these modules and elements,
- the extent to which these modules and elements are used to fulfil the required tasks,
- the system properties for each of the above functions,
- the influencing factors for each of the above modules/elements.

A list of potential assessment items shall be created from these topics. The assessment items shall be specified under specific system configuration(s) according to the objective of the assessment.

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

The statements should be described in qualitative and quantitative terms, and, if applicable, their range of values.

NOTE Examples of collation documentation are provided in Annex C.

Each task to be assessed should be described in terms of its inputs, outputs and operation.

For each input, notes should be made of:

- permissible input states and corresponding permissible output state(s);
- non-permissible input states and corresponding action(s) required.

For each output, notes should be made of:

- permissible output states;
- non-permissible output states and corresponding action(s) required.

For each of the tasks, the following information about tasks should be clearly stated:

- kinds of failures which affect each task;
- permissible frequency of occurrence of each failure;
- action to be taken for each failure;
- maximum time during which the task can be stopped before the module is restored.

5.3.4 Documenting collated information

The information collated as stated in 5.3.3 should be documented in a form that can be manipulated for the process of planning the assessment program.

If information for the collation is missing or incomplete, the required further information should be obtained from the originators of the SRD and SSD. This further or additional information should be properly recorded in the assessment specification.

5.3.5 Selecting assessment items

The complete list of assessment items is reduced by considering the following filters:

- importance of the task(s) to the mission;
- existing level of confidence based upon prior knowledge;
- the level of interdependency of different functions, the number of interfaces, the re-use of the same function in different tasks;
- the global pre-knowledge available and extent to which the knowledge applies to the assessment item(s).

The relative importance should be evaluated taking into account both aspects of importance of the task(s) in a particular phase of the system life time and of duration of the phase since importance can vary depending of the phase.

The existing level of confidence may be based on preceding success of the system in similar or identical missions, experience with the manufacturer, the experience of users with the same system type or comparable systems.

Assessment items which are required by international and/or national regulatory bodies shall be evaluated in accordance with the rules laid down in those regulations.

Assessment items shall include a check that the BCS complies with the national regulations in force at the site where the system is intended to be used.

5.3.6 Assessment specification

The assessment specification is a document that describes what should be evaluated. The assessment specification should specify at least the following points:

- the objective of the assessment as stated in 5.2;
- the system boundary as stated in 5.3.1.1;
- the system configuration as stated in 5.3.1.2;
- the assessment matrix as stated in 5.3.2;
- the list of assessment items as stated in 5.3.2;
- the list of tasks as stated in 5.3.3;
- the criteria used for filtering of the items as stated in 5.3.5;
- the referenced standards for each assessment item.

5.4 Planning of the assessment program

5.4.1 Overview

During this phase, an assessment program shall be planned based on the assessment specification prepared in the previous phase.

The objective of designing an assessment program is to increase confidence in the judgement of a system's suitability for the system mission.

The assessment activities shall maximize this increase in confidence, whilst remaining within defined cost and time constraints.

The assessment program shall specify the assessment activities and their sequence against a time scale in a manner that enables the assessment to be controlled.

The assessment program shall comprise a set of assessment activities, each of which may be:

- either an observation at system level, or
- observation at lower levels (if necessary down to an individual element) combined with a synthesis to system level.

The design of the individual assessment activities is dependent upon the system property being considered.

The assessment program should specify also detail of each assessment activity including:

- type of evaluation technique; and
- tools and utilities required.

The evaluation technique(s) to be used should be selected so that the results can be compared qualitatively and/or quantitatively against the requirements.

The evaluation techniques selected may be analytical using only system documentation or they may be empirical, requiring access to an evaluation system. In practice the techniques selected will be a combination of analysis and empirical tests using the system documentation and a restricted combination of modules.

The assessment activities shall be planned in a logical sequence abiding by all constraints of assessment items identified in the assessment specification. For the purpose of selecting assessment activities included in the assessment program, each potential assessment activity should be analysed by determining the following aspects.

- evaluation techniques and tools,
- cost and time required to execute,
- importance.

The steps of planning assessment program should be repeated until the program is agreed upon by all parties involved in the assessment.

5.4.2 Developing assessment activities

The list of assessment activities should be developed based on the following criteria:

- the type of analysis and/or evaluation required to support the assessment;
- the importance of the particular system property to the overall mission;
- the importance of system properties and influencing factors to the mission;
- knowledge and skill required to perform each analysis and/or test;
- constraints on the assessment schedule due to permanent effects that tests of the performance and other system properties can have;
- technical assessment constraints such as size, weight, availability of utilities, control of the test environment; and
- availability of the selected personnel;

- availability of a group of selected operators to perform distinct tasks for observation of operability;
- tools and utilities required to perform the analysis and tests;
- availability of tools for the assessment activities;
- estimation of cost and time for each of the analysis and test;
- estimated cost and time of the assessment activities;
- priority level for each of the assessment activities;
- level of confidence based upon prior knowledge.

It is sometimes necessary to consider several evaluation techniques, which are mutually supplementary.

All assessment activities lists shall be combined into the assessment program for the system.

5.4.3 Assessment program

The assessment program should specify at least the following points:

- the evaluation techniques selected as stated in 5.4.1;
- the criteria to be taken into account as given in 5.4.2;
- the assessment activities obtained in 5.4.2;
- the required increase in confidence level;
- the assessment schedule taking account of the possible permanent effects that tests can have;
- the failure modes to be analysed and/or evaluated and the resulting effects expected;
- the physical integrity and cyber security mechanisms provided in the system.

5.5 Execution of the assessment

The assessment activities shall be performed in accordance with the assessment program specified in 5.4 and in accordance with the prescribed assessment protocol specified in 5.2.

If and when deviations from the assessment program or the assessment protocol are necessary, these should be reported in the assessment report and, unless previously agreed contingency actions can be taken, these shall be approved by the assessment authority.

All observations, measurements, calculations shall be recorded at the time they are made for the assessment report.

5.6 Reporting of the assessment

The conduct and results of the assessment shall be documented in an assessment report. The assessment report should accurately, clearly, unambiguously and objectively present the objective, the results and all relevant information of the assessment.

The assessment reports shall include at least the following information:

- the title of the assessment report;
- a unique identification for the report;
- the date of issue;
- the name of assessment authority;
- the reference to the assessment specification described in 5.3.6;
- the reference to the assessment program specified in 5.4.3;

- the system configuration such as type and number of input/output, scan rate required, system mission, tasks and functions;
- characteristics of the mission such as type of process in the case of assessment for a particular mission;
- a description and identification of the system assessed, including a list showing the hardware with model numbers and the software used with release date;
- a summary of the salient points arising out of the assessment and the conclusions reached;
- an account of the procedures, methods, specifications and tests (preferably summarized in a matrix and supplemented by referenced documents);
- reasons to have selected the particular assessment items to evaluate, and reasons to have not selected other assessment items;
- any deviations from the assessment program (additions or exclusions);
- measurements, tests and derived results supported by tables, graphs, drawings or photographs as appropriate;
- failures observed;
- a statement of the measurement uncertainties;
- a statement as to whether or not the system complies with the requirements against which the system was assessed including a statement of any discrepancies.

The format of assessment report should be standardized to facilitate comparison of assessments of different systems. The results of the assessment should be supported by appropriate form of information such as lists, matrices and graphs.

Corrections or additions to the report after its issue shall be made only by a supplementary report, referring to the original report identified by its title and number. This supplementary report shall meet the same requirements as the original report, if it is applicable.

6 Evaluation techniques

The evaluation technique(s), to be used, shall be selected so that the results can be compared qualitatively and/or quantitatively against the requirements defined in the system requirements document, with the required level of confidence in the evaluation.

The techniques selected can be analytical, using only system documentation and prior evidence or data, or in some cases, they can be a combination of an analytical and an empirical techniques, requiring access to an evaluation system.

In practice the techniques selected are a combination of analysis and empirical tests using the system documentation and a (restricted) combination of modules.

For this purpose, a model of the system should be assembled with a selection of functions of the system, which represents the tasks to be performed sufficiently close and illustrates in detail the two-way communication means provided at the human-machine interface.

NOTE An example of a model is described in IEC 61069-4:—2, Annex D.

² To be published simultaneous with this part of IEC 61069.

Annex A (informative)

System Requirements Document (SRD)

A.1 Overview

Annex A describes a method of developing and reviewing SRD, including check points for each system property.

A.2 Analysis of system mission

A.2.1 General

To assess a BCS, it is necessary to establish the system mission.

The system mission can only be properly defined if the system is considered in its context, i.e. the personnel, the process to which it is related, any other related systems as well as the environment in which it operates.

The activities mentioned in A.2.2, A.2.3, A.2.4 and A.2.5 result in the system requirements document (SRD).

A.2.2 Formulation of system mission

The objective at this stage is to define the mission of, and not the role to be performed by, the BCS.

The description of the mission should state what is to be achieved, not why and how it is to be achieved.

The mission should be elaborated by describing its phases. These may include:

- initial configuration and commissioning of the total facility comprising personnel, plant, BCS, and other systems that will be used to accomplish the mission;
- configuration or set-up for specific production runs;
- production, which may involve steady continuous operation or programmed sequences of sub-operations;
- change-over from one production run to another;
- emergency shutdown or transition to a safe holding state;
- normal shutdown;
- updates and changes to the system to incorporate new tasks or functions;
- de-commissioning of the system after its operational phase.

Although not always obvious, the system generation, commissioning and decommissioning phases are important phases and can form part of the system mission.

A.2.3 Analysis of system mission into tasks

To achieve the mission, the BCS needs to perform specific tasks and/or have specific system properties associated with each of the mission phases identified above. These phases are examined to define the tasks that the system is required to perform.

Tasks, within a phase, may be, for example:

- monitoring and centralized display of monitored values, which may include processing of the measured variables to derive values of mission variables;
- activating a specific phase in the process in accordance with manually entered or automatic commands;
- automatic process control, e.g. automatic control of an individual process variable;
- interlock control between process variables;
- automatic initiation and execution of a phase.

The BCS may be required to perform any of the specific tasks either completely or partially, i.e. a task shared with another system or personnel.

Each task is defined in sufficient detail to make clear the extent of the task assigned to the BCS.

For each of the tasks, the requirements should be defined in terms of functionality, performance, dependability, operability, system safety, and/or other system properties, e.g. quality assurance, after sales services, etc.

It should be noted that at this stage the objective is to define the tasks of the system, not the functions of the system.

A.2.4 Assignment of relative importance to tasks

The dependency of the mission upon each of the tasks should be considered at this stage. Tasks should be classified into at least groups of importance to the mission:

- essential: tasks that are essential to accomplish the mission;
- significant: tasks that are not essential, but have a significant effect upon the cost-effectiveness of the mission;
- desirable: tasks that are desirable but have little quantifiable effect upon the mission.

A.2.5 Defining influencing factors

The correctness of the execution of each of the tasks required to fulfil the mission can be impaired by factors which influence that execution.

At this stage, it is necessary to consider, for each of the tasks, the factors which might influence the required criteria for that task.

A.3 Review of system requirements document (SRD)

The guidance about check points of the system requirements document for each type of property is provided in Annex A of the part corresponding to the property.

The effectiveness of the assessment is dependent upon a comprehensive statement of requirements.

Annex B (informative)

System Specification Document (SSD)

B.1 Overview

Annex B describes method of developing and reviewing SSD, including check points for each system property.

B.2 Development of system specification document

B.2.1 General

The starting point for specifying the SSD is the SRD as broken down into tasks with assigned relative importance.

From this and the mapping of the tasks on the functional model (see 5.1.1 and IEC 61069-1:—, Figure 4), it will be possible to derive a system implementation, which sets out to address the system requirements.

During the assessment phase, the system proposed by SSD will be compared with the detailed mission statement as laid down in the system requirements document.

In order to enable effective analysis of compliance with the system requirements, it is important that the specification of the system proposed identifies various key points. These are examined in detail in B.2.2 to B.2.7.

The activities, mentioned in B.2.2 to B.2.7, result in the system specification document.

B.2.2 System overview

The intent of the overview is to relate the system implementation to the system mission as reflected in the SRD.

Similarly as the mission can be broken down hierarchically into tasks, the system to be assessed can be hierarchically decomposed into modules and elements.

It is envisaged that the decomposition leads to overview diagrams and supplementary descriptions.

These should at least contain information on the following subjects:

- all modules interfacing to the process, to the operator, to external systems, etc.;
- communication modules;
- application processing modules;
- interaction between modules, and
- relative and absolute distances and locations of modules.

For the decomposition it is important to know that the majority of modern BCSs are based on a hybrid-architecture, composed of a combination of separate measurement and control equipment and related software.

B.2.3 Defining system boundaries

A system has several distinct boundaries, namely, to the process, to the utilities supplying the energy, to the environment in which the system is placed, to other connected external systems and to the system users (operators, maintenance personnel).

The boundary of the system is carefully defined by identifying "what does and what does not" belong to the system to be assessed, taking into account at least the following considerations:

- The boundary to the process can be placed so as to include or exclude signal conditioners, galvanic isolators, marshalling units, cables, input/output devices such as sensors and final control elements, etc.
- The boundary to the utilities is defined to take into account the equipment from different manufacturers such as those for uninterrupted power supplies, batteries, filters, regulators, etc., each of which can supply all or part of the system including the sensors and final control elements.
- The boundary to external equipment should take into account the required interfaces, communication functions, cables, etc.
- The boundary to the environment should take into account the physical distribution of the modules and elements, which may be placed in an air conditioned room, in an office environment, in the process area or directly on the process equipment itself, etc.
- The boundary to the human interface is particularly important when assessing the system dependability, since operational and maintenance personnel have an important role to play in the completion of the intended mission. The interaction of people and system takes place at several levels of the control hierarchy and depends highly on the mode of operation under consideration and involves all hardware and software modules of the system.
- Although it is not obvious, the tasks themselves are external to the system boundary. The influences of imposing, modifying and adding tasks are important aspects in the assessment of the system "flexibility and expandability" properties.

When the assessment objective is "to obtain a comparative assessment of different systems", it might not be possible to define the boundaries in exactly the same manner for each of the systems to be compared if these systems have a different functional scope. In this case, other equipment, foreign to the system under consideration, should be added to make the comparison possible. A specific note should be made of the equipment added.

B.2.4 Specification of system

The intent of the system specification is to provide the precise numerical, operational and relational data for the proposed system implementation.

It should typically contain:

- a complete list of all modules and elements;
- product specifications for each type of module and element, giving general, functional and technical specifications, and including environmental specifications;
- detailed interconnection diagrams identifying and further specifying the interconnection and intercommunication between individual module(s) and element(s), including redundant pathways, if applicable.

B.2.5 Description of system operation

The intent of the description of the operation of the system is to indicate in a systematic manner how the individual tasks are performed by the proposed system.

This systematic description should be on a task-by-task basis and typically contain:

- a list of the functions proposed to perform each task;
- a commentary showing, for each task, the way in which the proposed modules and elements provide these functions.

The level of detailing the implementation of the task(s) and the extent of subdivision into modules and elements should be only that which is necessary, yet sufficient to demonstrate that the requirements are met.

B.2.6 Statement of system implementation rationale

For the purpose of the assessment, the definition of the system implementation should be supported by statements of the underlying rationale.

Such statements should address one by one each of the properties (see 5.2) relevant for the system mission and provide additional information relating to the rationale of the system implementation to the achievement of the required system properties. This might include:

- reasons for selection between alternative solutions;
- supporting data (e.g. field experience), calculations, etc.;
- supporting test reports.

B.2.7 Statement of compliance with system requirements

Explicit statements are made for each of the system requirements not matched by the proposed system, defining the nature and the extent of the non-compliance.

IECNORM.COM : Click to view the PDF of IEC 61069-2:2016

Annex C (informative)

Examples of collation documentation

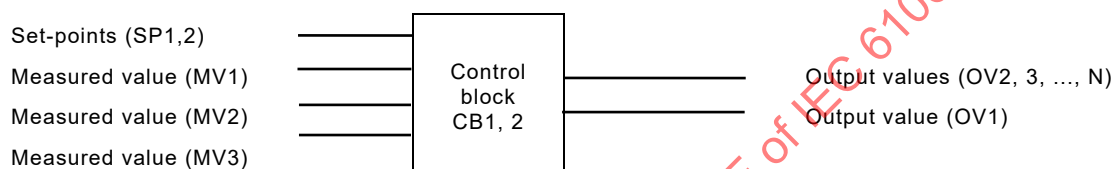
C.1 Overview

Annex C provides examples of collation documentation.

C.2 Example of furnace control documentation

C.2.1 Schematic of task

Figure C.1 shows a "master-slave control" for a furnace control documentation.



IEC

Figure C.1 – Control block

CB1 and CB2 are the PID parameters of the control blocks.

C.2.2 Task definition

C.2.2.1 Control and/or calculating algorithm

Temperature control	:	OV1	=	function [MV1, SP1 and CB1 (parameters PID)]
Fuel-gas control	:	OV2	=	function [function {MV2, MV3}, SP2/OV1 and CB2 (parameters PID)]
Fuel-gas throughput	:	OV3	=	function {M2, M3} = constant [square root {MV2*MV3}]
Temperature alarm	:	OV4	=	1 pour M1 < k degrees Celsius

C.2.2.2 Importance to mission

Task is of prime importance to the mission.

C.2.2.3 Boundary of the system

The system should include all modules and elements that allow the task as described to be fulfilled. The controlling elements (control valves) and sensors are outside the scope.

C.2.3 Input characteristics

Measured value 1 (MV1)	:	Measurement	:	temperature
		Type	:	thermocouple
		Characteristic	:	type J iron/copper-nickel
		Standard	:	IEC 60584-1
		Engineering units	:	degrees Celsius
Measured value 2	:	Measurement	:	differential pressure

(MV2)	Type	:	4 mA to 20 mA, intrinsically safe
	Power supply	:	by system
	Characteristic	:	linear with differential pressure
	Standard	:	
	Engineering units	:	

Measured value 3 (MV3)	Measurement	:	pressure
	Type	:	4 mA to 20 mA, intrinsically safe
	Power supply	:	by system
	Characteristic	:	linear with pressure
	Standard	:	
	Engineering units	:	Bar

Set-point value 1 (SP1)	Indication	:	as for MV1
	Engineering units	:	degrees Celsius

Set-point value 2 (SP2)	Indication	:	as for OV3
	Engineering units	:	tons per hour

C.2.4 Output characteristics

Output value 1 (OV1)	Duty	:	system internal set-point SP2
	Type	:	as for OV3
	Power supply	:	
	Characteristic	:	as for OV3
	Action	:	reverse
	Engineering units	:	

Output value 2 (OV2)	Duty	:	output to valve positioner
	Type	:	4 mA to 20 mA, intrinsically safe
	Power supply	:	by system
	Characteristic	:	linear
	Action	:	direct, valve closed at 4 mA
	Engineering units	:	linear, 0-100 %

Output value 3 (OV3)	Duty	:	input to CB2, fuel-gas control
	Type	:	internal calculation block
	Power supply	:	by system
	Characteristic	:	linear
	Action	:	
	Engineering units	:	linear, tons per hour

Output value 4 (OV4)	Duty	:	output to alarm panel
	Type	:	voltage free contact
	Power supply	:	from external source, 24 Vd.c.
	Characteristic	:	two position, open/closed
	Action	:	contact normally closed

Engineering units :

C.2.5 Operational functions

Operational personnel should be able to manipulate:

- set-points : set-point values SP1 and SP2;
- outputs : output values OV1 and OV2;
- modes : manual: output value OV2, manual: slave CB2, automatic: slave CB2, manual: master CB1, automatic: master CB1.

C.2.6 Monitoring functions

- Indications : MV1, MV2, MV3, SP1, SP2, OV(1...N)
- Recordings (short) : as for indications
- (medium) : MV1, MV2, MV3, OV3
- (long) : MV1, OV3
- Alarm : OV4 = MV1

C.2.7 Configuration

Operational personnel allowed to manipulate are:

- for control settings : the control/instrument engineer;
- for setting parameters : the control/instrument engineer;
- for commissioning : the instrument engineer/technician.

C.2.8 Flexibility

C.2.8.1 General

It should be possible to upgrade the system within the next five years with the following features.

C.2.8.2 Enhancing a function

Enhancing OV3 (function {MV2,MV3}) to:

function {MV2...5} = constant [square root {MV2*MV3*MV4/(MV5+variable)}]

C.2.8.3 Adding a control block

The addition of another control block to control the amount of fuel-oil with set-point SPy and output OVx, similar to the control block as specified for under C.2.2 above for OV2 and with the same enhancements as under C.2.8.2.

C.2.8.4 Adding a function

The addition of a logic function with the following possibilities:

- fuel-oil and fuel-gas outputs on manual control;
- fuel-oil and fuel-gas outputs on automatic control;
- fuel-oil on automatic control and fuel-gas on master-slave from temperature control;
- fuel-oil and fuel-gas both on master-slave, whereby it is possible to set the ratio between fuel-oil and fuel-gas.

C.2.8.5 Adding an external connection

The connection of the system to an optimizing and management information system including data collection and manipulation of control-parameters.

C.2.9 Functionality collation tables³

C.2.9.1 Coverage

Table C.1 – SRD coverage analysis

Task (SRD)			Coverage (SSD)			Analysis			
Type	Importance	Description/ characteristic	Supported by: ^{b)}			Compliance?		Further assessment?	
			Function	Module	Element	Yes	No	Yes	No
							Accepted?		
Master-slave: furnace control	Critical	Process interface ^{a)}	I/O monitor	I/O module					
		Measurements: MV1: temperature thermocouple type J	I/O reference tables	I/O module	I-card TC/J				
		MV2: differential pressure 4 mA to 20 mA intrinsically safe linear	I/O		I-card mA + intrinsically safe barrier				
		MV3 ... n							
		Outputs ^{a)} : valve position 4 mA to 20 mA			O-card, intrinsically safe				
		Data processing ^{a)}	Control	Process module	CPU-C				
		Computation ^{a)} : multiplication square root, Boolean			CPU-CB				
		Control 1): PID control logic control			CPU-CB				
		Trends ^{a)} : real time historical			PS-PM				

³ Tables 1, 2 and 3 provide examples of tables for three aspects of an SRD analysis, coverage, configurability and flexibility.

Task (SRD)			Coverage (SSD)			Analysis			
Type	Importance	Description/ characteristic	Supported by: ^{b)}			Compliance?		Further assessment?	
			Function	Module	Element	Yes	No	Yes	No
							Accepted?		
		archiving							
		Communication ^{a)} : I/O bus module bus system bus			Fbus FBusC SysBus				
		Human interface ^{a)}	OPS- DRV	OPS	CPU-ops Mem/GRD SysBusC				
		Indications in – raw values – engineering units							
		Calculations in – raw values – engineering units							
		Outputs in – raw values – engineering units							
		Parameters, constants and settings of: – control blocks – logic blocks – calculation blocks							
		Trends: real time historic			Mem-Ex				
		Reports: alarm shift logging			Mem-Ex				
		Graphics: plant displays templates configuration menus			GRD-Ex				
		Manipulation of: – set-points – control modes – outputs – parameters							

Task (SRD)			Coverage (SSD)			Analysis			
Type	Importance	Description/ characteristic	Supported by: ^{b)}			Compliance?		Further assessment?	
			Function	Module	Element	Yes	No Accepted?	Yes	No
		– settings – constants							
		Configuration tools			GRD-Ex				
		Interfaces to external systems ^{a)}			Special				

^{a)} Arranged as in IEC 61069-1:—, 5.1.1.

^{b)} The abbreviations shown are those encountered in the list of a manufacturer and are only used for illustration purposes.

C.2.9.2 Configurability

Table C.2 – SRD configurability analysis

Task (SRD)				Configurability		Analysis			
Type	Importance	Description/ characteristic	Configuration requirements	Supported by:		Compliance?		Further assessment?	
				Method	System state	Yes	No Accepted?	Yes	No
Master-slave: furnace control	Critical	Process interface ^{a)}							
		Measurements: MV1: temperature thermocouple type J	Instrument engineer/ technician	Use of special cards	Control on manual				
		MV2: differential pressure							
		MV3: ...							
		Outputs ^{a)} : valve position 4 mA to 20 mA	Instrument engineer/ technician		Local control				
		Data processing ^{a)}							
		Computation ^{a)} : multiplication square root Boolean	Control/ instrument engineer	Menu-driven	Control on manual				
		Control ^{a)} : PID control logic control	Control/ instrument engineer	Menu-driven	Control on manual				
		Trends ^{a)} : real time	Control/ instrument	Menu-driven	On-line				

Task (SRD)				Configurability		Analysis			
Type	Importance	Description/ characteristic	Configuration requirements	Supported by:		Compliance?		Further assessment?	
				Method	System state	Yes	No Accepted?	Yes	No
		historical archiving	engineer						
		Communication ^{a)} : I/O bus module bus system bus	Instrument engineer		System off- line				
		Human interface ^{a)}	Control/ instrument engineer	Menu- driven	System off- line				
		Indications in – raw values – engineering units							
		Calculations in – raw values – engineering units							
		Outputs in – raw values – engineering units							
		Parameters, constants and settings of – control blocks – logic blocks – calculation blocks							
		Trends real time historic		Special cards					
		Reports: alarm shift logging							
		Graphics: plant displays templates configuration menus		Menu- driven					
		Manipulation of – set-points – control modes – outputs – parameters							

Task (SRD)				Configurability		Analysis			
Type	Importance	Description/ characteristic	Configuration requirements	Supported by:		Compliance?		Further assessment?	
				Method	System state	Yes	No Accepted?	Yes	No
		– settings – constants							
		Configuration tools		Menu-driven					
		Interfaces to external systems ^{a)}			System off-line				

^{a)} Arranged as in IEC 61069-1:—, 5.1.1.

C.2.9.3 Flexibility

Table C.3 – SRD flexibility analysis

Task (SRD)				Flexibility		Analysis			
Type	Importance	Description/ characteristic	Flexibility requirement	Supported by:		Compliance?		Further assessment?	
				Method	System state	Yes	No Accepted?	Yes	No
Master-slave: furnace control	Critical	Process interface ^{a)}							
		Measurements: MV1: temperature, thermocouple type J	Addition	Plug-in of special cards/ config- uration	Control on manual				
		MV2: differential pressure							
		MV3...n							
		Outputs ^{a)} : valve position 4 mA to 20 mA	Addition		Control loop out of operation				
		Data processing ^{a)}							
		Computation ^{a)} : multiplication square root Boolean	Adding/ changing function	Menu- driven config- uration	Control on manual				
		Control ^{a)} : PID control logic control							
		Trends ^{a)} : real time historical archiving	Changes	Menu- driven	On-line				
		Communication ^{a)} : I/O bus module bus							

Task (SRD)				Flexibility		Analysis			
Type	Importance	Description/ characteristic	Flexibility requirement	Supported by:		Compliance?		Further assessment?	
				Method	System state	Yes	No	Yes	No
							Accepted?		
		system bus							
		Human interface ^{a)}							
		Indications in – raw values – engineering units	Addition of points	Menu- driven up to 256 pts	On-line				
		Calculations in – raw values – engineering units	Addition	Up to 64 calcula- tions	On-line				
		Outputs in – raw values – engineering units							
		Parameters, constants and settings of – control blocks – logic blocks – calculation blocks							
		Trends: real time historic		Max. 64 Max. 8					
		Reports: alarm shift logging		Max. 8 Max. 4					
		Graphics: plant displays templates configuration menus		Max. 4					
		Manipulation of – set-points – control modes – outputs – parameters – settings – constants							
		Configuration tools							
		Interfaces to external systems ^{a)}	Addition	Special	System off- line				

^{a)} Arranged as in IEC 61069-1:—, 5.1.1.

C.2.9.4 Reference document

IEC 60584-1:2013, *Thermocouples – Part 1: EMF specifications and tolerances*

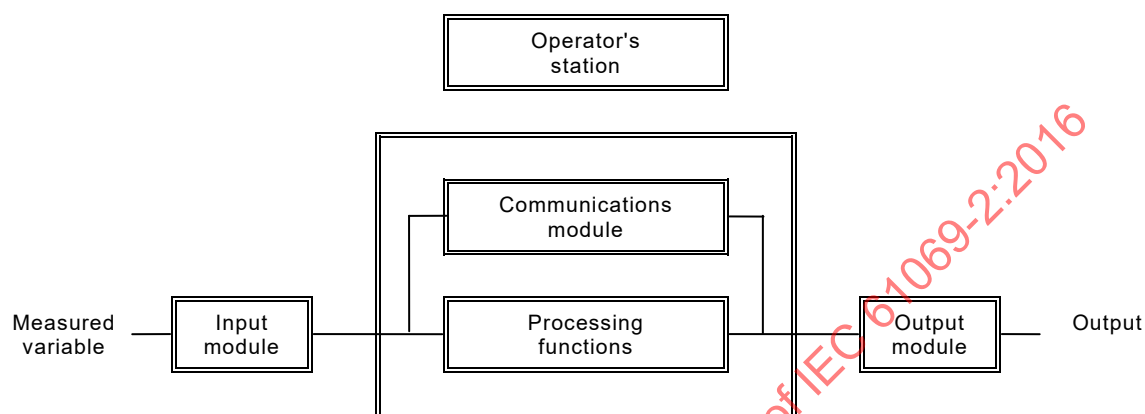
C.3 Example of simple control loop task documentation

C.3.1 Overview

Clause C.3 provides an example of simple control loop task documentation.

C.3.2 Schematic of task

Figure C.2 shows an example of schematic of a task.



IEC

Figure C.2 – Task schematic

C.3.3 Information flows

Process control action:	measured value	→ output
Keyboard manipulated process action:	operator station	→ output
Process measurement indication:	measured value	→ operator station
Feedback of manipulated value:	output	→ operator station

C.3.4 Performance tables

Table C.4 shows an example of performance table for information flow.

Table C.4 – Performance for information flow

Information flow	Accuracy %	Response time s	Sampling period s
Measured value – output	± 0,5	0,25	0,05
Operator station – output	± 0,5	0,50	0,20
Measured value – operator station	± 2,0	1,00	0,01
Output – operator station	± 2,0	1,00	0,01

Table C.5 shows an example of performance table for information translation.

Table C.5 – Information translation

Task	Information translation	Element	Accuracy %	Response times	Sampling periods
PID control	Measured value	Input module	0,2	0,1	0,01
	Output	PID module	0,1	N/A	0,01
		Output module	0,2	0,1	0,01
	Operator station	Keyboard	N/A	1,0	N/A
	Output	Communications module	N/A	0,2	0,001
		PID module	0,1	N/A	0,01
		Output module	0,2	0,1	0,01
	Measured value	Input module	0,2	0,1	0,01
	Operator station	Communications module	N/A	0,2	0,001
		Display	1,0	1,0	0,01
	Output	Output module	0,2	0,1	0,01
	Operator station	Communications module	N/A	0,2	0,001
		Display	1,0	1,0	0,01

C.3.5 Performance collation tables

Table C.6 shows an example of performance collation table.

C.4 Example of collation documentation (from SRD of a master-slave control task)

C.4.1 Overview

Clause C.4 provides an example of descriptions which provide requirements of dependability of a master-slave control task in the SRD.

C.4.2 Schematic of task

Figure C.3 provides a typical representation of a task as a control function block.

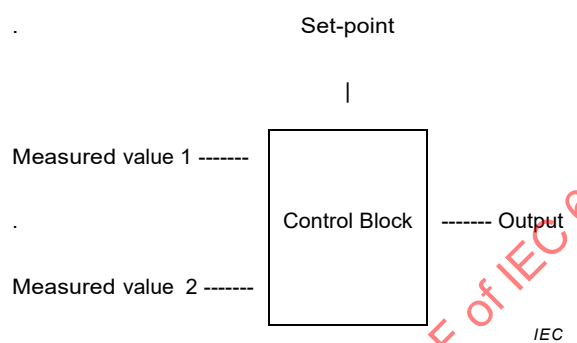


Figure C.3 – Schematic of task

C.4.3 Boundary states

Possible states of inputs:

- measured value 1: > high, normal, < low
- measured value 2: > high, normal, < low
- set-point: > high, normal, < low

Possible states of output(s):

- output: fully open, frozen, floating, fully closed.

Table C.7 provides an example of a concise method to describe the boundary states of a task.

Table C.7 – Failure states of task input and output

Task		Mode	Failure Event		
			Expected Frequency	Action to be taken	Time to restore
Master-Slave	Input	Measurement 1			
		>High	1 per year	Report/freeze output	*
		Normal	NA	N/A	-
		<Low	1 per year	Report/freeze output	*
		Measurement 2			
		>High	1 per year	Report/freeze last value	*
		Normal	NA	N/A	-
		<Low	1 per year	Report/output to high	*
		Set-point			
		>High	1 per year	Report/freeze last value	2 h
		Normal	NA	N/A	-
		<Low	1 per year	Report/output to high	2 h
	Output	Output			
		>High	1 per year	Report/freeze last value	2 h
		Normal	NA	N/A	-
		<Low	1 per year	Report/freeze last value	2 h

NOTES:

1. Depending on the boundary of the system under assessment, the inputs from measurements may or may not be under control of the system. In the case of the example, the measurements are outside the boundary and hence the term “expected” frequency of event is noted, equally the “time to restore” is not a system consideration. The set-point is controlled via a keyboard and hence under system control.
2. NA = non-applicable
3. * = This quantity is not a system property.

C.5 Example of collation documentation (from SSD of a master-slave control task)

Clause C.5 provides an example of descriptions which provide specifications of a master-slave control task related to dependability in the SRD.

Table C.8 provides an example of a dependability collation document for a master-slave control task.

Table C.8 – Dependability

Task	Supported by:			Dependability properties			
	Function	Module	Element ^{c)}	Availability ^{a)}		Credibility ^{b)}	
				Reliability ^{a)}	Maintainability ^{a)}	Integrity ^{b)}	Security ^{b)}
Master-Slave	I/O-monitor	I/O module	I-card Barrier				
			I-card Barrier				
			O-card Barrier				
			PS-I/O				
	Control	Process Module 1 or	CPU-PM				
			FbusC				
			DIA				
			PS-PM				
			SysBusC				
		Process Module 2	CPU-PM				
			FbusC				
			DIA				
			PS-PM				
			SysBusC				
	Human Interface	Operator Station 1 or	CPU-OPS				
			Mem-card				
			GrD-card				
			SysBusC				
		Operator Station 2	CPU-OPS				
			Mem-card				
			GrD-card				
			SysBusC				

^{a)} The abbreviations shown are those encountered in the list of a specific manufacturer and are only used for illustration purposes.
^{b)} Use format given in IEC 61709: Electric components – Reliability – Reference conditions for failure rates and stress models for conversion.
^{c)} Reference shall be made to the descriptions in the system specification document.

Bibliography

- [1] IEC TS 62603-1:2014, *Industrial process control systems – Guideline for evaluating process control systems – Part 1: Specifications*
 - [2] IEC 60584-1:2013, *Thermocouples – Part 1: EMF specifications and tolerances*
 - [3] ISO 9001:2015, *Quality management systems – Requirements*
 - [4] IEC 61069-4:—, *Industrial-process measurement, control and automation –Evaluation of system properties for the purpose of system assessment – Part 4: Assessment of system performance*
 - [5] IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*
-

IECNORM.COM : Click to view the full PDF of IEC 61069-2:2016

IECNORM.COM : Click to view the full PDF of IEC 61069-2:2016

SOMMAIRE

AVANT-PROPOS.....	42
INTRODUCTION.....	44
1 Domaine d'application.....	46
2 Références normatives	46
3 Termes, définitions, abréviations, acronymes, conventions et symboles	46
3.1 Termes et définitions	46
3.2 Abréviations, acronymes, conventions et symboles	46
4 Approche de l'évaluation.....	46
5 Méthode d'évaluation.....	47
5.1 Vue d'ensemble	47
5.1.1 Généralités	47
5.1.2 Phases	47
5.2 Définition des objectifs de l'évaluation	48
5.3 Conception et agencement de l'évaluation	49
5.3.1 Définition de l'objectif de l'évaluation	49
5.3.2 Propriétés du système et facteurs d'influence	50
5.3.3 Classement des informations détaillées	51
5.3.4 Mise en forme des informations recueillies	52
5.3.5 Sélection d'éléments d'évaluation	52
5.3.6 Spécifications de l'évaluation	52
5.4 Planification du programme d'évaluation	53
5.4.1 Vue d'ensemble	53
5.4.2 Développement d'activités d'évaluation.....	54
5.4.3 Programme d'évaluation.....	54
5.5 Exécution de l'évaluation.....	54
5.6 Rédaction du rapport d'évaluation.....	55
6 Techniques d'appréciation	55
Annexe A (informative) Cahier des charges du système (CdC).....	57
A.1 Vue d'ensemble	57
A.2 Analyse de la mission du système	57
A.2.1 Généralités	57
A.2.2 Formulation de la mission du système	57
A.2.3 Analyse de la mission du système en tâches	57
A.2.4 Attribution d'une importance relative aux tâches	58
A.2.5 Définition des facteurs d'influence	58
A.3 Revue du cahier des charges du système (CdC)	58
Annexe B (informative) Cahier des spécifications du système (CdS)	59
B.1 Vue d'ensemble	59
B.2 Développement du cahier des spécifications du système	59
B.2.1 Généralités	59
B.2.2 Vue d'ensemble du système	59
B.2.3 Définition des limites du système.....	60
B.2.4 Spécifications du système	60
B.2.5 Description du fonctionnement du système	61
B.2.6 Enoncé des justifications de la mise en œuvre du système	61

B.2.7	Déclaration de conformité avec les exigences du système	61
Annexe C (informative)	Exemples de recueil de documentation.....	62
C.1	Vue d'ensemble	62
C.2	Exemple de documentation de commande de chaudière	62
C.2.1	Schéma de principe de la tâche.....	62
C.2.2	Définition de la tâche	62
C.2.3	Caractéristiques d'entrée	62
C.2.4	Caractéristiques de sortie.....	63
C.2.5	Fonctions opérationnelles.....	64
C.2.6	Fonctions de surveillance	64
C.2.7	Configuration	64
C.2.8	Flexibilité	64
C.2.9	Tableaux de recueil des fonctionnalités	65
C.3	Exemple de documentation d'une tâche de commande en boucle simple	72
C.3.1	Vue d'ensemble	72
C.3.2	Schéma de principe de la tâche.....	72
C.3.3	Flux d'information.....	72
C.3.4	Tableaux de caractéristiques de fonctionnement	72
C.3.5	Tableaux de recueil de caractéristiques de fonctionnement.....	73
C.4	Exemple de recueil de documentation (à partir du CdC pour une tâche de commande maître-esclave)	75
C.4.1	Vue d'ensemble	75
C.4.2	Schéma de principe de la tâche.....	75
C.4.3	Etats des limites	75
C.5	Exemple de recueil de documentation (à partir du CdS pour une tâche de commande maître-esclave)	76
Bibliographie		78
Figure 1	Structure générale de l'IEC 61069	45
Figure 2	Matrice d'évaluation	50
Figure C.1	Bloc de commande	62
Figure C.2	Schéma de principe de la tâche.....	72
Figure C.3	Schéma de principe de la tâche.....	75
Tableau 1	Phases de l'évaluation, données d'entrée et de sortie	48
Tableau C.1	Analyse de la couverture du CdC.....	65
Tableau C.2	Analyse de la configurabilité du CdC.....	67
Tableau C.3	Analyse de la flexibilité du CdC	70
Tableau C.4	Caractéristiques de fonctionnement du flux d'information	73
Tableau C.5	Transfert d'information.....	73
Tableau C.6	Recueil de caractéristiques de fonctionnement.....	74
Tableau C.7	Etats de défaillance à l'entrée et en sortie de la tâche	76
Tableau C.8	Sûreté de fonctionnement.....	77

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

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, accèdent 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 61069-2 a été établie par le sous-comité 65A: Aspects systèmes, 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 1993. 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 61069-2:1993 visant à mieux organiser l'ensemble complet de normes et à le rendre plus cohérent;
- b) L'IEC TS 62603-1:2014 a été incorporée dans cette édition.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/790/FDIS	65A/799/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

Evaluer 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, la norme 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 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 des parties ainsi que la relation entre les parties de l'IEC 61069 sont représentées à la Figure 1.

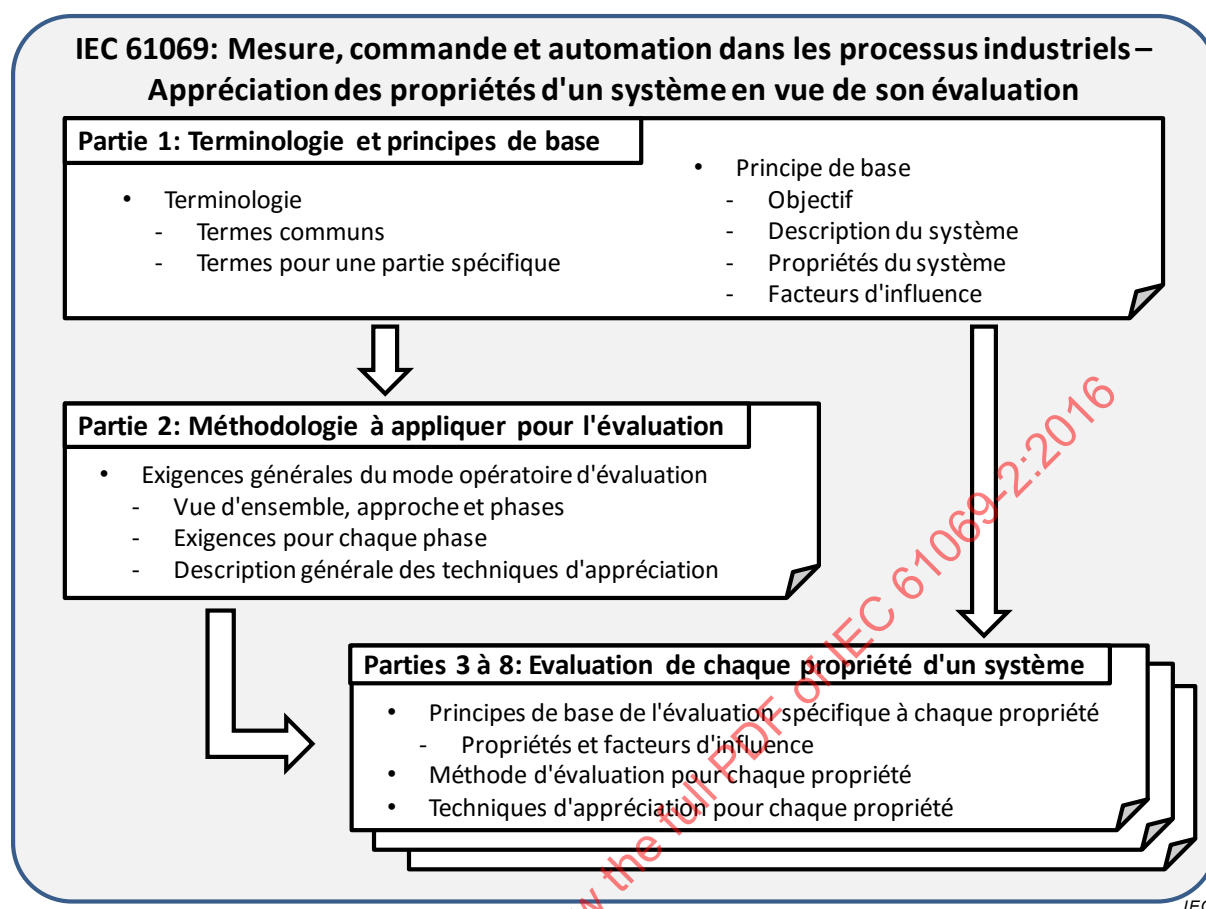


Figure 1 – Structure générale de l'IEC 61069

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

1 Domaine d'application

La présente partie de l'IEC 61069 spécifie la méthodologie de l'évaluation d'un système de commande de base (BCS, Basic Control System) reposant sur les principes de base de l'IEC 61069-1.

Celle-ci décrit la méthode d'analyse, de pondération de l'importance relative des diverses propriétés du système et des facteurs d'influence, et de détermination du programme d'évaluation.

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 61069-1:—¹, *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*

3 Termes, définitions, abréviations, acronymes, conventions et symboles

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'IEC 61069-1 s'appliquent.

3.2 Abréviations, acronymes, conventions et symboles

Pour les besoins du présent document, les abréviations, acronymes, conventions et symboles donnés dans l'IEC 61069-1 s'appliquent.

4 Approche de l'évaluation

Les BCS étant des systèmes complexes, une évaluation totalement exhaustive nécessite inévitablement des dépenses en termes d'effort et de temps qui ne sont ni pratiques ni rentables. Il est donc important d'analyser et de spécifier minutieusement les objectifs de l'évaluation avant de planifier un programme d'évaluation.

La mission du système, ou la classe de missions, est divisée en tâches.

¹ A paraître simultanément avec la présente partie de l'IEC 61069.

Il convient de définir la ou les tâches que le système doit exécuter en fonction du BCS sélectionné, de ses propriétés et des fonctions requises. Ceci permet de spécifier avec précision les fonctions exigées pour que le système exécute sa ou ses missions.

Les missions du système requièrent généralement certaines caractéristiques du système qui ne sont pas directement associées aux tâches du système. Ces caractéristiques sont par exemple la documentation et les services de support.

Le programme d'évaluation doit être conçu en fonction des objectifs de l'évaluation, des exigences du système et des spécifications du système. Il convient de le préparer à l'avance.

NOTE Dans certains cas, par exemple une application réglementée, il peut être nécessaire que l'évaluation soit conçue et exécutée par une partie indépendante.

En l'absence de mission, il n'est pas possible d'évaluer le système; toutefois, il est possible de réaliser un examen du système afin de rassembler et d'organiser des données qui pourront servir lors d'évaluations ultérieures.

5 Méthode d'évaluation

5.1 Vue d'ensemble

5.1.1 Généralités

Les détails du programme d'évaluation doivent être dérivés de l'étude des objectifs de l'évaluation (indiqués en 5.2) et des données comprises dans les documents suivants:

- cahier des charges du système (CdC),
- cahier des spécifications du système (CdS).

NOTE 1 Le cahier des charges du système est expliqué à l'Annexe A.

NOTE 2 Le cahier des spécifications du système est expliqué à l'Annexe B.

L'évaluation fait correspondre les éléments du cahier des charges du système avec ceux du cahier des spécifications du système dans le but d'atteindre les objectifs de l'évaluation.

Si au cours de l'une quelconque des phases de l'évaluation, certaines informations du CdC ou du CdS sont manquantes ou incomplètes, il convient d'adresser des questions spécifiques aux rédacteurs du CdC et du CdS afin d'obtenir les informations complémentaires requises.

La méthode d'évaluation est un outil à utiliser pendant le cycle de vie du BCS. Le cycle de vie ne fait cependant pas partie du domaine d'application de l'IEC 61069-2. Il convient toutefois de prendre en compte le cycle de vie général du BCS au cours du développement d'un BCS et de la définition de son évaluation.

Il convient de planifier des évaluations pour chaque étape appropriée du cycle de vie, par exemple à la mise en service.

5.1.2 Phases

L'évaluation comporte les phases suivantes:

- définition des objectifs de l'évaluation;
- conception et agencement de l'évaluation;
- planification du programme d'évaluation;
- exécution de l'évaluation;
- rédaction des résultats.

Les phases ainsi que leurs données d'entrée et de sortie sont représentées dans le Tableau 1.

Tableau 1 – Phases de l'évaluation, données d'entrée et de sortie

Phase	Données d'entrée	Données de sortie
Définition des objectifs de l'évaluation	CdC et CdS	Objectif (documenté) de l'évaluation Protocole d'évaluation
Conception et agencement de l'évaluation	Objectif de l'évaluation CdC CdS	Spécifications de l'évaluation
Planification du programme d'évaluation	Spécifications de l'évaluation	Programme d'évaluation
Exécution de l'évaluation	Programme d'évaluation	Résultat des appréciations
Rédaction des résultats	Résultat des appréciations	Rapport d'évaluation

5.2 Définition des objectifs de l'évaluation

Les objectifs de l'évaluation doivent être indiqués et documentés avant le début de l'évaluation, comme base de la planification et de la préparation du programme d'évaluation. Il convient qu'ils soient clairement et soigneusement indiqués.

Ces objectifs forment la base des principes directeurs tout au long de l'évaluation en déterminant:

- le domaine d'application,
- la nature de l'appréciation,
- le degré d'exhaustivité de l'appréciation,
- les mesures et les observations à exécuter,
- le type de rapports à produire.

Les objectifs orientent le coût de l'évaluation et les ressources exigées pour mener l'évaluation.

Il est donc de la plus haute importance que les objectifs et le domaine d'application de l'évaluation soient bien documentés et aient fait l'objet d'un accord avant la poursuite du développement du programme d'évaluation.

Il convient de définir la description de l'ampleur des changements du BCS nécessitant une réévaluation, par exemple une extension du BCS.

Il convient de définir et planifier les mises à jour de l'évaluation, au cours du cycle de vie du BCS, indépendamment des changements et extensions, par exemple après 10 ans de fonctionnement.

Il convient de définir la ou les autorités pouvant exiger une évaluation ou une réévaluation.

Il convient en outre de définir la ou les autorités qui approuvent les évaluations ou les réévaluations.

Pendant l'évaluation, il convient de réaliser des revues à des points de revue planifiés ou à intervalles prédéterminés. Il convient que ces revues aient lieu au moins à la fin de chaque phase.

Les objectifs de l'évaluation peuvent être, par exemple:

- évaluer un système spécifique pour une mission particulière;
- évaluer plusieurs configurations d'un système unique pour une mission particulière;
- comparer plusieurs systèmes pour une mission particulière;
- obtenir l'évaluation d'un système particulier à usage général pour plusieurs missions différentes;
- établir l'aptitude d'un système pour une mission particulière;
- établir l'aptitude d'un système pour une classe de missions définie.

Le protocole d'évaluation doit être défini de manière à inclure:

- les autorités d'évaluation en charge de la modification et de la publication du programme d'évaluation;
- les spécifications de l'évaluation et les rapports d'évaluation;
- les modes opératoires à suivre;
- les actions d'urgence permises sans autorisation préalable au cas où l'évaluation ne peut être menée comme prévu.

5.3 Conception et agencement de l'évaluation

5.3.1 Définition de l'objectif de l'évaluation

5.3.1.1 Limites du système

Les limites du système doivent être définies minutieusement en identifiant «ce qui appartient et ce qui n'appartient pas» au système à évaluer.

On doit définir les limites du système à évaluer en tenant compte de tous les aspects des facteurs d'influence décrits en 5.3 de l'IEC 61069-1; —. Elles doivent être documentées dans les spécifications de l'évaluation.

La limite du système peut être physique (par exemple, matériel, géographie) et/ou virtuelle (par exemple, informations, communication).

Les objectifs de l'évaluation sont traduits en un domaine d'application de l'évaluation. Pour pouvoir développer le domaine d'application, les propriétés du système décrites aux paragraphes 5.2.2 à 5.2.7 de l'IEC 61069-1; — doivent être prises en compte.

5.3.1.2 Configuration du système

La ou les configurations du système à évaluer doivent être spécifiées dans les spécifications de l'évaluation. La configurabilité du système à proprement parler pouvant être une propriété du système à évaluer, il convient de spécifier avec soin la configuration du système dont les éléments d'évaluation sont appréciés.

Si l'objectif de l'évaluation est d'évaluer un système spécifique pour une mission particulière, l'évaluation doit être menée sur une configuration spécifique du système et cette configuration doit être documentée dans les spécifications de l'évaluation.

Si l'objectif de l'évaluation est d'évaluer la flexibilité d'un système à satisfaire à une large gamme d'exigences typiques rencontrées dans un secteur industriel spécifique, l'évaluation doit être menée sur une gamme de modules définis pouvant être configurés de différentes manières. La gamme de modules et la variété des configurations doivent être documentées dans les spécifications de l'évaluation.

Il arrive quelquefois qu'un système soit si complexe que des appréciations exhaustives de toutes les propriétés du système ne soient pas rentables, ni même possibles. En prenant bien en compte les objectifs, la configuration du système et les facteurs d'influence, les

appréciations peuvent être réduites afin d'inclure uniquement les éléments de l'évaluation qui sont les plus importants pour la mission du système.

5.3.2 Propriétés du système et facteurs d'influence

Les éléments d'évaluation requis pour l'évaluation doivent être spécifiés. La valeur ou la plage de valeurs requises pour chaque propriété du système et chaque facteur d'influence doit également être spécifiée.

De plus, autant que possible, il convient d'inclure les facteurs d'influence tels que décrits dans l'IEC 61069-1.

Il convient d'examiner soigneusement chaque élément d'évaluation afin de déterminer s'il influence ou dégrade le système de telle sorte qu'il entrave ou empêche le bon fonctionnement des autres éléments d'évaluation.

Ces considérations doivent être documentées sous forme de spécifications de l'évaluation afin de montrer les contraintes pesant sur l'ordonnancement des activités de l'évaluation.

Une matrice, dans laquelle les cellules correspondent aux éléments d'évaluation, constitue un moyen pratique de documenter les propriétés d'un système et les facteurs d'influence.

Une matrice générale récapitulant les éléments d'une évaluation est représentée à la Figure 2.

Propriétés du système		Fonctionnalité			Caractéristiques de fonctionnement			Sûreté de fonctionnement			Opérabilité			Sécurité du système			Autres propriétés		
Facteurs d'influence																			
Mission / Tâche																			
Personnel																			
Processus																			
Infrastructure																			
Environnement																			
Systèmes extérieurs																			

IEC

Figure 2 – Matrice d'évaluation

Les éléments d'évaluation qu'il est nécessaire d'inclure dans l'évaluation doivent être sélectionnés et leurs priorités relatives doivent être déterminées. Ceci peut effectuer cela à l'aide de cette matrice, qui permet d'examiner chaque propriété du système et chaque facteur d'influence, et de tenir compte de l'objectif de l'évaluation.

Un élément d'évaluation peut ensuite être progressivement détaillé, par exemple au moyen de groupes ou de sous-groupes de propriétés, dans lesquels les titres de la matrice générale sont développés en propriétés du système et facteur d'influence plus détaillés.

Il convient également d'identifier pour référence ultérieure les éléments d'évaluation non pertinents pour l'évaluation particulière et de documenter les raisons de leur exclusion.

5.3.3 Classement des informations détaillées

Le recueil est l'étape de cette phase qui consiste à extraire les informations nécessaires à la détermination des candidats potentiels parmi les éléments d'évaluation. Les informations fournies par ce processus servent à la conception et à l'agencement de l'évaluation.

Pour le recueil, les informations nécessaires doivent être extraites du CdC et du CdS.

Le CdC et le CdS doivent être soigneusement examinés afin de compiler des énoncés précis et concis des sujets. Les sujets peuvent être:

- les limites du système;
- les zones de non-conformité des spécifications du système par rapport aux exigences du système;
- la liste des tâches requises et futures;
- les fonctions fournies pour exécuter les tâches requises et futures;
- la liste des chemins de données alternatifs reliant les fonctions en soutien aux tâches requises;
- l'attribution des fonctions aux modules et aux éléments;
- le nombre de ces modules et éléments;
- la mesure dans laquelle ces modules et éléments sont utilisés pour remplir les tâches requises;
- les propriétés du système pour chacune des fonctions ci-dessus;
- les facteurs d'influence pour chacun des modules et éléments ci-dessus.

Une liste des éléments d'évaluation potentiels doit être créée à partir de ces sujets. Les éléments d'évaluation doivent être spécifiés suivant les configurations spécifiques du système en fonction de l'objectif de l'évaluation.

Chaque élément d'évaluation potentiel doit être examiné afin de décider de la mesure dans laquelle cet élément sera apprécié pour obtenir l'augmentation nécessaire du niveau de confiance.

Il convient de décrire les énoncés en termes qualitatifs et quantitatifs, ainsi que leur plage de valeurs, le cas échéant.

NOTE L'Annexe C donne des exemples de recueil de documentation.

Pour chaque tâche à évaluer, il convient de décrire les données d'entrée, les résultats en sortie et le fonctionnement.

Il convient que les notes relatives aux données d'entrée comprennent:

- les états d'entrée autorisés et les états de sortie correspondants autorisés;
- les états d'entrée non autorisés et les actions correspondantes requises.

Il convient que les notes relatives aux résultats en sortie comprennent:

- les états de sortie autorisés;

- les états de sortie non autorisés et les actions correspondantes requises.

Pour chaque tâche, il convient d'indiquer clairement les informations suivantes concernant les tâches:

- types de défaillances qui affectent chaque tâche;
- fréquence autorisée d'apparition de chaque défaillance;
- action à entreprendre pour chaque défaillance;
- durée maximale d'arrêt de la tâche avant la restauration du module.

5.3.4 Mise en forme des informations recueillies

Il convient de documenter les informations recueillies comme indiqué en 5.3.3, sous une forme qui permette leur utilisation lors de la planification du programme d'évaluation.

S'il manque des informations pour le recueil, il convient d'obtenir les informations requises supplémentaires auprès des rédacteurs du CdC et du CdS. Il convient que ces informations supplémentaires soient enregistrées correctement dans les spécifications de l'évaluation.

5.3.5 Sélection d'éléments d'évaluation

La liste complète des éléments d'évaluation est réduite en appliquant les filtres suivants:

- importance de la ou des tâches pour la mission;
- niveau de confiance existant, basé sur une connaissance préalable;
- niveau d'interdépendance des différentes fonctions, nombre d'interfaces, réutilisation de la même fonction dans différentes tâches;
- disponibilité de connaissances préalables générales et la mesure dans laquelle elles s'appliquent aux éléments d'évaluation.

Il convient d'évaluer l'importance relative des tâches en tenant compte à la fois de l'importance des tâches lors d'une phase particulière de la durée de vie du système et de la durée de la phase; en effet, l'importance peut varier en fonction de la phase.

Le niveau de confiance existant peut s'appuyer sur la réussite du système dans des missions similaires ou identiques, l'expérience acquise avec le fabricant, l'expérience d'utilisateurs possédant le même type de système ou des systèmes comparables.

Les éléments d'évaluation qui sont requis par les organismes de réglementation nationaux et/ou internationaux doivent être évalués selon les règles figurant dans lesdites réglementations.

Les éléments d'évaluation doivent permettre de vérifier que le BCS est conforme à la réglementation nationale en vigueur sur le site où le système doit être utilisé.

5.3.6 Spécifications de l'évaluation

Les spécifications de l'évaluation consistent en un document qui décrit ce qu'il convient d'évaluer. Il convient que les spécifications de l'évaluation spécifient au moins les points suivants:

- l'objectif de l'évaluation comme spécifié en 5.2;
- les limites du système comme spécifié en 5.3.1.1;
- la configuration du système comme spécifié en 5.3.1.2;
- la matrice d'évaluation comme spécifié en 5.3.2;
- la liste d'éléments d'évaluation comme spécifié en 5.3.2;

- la liste de tâches comme spécifié en 5.3.3;
- les critères utilisés pour filtrer les éléments comme spécifié en 5.3.5;
- les normes de référence pour chaque élément d'évaluation.

5.4 Planification du programme d'évaluation

5.4.1 Vue d'ensemble

Au cours de cette phase, un programme d'évaluation doit être planifié sur la base des spécifications de l'évaluation préparées à la phase précédente.

L'objectif de la conception du programme d'évaluation est d'accroître la confiance dans le jugement de la bonne aptitude d'un système à exécuter sa mission.

Les activités d'évaluation doivent maximiser cet accroissement de la confiance tout en restant dans des limites définies de contraintes de coût et de temps.

Le programme d'évaluation doit spécifier les activités d'évaluation et leur ordre sur une échelle temporelle de manière à pouvoir contrôler l'évaluation.

Le programme d'évaluation doit comprendre un ensemble d'activités d'évaluation, dont chacune peut être:

- une observation au niveau du système;
- une observation à des niveaux inférieurs (si nécessaire jusqu'à un élément individuel) combinée à une synthèse au niveau du système.

La conception de chaque activité d'évaluation dépend de la propriété du système étudiée.

Il convient que le programme d'évaluation spécifie également le détail de chaque activité d'évaluation, dont:

- le type de technique d'évaluation;
- les outils et alimentations nécessaires.

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

Les techniques d'appréciation choisies peuvent être soit des techniques analytiques, fondées uniquement sur la documentation du système, soit des techniques empiriques, nécessitant l'accès à un système d'appréciation. En pratique, les techniques choisies sont une combinaison d'analyses et d'essais empiriques utilisant la documentation du système et une combinaison limitée de modules.

Les activités d'évaluation doivent être planifiées en ordre logique en respectant toutes les contraintes des éléments d'évaluation identifiés dans les spécifications de l'évaluation. Pour pouvoir sélectionner les activités d'évaluation incluses dans le programme d'évaluation, il convient d'analyser chaque activité d'évaluation en déterminant les aspects suivants:

- techniques et outils d'appréciation,
- coût et temps nécessaires à l'exécution,
- importance.

Il convient de répéter les étapes de la planification du programme d'évaluation jusqu'à ce que toutes les parties impliquées se mettent d'accord sur le programme.

5.4.2 Développement d'activités d'évaluation

Il convient de développer la liste des activités d'évaluation sur la base des critères suivants:

- le type d'analyse et/ou d'appréciation requis pour étayer l'évaluation;
- l'importance de la propriété particulière du système par rapport à l'ensemble de la mission;
- l'importance des propriétés du système et des facteurs d'influence pour la mission;
- les connaissances et compétences requises pour exécuter chaque analyse et/ou essai;
- les contraintes sur la planification de l'évaluation en raison des effets permanents que peuvent avoir les essais portant sur les caractéristiques de fonctionnement ou les autres propriétés du système;
- les contraintes techniques pour l'évaluation telles que taille, poids, disponibilité des alimentations, maîtrise de l'environnement d'essai;
- la disponibilité du personnel choisi;
- la disponibilité d'un groupe d'opérateurs choisis pour effectuer certaines tâches permettant d'étudier l'opérabilité;
- les outils et services requis pour exécuter les analyses et essais;
- la disponibilité des outils pour les activités d'évaluation;
- l'estimation du coût et du temps pour chaque analyse et essai;
- l'estimation du coût et du temps nécessaires aux activités d'évaluation;
- le niveau de priorité pour chacune des activités d'évaluation;
- le niveau de confiance en fonction des connaissances préalables.

Il est quelquefois nécessaire d'envisager plusieurs techniques d'appréciation qui se complètent mutuellement.

Toutes les listes d'activités d'évaluation doivent être combinées dans le programme d'évaluation pour le système.

5.4.3 Programme d'évaluation

Il convient que le programme d'évaluation spécifie au moins les points suivants:

- les techniques d'appréciation sélectionnées comme spécifié en 5.4.1;
- les critères à prendre en compte comme indiqué en 5.4.2;
- les activités d'évaluation obtenues en 5.4.2;
- l'augmentation requise du niveau de confiance;
- la planification de l'évaluation, en tenant compte des effets permanents possibles que peuvent avoir les essais;
- les modes de défaillance à analyser et/ou à évaluer et les effets résultants prévus;
- les mécanismes d'intégrité physique et de cybersécurité prévus dans le système.

5.5 Exécution de l'évaluation

Les activités d'évaluation doivent être réalisées conformément au programme d'évaluation spécifié en 5.4 et au protocole d'évaluation prescrit spécifié en 5.2.

Si et lorsque des écarts sont nécessaires par rapport au programme ou au protocole d'évaluation, il convient de les signaler dans le rapport d'évaluation et, sauf si des mesures précédemment agréées peuvent être prises, ceux-ci doivent être approuvés par l'autorité d'évaluation.

Tous les calculs, observations et mesures doivent être enregistrés au moment de leur exécution en vue de les inclure dans le rapport d'évaluation.

5.6 Rédaction du rapport d'évaluation

La conduite et les résultats de l'évaluation doivent être documentés dans un rapport d'évaluation. Il convient que le rapport d'évaluation soit précis, clair, non ambigu et objectif dans la présentation de l'objectif, des résultats et de toutes les informations pertinentes de l'évaluation.

Les rapports d'évaluation doivent comprendre au moins les renseignements suivants:

- le titre du rapport d'évaluation;
- une identification unique du rapport;
- la date de publication;
- le nom de l'autorité d'évaluation;
- la référence des spécifications de l'évaluation décrites en 5.3.6;
- la référence du programme d'évaluation spécifié en 5.4.3;
- la configuration du système, par exemple le type et le nombre de données d'entrée/de sortie, le rythme de balayage requis, la mission du système, les tâches et fonctions;
- les caractéristiques de la mission, comme le type de processus dans le cas de l'évaluation d'une mission particulière;
- une description et une identification du système évalué, comprenant une liste représentant le matériel avec les numéros de modèle et le logiciel utilisés, avec la date de publication;
- un résumé des points importants découlant de l'évaluation et des conclusions obtenues;
- un compte rendu des modes opératoires, méthodes, spécifications et essais (de préférence résumés sous forme de matrice et complétés de documents de référence);
- les raisons de la sélection des éléments d'évaluation particuliers à évaluer, et les raisons de la non-sélection d'autres éléments d'évaluation;
- tout écart par rapport au programme d'évaluation (additions ou exclusions);
- les mesures, essais et résultats dérivés illustrés par des tableaux, graphiques, schémas ou photographies, suivant le cas;
- les défaillances observées;
- un énoncé des incertitudes de mesure;
- un énoncé indiquant si oui ou non le système est conforme aux exigences vis-à-vis desquelles le système a été évalué, comprenant la déclaration de toute divergence éventuelle.

Il convient que le format du rapport d'évaluation soit normalisé, afin de faciliter la comparaison d'évaluations de systèmes différents. Il convient d'illustrer les résultats de l'évaluation au moyen d'informations sous des formes appropriées, telles que des listes, des matrices et des graphiques.

Les corrections ou additions au rapport après sa publication doivent être apportées uniquement au moyen d'un rapport supplémentaire, se référant au rapport original identifié par son titre et son numéro. Ce rapport supplémentaire doit satisfaire aux mêmes exigences que le rapport original, le cas échéant.

6 Techniques d'appréciation

La ou les techniques d'appréciation utilisées doivent être choisies de façon à ce que les résultats puissent être comparés de manière qualitative et/ou quantitative aux exigences

définies dans le cahier des charges du système, avec le niveau de confiance requis dans l'évaluation.

Les techniques d'appréciation choisies peuvent être des techniques analytiques, se basant uniquement sur la documentation du système et des preuves ou des données antérieures, mais dans certains cas une combinaison de techniques analytiques et empiriques, nécessitant l'accès à un système d'appréciation, peut être utilisée.

En pratique, les techniques choisies sont une combinaison d'analyses et d'essais empiriques utilisant la documentation du système et une combinaison (limitée) de modules.

Dans ce but, il convient de recourir à un modèle du système qui intègre une sélection de fonctions du système; ces dernières doivent être suffisamment représentatives des tâches à exécuter et illustrer en détail les possibilités de communications bidirectionnelles offertes par l'interface homme-machine.

NOTE Un exemple de ce modèle est décrit à l'Annexe D de l'IEC 61069-4:—².

² A paraître simultanément avec la présente partie de l'IEC 61069.

Annexe A (informative)

Cahier des charges du système (CdC)

A.1 Vue d'ensemble

L'Annexe A décrit une méthode de développement et de révision du CdC, comprenant les points de contrôle de chaque propriété du système.

A.2 Analyse de la mission du système

A.2.1 Généralités

Pour évaluer un BCS, il est nécessaire d'établir la mission du système.

La mission du système ne peut être correctement définie que si le système est étudié dans son contexte, constitué par le personnel, le processus auquel il est associé et tout autre système associé, ainsi que l'environnement dans lequel le système fonctionne.

Les activités mentionnées en A.2.2, A.2.3, A.2.4 et A.2.5 conduisent au cahier des charges du système (CdC).

A.2.2 Formulation de la mission du système

L'objectif, à cette étape, est de définir la mission du BCS, et non la fonction qu'il doit exécuter.

Il convient que la description de la mission indique l'objectif à atteindre, et non pourquoi et comment l'atteindre.

Il convient d'élaborer la mission en décrivant ses phases. Celles-ci peuvent comprendre:

- la configuration initiale et la mise en service de l'installation complète, dont le personnel, l'usine, le BCS et les autres systèmes utilisés pour accomplir la mission;
- la configuration ou l'installation pour des cycles de production spécifiques;
- la production, qui peut consister en un fonctionnement stable et continu ou en des séquences programmées de sous-opérations;
- le transfert d'un cycle de production à un autre;
- l'arrêt d'urgence ou la transition à un état de veille sécurisé;
- l'arrêt normal;
- les mises à jour et les modifications au système en vue d'incorporer de nouvelles tâches ou fonctions;
- le déclassement du système après sa phase opérationnelle.

Cela n'est pas toujours évident, mais la génération, la mise en service et le déclassement du système sont des phases importantes qui peuvent faire partie de la mission du système.

A.2.3 Analyse de la mission du système en tâches

Pour exécuter la mission, le BCS doit exécuter des tâches spécifiques et/ou associer des propriétés du système spécifiques à chacune des phases de la mission identifiées ci-dessus. Ces phases sont examinées afin de définir les tâches que le système doit exécuter.

Les tâches d'une phase peuvent être par exemple:

- surveillance et affichage centralisé des valeurs surveillées, qui peuvent comprendre le traitement des variables mesurées en vue de dériver les valeurs des variables de la mission;
- activation d'une phase spécifique du processus en fonction de commandes manuelles ou automatiques;
- commande automatique de processus, par exemple commande automatique d'une variable de processus particulière;
- commande de verrouillage entre les variables de processus;
- initiation et exécution automatiques d'une phase.

Le BCS peut se voir demander d'exécuter l'une des tâches spécifiques en totalité ou en partie, c'est-à-dire une tâche partagée avec un autre système ou un autre membre du personnel.

Chaque tâche est définie de manière suffisamment détaillée pour que l'étendue de la tâche attribuée au BCS soit claire.

Pour chacune des tâches, il convient que les exigences soient liées à la fonctionnalité, aux caractéristiques de fonctionnement, à la sûreté de fonctionnement, à l'opérabilité, à la sécurité du système et/ou à d'autres propriétés du système, par ex. l'assurance de la qualité, les services après-vente, etc.

Il convient de noter qu'à ce stade, l'objectif est de définir les tâches du système, et non les fonctions du système.

A.2.4 Attribution d'une importance relative aux tâches

Il convient d'étudier à ce stade dans quelle mesure la mission dépend de chacune des tâches. Il convient de classer les tâches au moins en groupes relatifs à leur importance pour la mission:

- essentielle: tâches essentielles pour accomplir la mission;
- significative: tâches non essentielles mais ayant un effet significatif sur la rentabilité de la mission;
- souhaitable: tâches souhaitables mais ayant peu d'effets quantifiables sur la mission.

A.2.5 Définition des facteurs d'influence

La bonne exécution de chacune des tâches nécessaires à la mission peut être affectée par des facteurs qui influencent cette exécution.

A ce stade, il est nécessaire d'étudier, pour chacune des tâches, les facteurs qui peuvent influencer les critères requis pour cette tâche.

A.3 Revue du cahier des charges du système (CdC)

Les lignes directrices relatives aux points de contrôle du cahier des charges du système pour chaque type de propriété sont données en Annexe A de la Partie correspondant à la propriété considérée.

L'efficacité de l'évaluation dépend de la clarté avec laquelle sont exprimées les exigences et de leur exhaustivité.

Annexe B (informative)

Cahier des spécifications du système (CdS)

B.1 Vue d'ensemble

L'Annexe B décrit une méthode de développement et de révision du CdS, comprenant les points de contrôle de chaque propriété du système.

B.2 Développement du cahier des spécifications du système

B.2.1 Généralités

Le point de départ de la spécification du CdS est le CdC divisé en tâches, en fonction de leur importance relative.

De ce point de départ et à partir du mapping des tâches sur le modèle fonctionnel (voir 5.1.1 et l'IEC 61069-1:—, Figure 4), il est possible de dériver une mise en œuvre du système qui répond aux exigences du système.

Pendant la phase de mapping, le système proposé par le CdS est comparé à la mission détaillée décrite dans le CdC.

Pour permettre une analyse efficace de la conformité avec les exigences du système, il est important que les spécifications du système proposées identifient plusieurs points clés. Ceux-ci sont examinés en détail dans les B.2.2 à B.2.7.

Les activités, mentionnées aux B.2.2 à B.2.7, conduisent au cahier des spécifications du système.

B.2.2 Vue d'ensemble du système

L'objet de la vue d'ensemble est de relier la mise en œuvre du système à la mission du système telle que décrite dans le CdC.

De même que la mission peut être divisée de manière hiérarchique en tâches, le système à évaluer peut être décomposé de manière hiérarchique en modules et éléments.

Il est possible que cette décomposition entraîne des schémas de présentation et des descriptions supplémentaires.

Il convient que ceux-ci contiennent au moins des informations sur les aspects suivants:

- tous modules d'interface avec le processus, l'opérateur, les systèmes extérieurs, etc.;
- modules de communication;
- modules de traitement de l'application;
- interaction entre les modules;
- distances relatives et absolues et emplacements des modules.

Pour la décomposition, il est important de savoir que la plupart des BCS modernes sont basés sur une architecture hybride, constituée d'une combinaison d'équipements de mesure et commande séparés et de logiciels associés.

B.2.3 Définition des limites du système

Un système possède plusieurs limites distinctes, inhérentes au processus, à l'alimentation en énergie, à l'environnement dans lequel le système est placé, aux autres systèmes extérieurs connectés et aux utilisateurs du système (opérateurs, personnel de maintenance).

Les limites du système sont définies minutieusement en identifiant «ce qui appartient et ce qui n'appartient pas» au système à évaluer, en tenant compte au moins des éléments suivants:

- Les limites du processus peuvent être placées de façon à inclure ou exclure les conditionneurs de signal, les isolateurs électriques, les unités de conversion, les câbles, les appareils d'entrée/sortie tels que les capteurs et les éléments de commande finaux, etc.
- Les limites des alimentations sont définies de façon à tenir compte des équipements de différents fabricants, tels que les alimentations sans coupure, les batteries, les filtres, les régulateurs, etc., dont chacun peut alimenter tout le système ou une partie, y compris les capteurs et les éléments de commande finaux.
- Il convient que les limites des équipements extérieurs tiennent compte des interfaces requises, des fonctions de communication, des câbles, etc.
- Il convient que les limites de l'environnement tiennent compte de la répartition physique des modules et éléments, qui peuvent être placés dans une salle climatisée, dans un environnement de bureau, dans la zone du processus ou directement sur l'équipement à proprement parler, etc.
- Les limites de l'interface homme-machine sont particulièrement importantes pour évaluer la sûreté de fonctionnement du système, puisque le personnel de conduite et de maintenance joue un rôle important dans l'achèvement de la mission prévue. L'interaction entre les personnes et le système a lieu à plusieurs niveaux de la hiérarchie de commande, dépend fortement du mode de fonctionnement à l'étude et implique tous les modules matériels et logiciels du système.
- Ceci n'est pas évident, mais les tâches à proprement parler sont extérieures aux limites du système. Les influences de l'imposition, de la modification et de l'addition de tâches sont des aspects importants de l'évaluation des propriétés de flexibilité et d'extensibilité d'un système.

Lorsque l'objectif de l'évaluation est «d'obtenir une évaluation comparative de différents systèmes», il peut être impossible de définir les limites exactement de la même manière pour chacun des systèmes à comparer, si ces systèmes ont un domaine d'application fonctionnel différent. Dans ce cas, il convient d'ajouter d'autres équipements, étrangers au système à l'étude, pour pouvoir effectuer la comparaison. Il convient de réaliser une note spécifique sur l'équipement ajouté.

B.2.4 Spécifications du système

L'objet des spécifications du système est de fournir les données numériques, opérationnelles et relationnelles précises de la mise en œuvre du système proposé.

Il convient qu'elles contiennent typiquement:

- une liste complète de tous les modules et éléments;
- les spécifications de produit pour chaque type de module et d'élément, donnant les spécifications générales, fonctionnelles et techniques et les spécifications environnementales;
- des schémas d'interconnexion détaillés identifiant et spécifiant en détail l'interconnexion et l'intercommunication entre les modules et éléments individuels, y compris, le cas échéant les chemins redondants.

B.2.5 Description du fonctionnement du système

L'objectif de la description du fonctionnement du système est d'indiquer de manière systématique la manière dont chaque tâche est exécutée par le système proposé.

Il convient que cette description systématique soit réalisée tâche par tâche et qu'elle contienne:

- une liste des fonctions proposées pour exécuter chaque tâche;
- un commentaire expliquant, pour chaque tâche, la manière dont les modules et éléments proposés exécutent ces fonctions.

Il convient que le niveau de détail nécessaire pour décrire la réalisation des tâches et le découpage en modules et éléments se limite à ce qui est nécessaire et suffisant pour démontrer la satisfaction aux exigences.

B.2.6 Énoncé des justifications de la mise en œuvre du système

Aux fins de l'évaluation, il convient que la définition de la mise en œuvre du système soit soutenue par des énoncés des justifications sous-jacentes.

Il convient que ces énoncés traitent une par une chacune des propriétés (voir 5.2) pertinentes pour la mission du système et donnent des informations supplémentaires relatives aux justifications de la mise en œuvre du système pour l'obtention des propriétés requises du système. Celles-ci peuvent comprendre:

- les raisons des choix de solutions parmi les alternatives possibles;
- les données explicatives (par exemple expérience sur le terrain), les calculs, etc.;
- les rapports d'essai explicatifs.

B.2.7 Déclaration de conformité avec les exigences du système

Des déclarations explicites sont faites pour chacune des exigences du système non atteintes par le système proposé, définissant la nature et l'étendue de la non-conformité.

Annexe C (informative)

Exemples de recueil de documentation

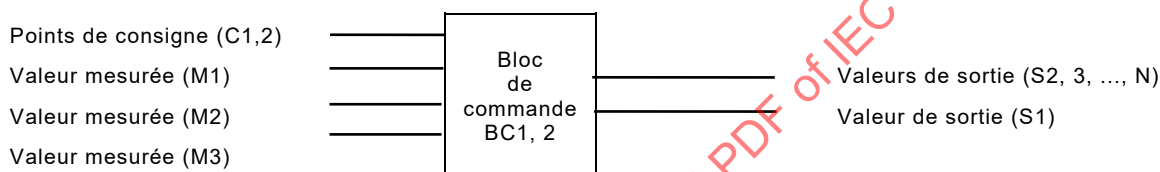
C.1 Vue d'ensemble

L'Annexe C donne des exemples de recueil de documentation.

C.2 Exemple de documentation de commande de chaudière

C.2.1 Schéma de principe de la tâche

La Figure C.1 montre une «commande maître-esclave» pour la documentation de commande d'une chaudière.



IEC

Figure C.1 – Bloc de commande

BC1 et BC2 sont les paramètres de proportionnelle intégrale dérivée (PID) des blocs de commande.

C.2.2 Définition de la tâche

C.2.2.1 Algorithme de commande et/ou de calcul

Commande de la température	: S1	= fonction [M1, C1 et BC1 (paramètres PID)]
	: S2	= fonction [fonction {M2, M3}, C2/S1 et BC2 (paramètres PID)]
Commande du gaz	: S3	= fonction M2, M3 = constante [racine carrée {M2*M3}]
Débit de gaz	: S4	= 1 pour M1 < k degrés Celsius
Alarme en température		

C.2.2.2 Importance pour la mission

La tâche est de première importance pour la mission.

C.2.2.3 Limites du système

Il convient que le système contienne tous les modules et éléments qui permettent d'accomplir la tâche telle qu'elle est décrite. Les actionneurs (vannes de régulation) et les capteurs ne font pas partie du système.

C.2.3 Caractéristiques d'entrée

Valeur mesurée 1 (M1)	:	Mesure	:	température
		Type	:	thermocouple
		Caractéristique	:	type J fer / cuivre-nickel
		Norme	:	IEC 60584-1

	Unités	:	degrés Celsius
Valeur mesurée 2 (M2)	Mesure	:	pression différentielle
	Type	:	4 mA à 20 mA, sécurité intrinsèque
	Alimentation	:	par le système
	Caractéristique	:	linéaire avec la pression différentielle
	Norme	:	
	Unités	:	
Valeur mesurée 3 (M3)	Mesure	:	pression
	Type	:	4 mA à 20 mA, sécurité intrinsèque
	Alimentation	:	par le système
	Caractéristique	:	linéaire avec la pression
	Norme	:	
	Unités	:	bar
Valeur de consigne 1 (C1)	Affichage	:	comme pour M1
	Unités	:	degrés Celsius
Valeur de consigne 2 (C2)	Affichage	:	comme pour S3
	Unités	:	tonnes par heure

C.2.4 Caractéristiques de sortie

Valeur de sortie 1 (S1)	Rôle	:	point de consigne interne du système C2
	Type	:	comme pour S3
	Alimentation	:	
	Caractéristique	:	comme pour S3
	Action	:	inverse
	Unités	:	
Valeur de sortie 2 (S2)	Rôle	:	sortie vers le positionneur de vanne
	Type	:	4 mA à 20 mA, sécurité intrinsèque
	Alimentation	:	par le système
	Caractéristique	:	linéaire
	Action	:	directe, vanne fermée à 4 mA
	Unités	:	linéaire, 0-100 %
Valeur de sortie 3 (S3)	Rôle	:	entrée du BC2, commande du gaz
	Type	:	bloc de calcul interne
	Alimentation	:	par le système
	Caractéristique	:	linéaire
	Action	:	
	Unités	:	linéaire, tonnes par heure
Valeur de sortie 4 (S4)	Rôle	:	sortie vers le panneau d'alarmes
	Type	:	contact libre de potentiel