IEC 61069-3

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 3: Assessment of system functionality

Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 3: Évaluation de la fonctionnalité d'un système

IEC 61069-3:2016-06(en-fr)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

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

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

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

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

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

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

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

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

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

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

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

IEC 61069-3

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 3: Assessment of system functionality

Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 3: Évaluation de la fonctionnalité d'un système

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-3409-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 3: Assessment of system functionality

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 61069-3 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 1996. 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 61069-3:1996 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/791/FDIS	65A/800/RVD

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

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

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

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

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

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

INTRODUCTION

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

Part 1: Terminology and basic concepts

Part 2: Assessment methodology

Part 3: Assessment of system functionality

Part 4: Assessment of system performance

Part 5: Assessment of system dependability

Part 6: Assessment of system operability

Part 7: Assessment of system safety

Part 8: Assessment of other system properties

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

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the specific mission or class of missions.

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

– the identification of the importance of each of the relevant system properties,
– the planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various system properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of a system within practical cost and time constraints.

An assessment can only be carried out if a mission has been stated (or given), or if any mission can be hypothesized. In the absence of a mission, no assessment can be made; however, evaluations can still be specified and carried out for use in assessments performed by others. In such cases, IEC 61069 can be used as a guide for planning an evaluation and it provides methods for performing evaluations, since evaluations are an integral part of assessment.

In preparing the assessment, it can be discovered that the definition of the system is too narrow. For example, a facility with two or more revisions of the control systems sharing resources, for example a network, should consider issues of co-existence and inter-operability. In this case, the system to be investigated should not be limited to the “new” BCS; it should include both. That is, it should change the boundaries of the system to include enough of the other system to address these concerns.

The part structure and the relationship among the parts of IEC 61069 are shown in Figure 1.

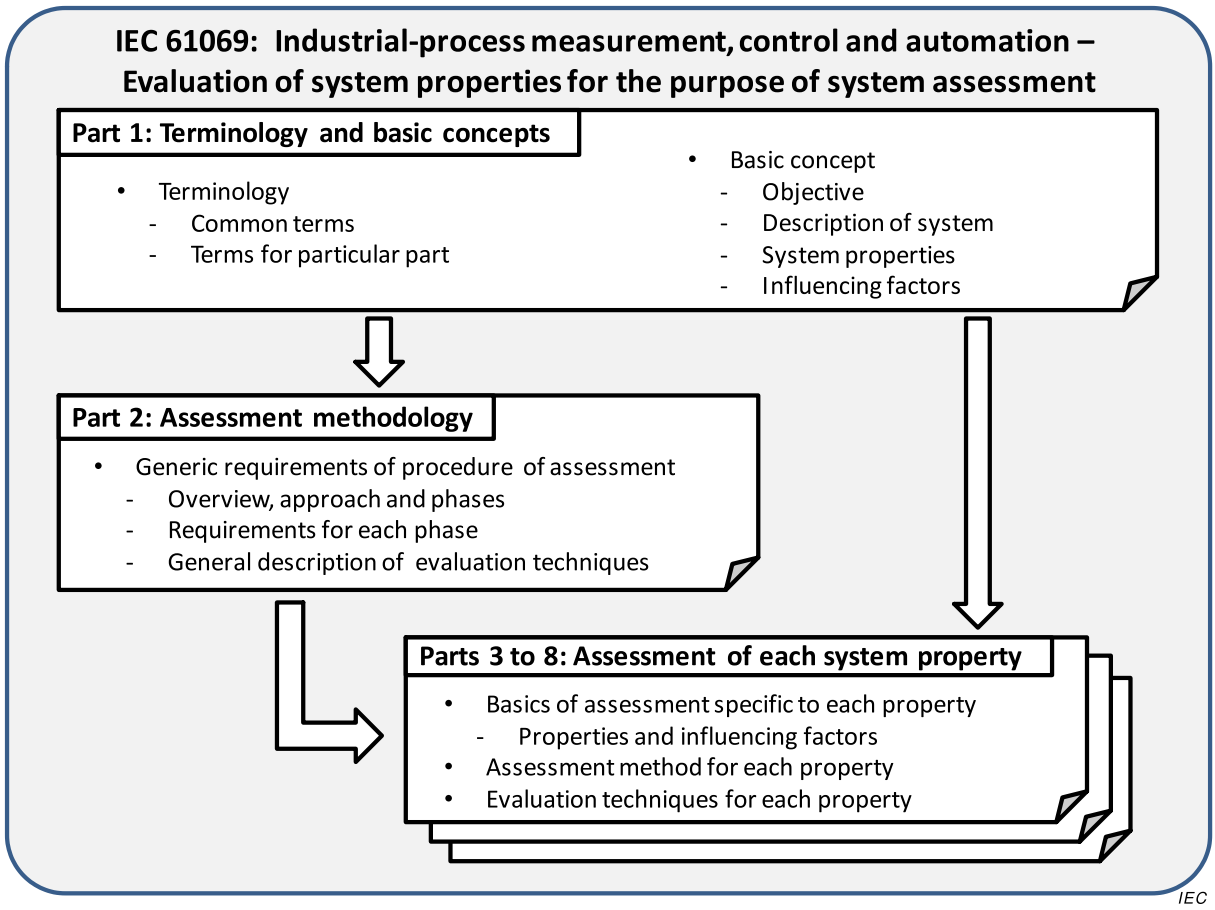


Figure 1 – General layout of IEC 61069

Some example assessment items are integrated in Annex C.

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

Part 3: Assessment of system functionality

1 Scope

This part of IEC 61069:

– specifies the detailed method of the assessment of functionality of a basic control system (BCS) based on the basic concepts of IEC 61069-1 and methodology of IEC 61069-2,

– defines basic categorization of functionality properties,

– describes the factors that influence functionality and which need to be taken into account when evaluating functionality, and

– provides guidance in selecting techniques from a set of options (with references) for evaluating the functionality.

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*

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

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

3.1 Terms and definitions

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

---

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

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

4 Basis of assessment specific to functionality

4.1 Functionality properties

4.1.1 General

A system is able to perform the required mission if the functions provided by the system cover the mission. The extent to which this is the case can be expressed as the system property coverage.

For a system designed for a set of rigid and fixed tasks, coverage can describe fully the functionality of a system.

Tasks required, however, can differ for different applications of the system or the mission can change or be extended over time due to changes in the industrial process or arrangements in the control strategy. To cope with this, the system should provide means for configuring the selection and arrangement of modules, and should have a system configuration which provides flexibility for additions and modifications.

To fully assess the functionality of a system, the system properties are categorised in a hierarchical way.

Functionality properties are categorized as shown in Figure 2.

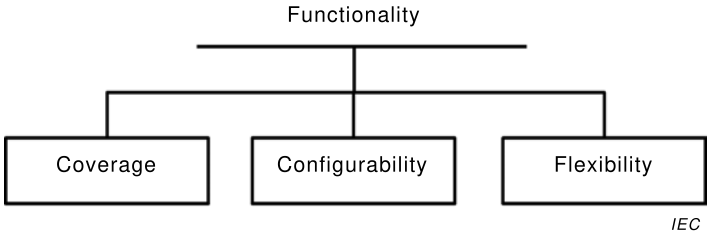


Figure 2 – Functionality

Functionality cannot be assessed directly and cannot be described by a single property. Functionality can only be determined by analysis and testing of each of the functionality properties individually.

Some of the functionality properties can be expressed in quantitative terms as an absolute or relative value; others can only be described in a qualitative way with some quantitative elements.

When assessing the functionality of a system, the availability of facilities necessary for the system to operate should be taken into account.

4.1.2 Coverage

Coverage is determined by:

– the range of distinct functions provided, each differentiated by type, execution frequency, data volume, etc.;

– the variety of ways in which the functions cooperate, as determined by the system configuration, to perform the task(s) required;

– the number of replications available of each function, as determined by the way in which the system modules provide these functions and how these functions are allocated within the modules.

The way in which the individual functions are set up and combined to perform tasks can impose interdependent limits on each function. It can also impose limits on the simultaneous use of separate functions when there is sharing of system resources.

The coverage of the system should be quantified as a coverage factor, which is the ratio of tasks which the system covers against the totality of tasks required by the system mission. If appropriate, partial coverage factors should be expressed for each individual task.

System mission = n Tasks

Coverage factor (CF) = tasks covered / n tasks

4.1.3 Configurability

Configurability is dependent upon the architecture of the system and the ease with which modules can be selected, set up, arranged and combined to assemble function(s) to perform tasks required by the mission of system.

There can be configuration elements at any level of the system. Methods to configure systems are shown in Figure 3. The method can be implemented by hardware or software.

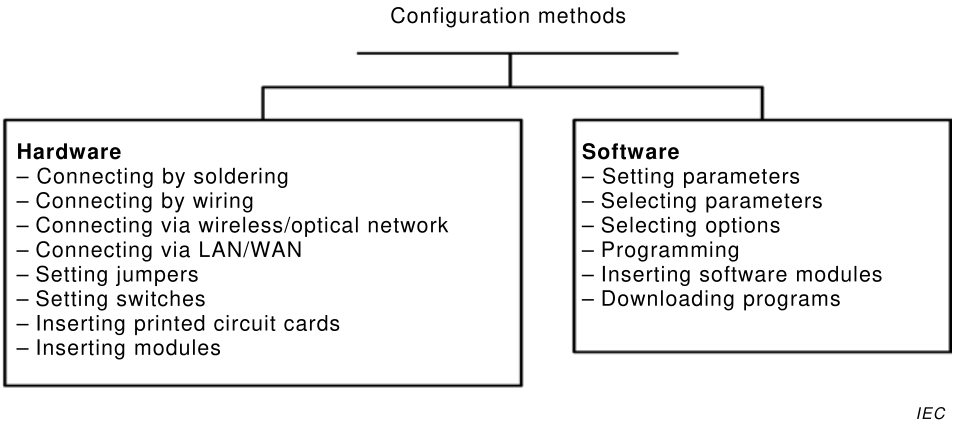


Figure 3 – Configuration methods

It is also important to bear in mind that configuration changes can modify system properties unexpectedly.

The configuration facilities are parts of the system and considered as "supporting functions" if they are fully described in the system specification document.

In practice the activity of configuring a system sometimes requires deep knowledge of system architecture, module behaviour and module interfaces. The need for this knowledge can be reduced by the configuration facilities.

Depending on the mode of operation of the system ("on-line", "off-line", etc.) some of the configuration actions are permissible or not permissible. Some actions (such as module set-up, changes to module connections, module insertion or removal, etc.) are possible only while the system is disabled from process operation. Configurability cannot be quantified as a number. It can be described in a qualitative manner by detailing configuration actions and tools, and stating for each of these the know-how, skills and time required.

4.1.4 Flexibility

4.1.4.1 General

The flexibility of a system depends on the ways the system can be adapted.

The system has higher flexibility when it has more capability to add, remove, change and/or rearrange modules of the system.

Flexibility cannot be expressed by a single system property.

4.1.4.2 Scalability

A system can be designed in such a way that it is possible to scale the system. For example, a system might be able to increase in size (more I/O points) or in communication capabilities (more network interfaces) or supported operator workstations, or in some other countable/measurable way.

The extent to which the system can be scaled can be assessed by analysis of the system configuration, communication functions and shared resources.

Scalability can be expressed by a qualitative description containing some quantified elements.

4.1.4.3 Variability

A system can be designed in such a way that it is possible to vary the range of executable tasks.

Variability can be assessed by analysis of the system configuration, the degree of modularity, the specification of interfaces between the modules, and the number and scope of functions provided by the individual modules.

Variability can be expressed by a qualitative description containing some quantified elements.

4.1.4.4 Enhanceability

A system can be designed in such a way that it is possible to enhance certain system properties.

Enhanceability can be assessed by analysing the system configuration and the range of available modules with alternative property values.

Some examples of implementation which achieve higher enhanceability are:

– modules with a larger main memory to allow a decrease in response time via reduced data transfers;
– modules which allow an increased number of iterations of mathematical procedures to increase the accuracy of a calculated value;
– use of better protected input or output cards against electrical noise to increase the system's security, or to increase the system's usability in areas where there is explosive atmosphere.

The potential for improvement of these properties can extend beyond the requirements stated in the system requirements document.

Enhanceability can be expressed by a qualitative description containing some quantified elements.

4.2 Factors influencing functionality

The functionality of a system can be affected by the influencing factors listed in IEC 61069-1:–, 5.3.

For each of the system functionality properties listed in 4.1, the primary influencing factors are as follows:

a) Coverage can be affected by:

   No influencing factors.

b) Configurability can be affected by:

   1) licensing of specific functionality;

   2) installation, for example all modules and elements are in place.

c) Operational rules, dictated by the mission, training of personnel, and deficiencies in documentation, manuals and technical support can hamper the full use of the system functionality.

5 Assessment method

5.1 General

The assessment shall follow the method as laid down in IEC 61069-2:—, Clause 5.

5.2 Defining the objective of the assessment

Defining the objective of the assessment shall follow the method as laid down in IEC 61069-2:—, 5.2.

5.3 Design and layout of the assessment

Design and layout of the assessment shall follow the method as laid down in IEC 61069-2:—, 5.3.

Defining the scope of assessment shall follow the method laid down in IEC 61069-2:—, 5.3.1.

Collation of documented information shall be conducted in accordance with IEC 61069-2:—, 5.3.3.

The statements compiled in accordance with IEC 61069-2:—, 5.3.3, should include the following in addition to the items listed in IEC 61069-2:–, 5.3.3:

– No additional items are noted.

Documenting collated information shall follow the method in IEC 62069-2:—, 5.3.4.

Selecting assessment items shall follow IEC 61069-2:—, 5.3.5.

Assessment specification should be developed in accordance with IEC 61069-2: —, 5.3.6.

Comparison of the SRD and the SSD shall follow IEC 61069-2:—, 5.3.

NOTE 1 A check list of SRD for system functionality is provided in Annex A.

NOTE 2 A check list of SSD for system functionality is provided in Annex B.

5.4 Planning of the assessment program

Planning the assessment program shall follow the method as laid down in IEC 62069-2:—, 5.4.

Assessment activities shall be developed in accordance with IEC 61069-2:—, 5.4.2.

The final assessment program should specify points specified in IEC 61069-2:—, 5.4.3.

5.5 Execution of the assessment

The execution of the assessment shall be in accordance with IEC 61069-2:—, 5.5.

5.6 Reporting of the assessment

The reporting of the assessment shall be in accordance with IEC 61069-2:—, 5.6.

The report shall include information specified in IEC 61069-2:—, 5.6. Additionally, the assessment report should address the following points:

– information specified in Clause 6.

6 Evaluation techniques

6.1 General

Within IEC 61069-3 several evaluation techniques are suggested. Other methods may be applied, but in all cases the assessment report should provide references to documents describing the techniques used.

Those evaluation techniques are categorized as described in IEC 61069-2:—, Clause 6.

Factors influencing the functionality properties of the system as per 4.2 shall be taken into account.

The techniques given in 6.2, 6.3 and 6.4 are used to assess the functionality properties.

It is not possible to evaluate the functionality property as one entity. Instead each functionality property should be addressed separately.

Functionality which is built in the system but is not specified in the SRD may be omitted from the evaluation, but such omissions shall be recorded in the report.

NOTE An example of a list of assessment items is provided in Annex C.

6.2 Analytical evaluation techniques

6.2.1 Coverage

Coverage can be evaluated by analytically checking whether the number of modules or elements of the system and their scopes specified in the SSD are able to perform the system functions required for the tasks specified in the SRD.

The following information shall be included in the report:

– the tasks and the supporting functions analysed,

– the functions not provided,

– the deficiencies of function found.

6.2.2 Configurability

Configurability can be evaluated by listing the actions to be taken and the time necessary to set up, change or add a system function to perform a task under defined circumstances, for example:

– know-how and skill of personnel involved;
– the tools used, which are provided by the system or specified in the SSD;
– the system modes of operation ("on-line, "off-line", etc.) for which each configuration action is permissible.

6.2.3 Flexibility

Flexibility can be evaluated by analytically:

– listing the maximum number of functional replicas to which the system can be expanded without hampering the correct performance of the functions necessary to perform tasks for the mission;
– listing the number of different functions to which the system can be extended without hampering the correct performance of the functions necessary to perform tasks for the mission;
– listing alternative modules and elements available to the system to enhance the system with different performance, dependability, operability and system safety characteristics, which can be used without hampering the correct performance of the functions necessary to perform tasks for the mission.

6.3 Empirical evaluation techniques

Empirical evaluation shall also be conducted for coverage, compatibility and flexibility.

Empirical evaluation is conducted to verify the result of the analytical evaluation described in 6.2.

6.4 Additional topics for evaluation techniques

No additional items are noted.

Annex A
(informative)

Checklist and/or example of SRD for system functionality

The matrix in Table A.1 provides guidance on the type of information (task by task and/or information translation) which should be given in the SRD for the purpose of performance assessment.

Particular attention should be given to checking that the required configuration facilities and the future requirements for the system have been stated and appropriately quantified, both in relation to individual tasks as well as in relation to the total system mission.

Table A.1 – SRD checklist

Property	Data, drawings, etc.
Coverage	Present and future required tasks supported by: – process control and measurement diagram; – description of the control and measurement requirements in support of each task; – operational and monitoring requirements of each task; – importance of task for mission. Environment including: – a plot plan showing suggested location of measurement and control points, operator's control desk/panel, etc.; – hazardous area classification drawing; – space, location, physical access, expansion constraints.
Configurability	Level of provision required, for example: – fixed; – configurable within constraints (under lock, etc.); – freely programmable. Operational circumstances under which configuration is allowed and/or required.
Flexibility	Expected future expansion of the mission in terms of: – replication of tasks; – new set of tasks, measurements, outputs, etc.; – additional or extended displays or reports. Gradual or "all at once" project realisation. Expected future change in property requirements: – higher dependability; – higher performance (faster, higher accuracy); – better operability (use of touch screen, etc.); – maximum I/O per controller; – task rate; – scan rate.

Annex B
(informative)

Checklist and/or example of SSD for system functionality

B.1 SSD information

The system specification document should be reviewed to check that the properties given in the SRD are listed as described in IEC 61069-2:–, Annex B.

B.2 Check points for system functionality

Particular attention should be paid to check that information is given on:

a) the modules and elements, both hardware and software, supporting each function;
b) quantitative and/or qualitative data on the properties of these modules and elements, and the availability of modules and elements with alternative properties;
c) details of configuration tools, their use and constraints on the system operation;
d) facilities provided by the system which, in the assembled operational system, support analysis of functionality properties. Examples of these facilities are utilities for:
    1) listing all loaded programs, the supporting modules and elements;
    2) calculation of the spare capacity on memories devices, etc.;
    3) statistical analysis of system resource utilisation, etc.;
    4) listing any side-effects on any of the other system properties, which can occur due to changes to the system.

Annex C
(informative)

Example of a list of assessment items (information from IEC TS 62603-1)

C.1 Overview

Annex C provides some examples about assessment items related to this part of IEC 61069 which were extracted from IEC TS 62603-1.

The classifications of the values of properties described in this document are only examples.

C.2 System characteristics

C.2.1 Overview

Clause C.2 of the standard defines the main characteristics that influence the BCS structure and capability in general terms, with a special focus on its integration and scalability.

C.2.2 System scalability

Scalability is the ability of a system and/or an application to grow incrementally larger without total replacement of hardware or software, and without the need to re-engineer the entire architecture of the system.

C.2.3 System expandability

The system expandability is the possibility of the system to be enlarged without changing the architecture and/or the used equipment. The expandability can be both for the entire system and for each apparatus.

The system expandability means that it is possible to add usable components to the system.

For a component, i.e. a programmable logic controller, expandability means that it is possible to add usable spare parts to the components (i.e. free memory or Central Processing Unit (CPU) in a Programmable Logic Controller (PLC)).

C.2.4 Integration of subsystems

The integration of subsystems needs a procedure for combining separately developed modules of components so that they work together as a unique system. A subsystem is a set of components that operates as a part of a system and that is capable of performing a specific task within a system.

Another option is that a subsystem has been provided by other suppliers and manufactures (i.e. third party subsystem).

C.2.5 Automatic documentation

The BCS automatically generates the documentation after the configuration phase. Documents can include:

– system architecture,
– configuration parameters,

– list of material,
– application software,
– wiring table for terminations,
– cables and plugs configuration,
– others.

C.2.6 Programming languages for control

C.2.6.1 General

The control part of the system should support specific programming languages for implementing the control logic. According to the type of functions required for the BCS, a different standard programming language can be used.

Programmable (logic) controller (PLC) is a digitally operating electronic system, designed for use in an industrial environment, that uses a programmable memory for the internal storage of user-oriented instructions for implementing specific functions such as logic, sequencing, timing, counting and arithmetic. A PLC can control, through digital or analog inputs and outputs, counter inputs and pulse outputs, various types of machines or processes. In large scale BCS, the term controller is often used with the same meaning. Both the PLC and its associated peripherals are designed so that they can be easily integrated into an industrial control system and easily used in all their intended functions.

The term PLC-system means a user-built configuration, consisting of a programmable controller and associated peripherals, that is necessary for the intended automated system. It consists of units interconnected by cables or plug-in connections for permanent installation and by cables or other means for portable and transportable peripherals.

C.2.6.2 Programming languages for programmable controllers

IEC 61131-3 defines a set of languages for programming PLCs and controllers. The standard programming languages are divided into two categories:

a) graphical languages:
   1) Ladder: (LL) it is a symbolic representation that schematically illustrates the control functions in the form of electrical circuit diagrams;
   2) Function Block Diagram (FBD): it allows program elements (i.e. PID and other algorithms) to appear as blocks that are connected together as shown in a visual presentation similar to a logic diagram;

b) textual languages:
   1) Instruction List (IL): it is a low level language similar to an assembler in which only one elementary operation, such as storing a value in a register, is allowed per line;
   2) Structured Text (ST): it is a high-level, block-structure language, whose syntax resembles Pascal. ST allows to express complex statements involving variables that represent a wide range of different types of data.

C.2.6.3 Sequential Function Chart (SFC) programming tool

In addition to the programming languages defined in IEC 61131-3, the SFC programming tool allows a graphical representation and structuring of the control software. SFC is a way of graphically representing a complex control program as a sequence of alternating steps and transitions.

C.2.6.4 Continuous Function Chart (CFC) programming tool

Continuous Function Chart (CFC) allows the straightforward conversion of technological specifications into executable automation programs: it works using function blocks that are linked together and configured individually.

The CFC can be intended as a special form of FBD. The main difference between CFC and FBD is that it also shows the resources and task assignments. Each function block shows the name of the task that controls its execution.

The CFC is mainly used to show the top-level structure of the resources and programs.

C.2.6.5 Definition of custom function block

IEC 61131-3 defines a set of standard function blocks common to all the programmable controllers. A function block is a set of elements consisting of:

a) the definition of a data structure partitioned into input, output, and internal variables; and
b) a set of operations to be performed upon the elements of the data structure when an instance of the function block type is invoked.

Examples of standard function blocks are:

– latch;
– edge detection;
– counter;
– timer.

In addition to the standard function blocks it can be useful to define custom function blocks actuating specific functions. Once defined, a custom function block behaves like standard ones.

C.2.6.6 Batch programming tool

The BCS can support the environment for batch control defined in either IEC 61512.

C.2.6.7 Multitasking operating software for controller

Multitasking operating software is a method for managing the resources of the controller CPU in order to allow multiple tasks to share common processing resources. The multitasking facility allows the programmer to make use of the multiprogramming capability of the controller. The term multiprogramming refers to a programming method in which more than one task is in an executable state contemporaneously.

C.2.6.8 Advanced process control (APC)

The APC can be simply defined as the process control strategies beyond straightforward PID control loops. APCs are software tools sold as additional packages that can be either interfaced or installed in the BCS. The APC allows a better control and optimization of the process, and it normally makes use of sophisticated control techniques, such as: expert systems, sliding mode control, multi-variable control, etc.

C.2.7 BCS localisation

Localisation is the ability of a BCS to support local languages for different functions, such as:

– programming;
– documentation;

– human-machine interface (HMI).

The required language(s) and function(s) are to be specified.

C.3 Functionality properties

C.3.1 Input/output specifications

The considered types of input/output are: conventional analog I/O (i.e. 4 mA to 20 mA, 0 V to 10 V, etc.), digital I/O, counters (for example high speed counters), pulse outputs, Hart I/O and fieldbus. For each type of I/O the user should specify the resolution, the accuracy and the repeatability.

C.3.2 Conventional input/output

C.3.2.1 Digital input

The specification of the digital inputs can include:

– the rated input voltage (i.e. 24 V direct current) and current (i.e. 10 mA);
– the input delay (fixed or variable);
– the local status display of the inputs;
– the electrical insulation between inputs and between inputs and backplane;
– the insulation level (i.e. 1 kV direct current).

C.3.2.2 Digital output

The specification of the digital output can include:

– the type of output: static or relay;
– the connected load, i.e. solenoid valves, contactors, lights, etc.;
– the rated output voltage (i.e. 24 V direct current);
– the rated output current (permanent and short time);
– the local display of outputs (i.e. led);
– the electrical insulation between inputs and between inputs and backplane;
– the insulation level (i.e. 1 kV).

C.3.2.3 Analog input

The specification of the analog input can include:

– the type of inputs, i.e. thermo-couple, RTD (2-3-4 wires), 4 mA to 20 mA;
– the reverse polarity protection;
– the electrical insulation between inputs and between inputs and backplane;
– the insulation level (i.e. 500 V direct current).

C.3.2.4 Analog output

The specification of the analog output can include:

– the type of output, i.e. 4 mA to 20 mA, ± 10 V, 0 V to 5 V, etc.;
– the resolution (or the number of conversion bits);
– the electrical insulation between outputs and between outputs and backplane;
– the insulation level (i.e. 500 V direct current);

– the individual output protection with fuse.

C.3.2.5 Counters

These are typically digital and are used for items such as flow meter totalizers.

C.3.2.6 Pulse outputs

These are typically digital and are particularly good for leaving items such as valves in a fixed position on failure of the BCS. Recovery from failure also avoids moving the output to an unexpected position.

C.3.3 Input/output from/to smart devices

It is a common practice to use smart devices in the field. In this case the analog input/output supports the conversion between the protocol used for the smart devices (i.e. Hart) and the protocol used for process control. In addition to the data specified for analog I/Os the user specifies the protocols used.

C.3.4 Fieldbus connection to the remote I/O

The user specifies if a fieldbus connection is used for connecting the remote I/O and the controllers. The fieldbus can be either a standard IEC 61158 fieldbus or a proprietary fieldbus.

C.3.5 Input validation

When a single pole double throw (SPDT) contact is acquired as two digital inputs, validation logic is implemented to detect abnormal statuses. Similarly, the out-of-range of an analogue signal is detected when the signal rises above or drops below the valid range.

C.3.6 Special inputs

Specific requirements for inputs different from the usual ones are to be specified.

C.3.7 Software requirements

C.3.7.1 System database requirements

The system database provides the information needed by various system transactions (functions) to perform their tasks. Input data comes from the field devices (sensors, transmitters, switches, etc.) via the controller's data acquisition interfaces, from supervisory control systems (PC, DCS, PLC), via external controller links, and from other controllers via inter-controller connections. Output data are directed to field control and indication devices, supervisory systems, and other controllers.

The system database is a real-time database, i.e. it needs to provide a predictable response time to guarantee the completion of time-critical transactions.

C.3.7.2 Physical layout of database (implementation)

The system database can have two possible physical layouts:

– distributed database: data are distributed across multiple physical locations. The control of the entire database is under a central database management system (DBMS) that has the role of coordinating all the data files;

– concentrated database: all the data are stored into a central database, i.e. all the records are recorded on an unique machine and can be accessed by the database management system (DBMS).

C.3.7.3 Compatibility with external database

If the system database guarantees the compatibility and the connection with other databases, it is necessary to specify which are the databases that have access or that are accessed by the system database.

C.3.7.4 Type of software

The software for implementing the database can be a commercial product or a proprietary one. If some specific requirement or constraint applies, it is necessary to specify the needed programming language for the database. Normally, this choice is up to the BCS manufacturer.

C.3.8 Alarm management

C.3.8.1 General

The alarm management system of the BCS supports the selection of the events to be considered as alarms, the setting of the alarm priorities, the acknowledgement procedures, etc.

The alarm management should be designed in order to avoid a flood of alarms prompted to the operator interface. The alarm management should be designed by following the following rules:

– simple alarms have to show the location and recommended action;
– access to appropriate screen views should be quick, decisive and with minimum keystrokes;
– handling techniques should be implemented, in particular priority settings and annunciating;
– techniques should be easily reconfigurable.

C.3.8.2 Types of alarms

Different types of alarm can be set or defined. Typical alarm functions include:

– absolute threshold: a given parameter reaches a certain set threshold;
– single delta: an additional alarm notifies that the signal continues to rise. The signal has overcome a certain percentage above the defined threshold;
– repetitive delta: there is an alarm at every selected change beyond that has been selected for the single delta alarm;
– rate of change: there is an alarm if there is a rapid rate of change of the variable even though a threshold has not been passed. The rate of change is normally expressed either in units per second or percent per time;
– return to normal: when required, the operator needs to be notified when a parameter returns to normal, not just when that parameter goes into an alarm;
– time delay: some parameters are relatively unstable, or just continually fluctuate, such as pressures and flows. Often it is useful to set some time delay on those alarms to act as a dead band, so that a spike does not trip an unnecessary alarm;
– “snooze” alarm: the “snooze” alarm re-alarms if the conditions persists beyond some selected time after acknowledging. In some cases, this type of alarm can be set to acknowledge itself if the condition clears;
– hysteresis alarm: a hysteresis alarm has different thresholds in each direction, up or down. Used much like the time delay, this dead band reduces unnecessary alarms in dynamically active fluids.

C.3.8.3 Alarm severity

Any failure or abnormal operation of the BCS should be signalled to the operator with an indication of the alarm severity. Alarm severity indicates the order in which users should handle that event relative to alarms of other severities. Levels of severity can help schedule the maintenance and repair activities, and are an important feature of self-diagnostic messages (system alarms). Severity is not relevant to process alarms.

A possible definition of severity levels is:

– down: no response from the monitored entity or device;
– high (critical): alarm condition that seriously impairs service and requires immediate correction;
– medium (advisory): alarm condition impairing service but not seriously;
– low (journal): alarm condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.

The definition of severity levels is up to the BCS maker as well as their display procedures.

C.3.8.4 Alarm priority level

Alarm priority indicates the urgency of operator response, for example seriousness of consequences and allowable response time. Three levels of priority are defined:

– level 1: immediate operator action. Endangerment of personnel, catastrophic equipment failure/environmental impact, unit shutdown or shutdown of other units imminent;
– level 2: rapid operator action required. Unit shutdown possible. Partial shutdown has occurred. Emergency priority alarm possible;
– level 3: prompt operator action required. High-priority alarm possible. Off-spec or production loss imminent.

User should specify if the BCS alarm management system should support the priority levels.

C.3.8.5 Alarm grouping

Alarms can be organized into groups according to geographical or functional criteria. The purpose of alarm grouping is to allow the operator to quickly recognize patterns in a sequence of alarms and to find-out the areas or machines involved.

C.3.8.6 Alarm acknowledgment

All the alarms should be acknowledged by the operator(s). For each alarm, according to its group, severity and priority, a sequence of actions that indicate that the alarm has been recognized is defined. Different acknowledgment sequences can be implemented.

C.3.8.7 “Smart” alarming/alarm hiding

To reduce the effort for the operator to understand the causes of an abnormal event, alarms that are obvious or redundant shall not be displayed. The BCS supports “smart” alarming whereby pre-defined alarms can be automatically hidden to the operator on the occurrence of specific process or plant conditions.

The system should provide tools and capability for easy configuration of which alarms will be “hidden” based on plant state or process condition.

Hidden alarms are not presented to the operator on the standard alarm displays or on process graphics, but their occurrence is recorded in the alarm history. A “hidden alarm” display will be provided which lists all of the alarms that are currently hidden from the operator.

C.3.8.8 Alarm annunciation

Alarm annunciation is the capacity of the system to notify the alarms to the operators. The annunciation process can include, for example:

– activation of an external audible alarm or lights;
– activation of the internal PC audio card (e.g. to play .wav files);
– updating an alarm display with the current alarm;
– updating an alarm overview screen to indicate the occurrence of an alarm in a specific process area / display;
– printing the alarm message on an alarm printer;
– any graphic object associated with the alarm point will change colour, shape, appear, disappear, etc. as configured.

C.3.8.9 Alarm summary display lists

A summary of the alarms could be useful, and it can include:

– active process alarms
– cleared process alarms
– acknowledged process alarms
– active system alarms
– cleared system alarms
– acknowledged system alarms
– alarm history
– operator action list
– suppressed (locked) alarm list
– hidden alarm list
– alarm frequency display (hit) list

Accessing an alarm summary display from any other display shall require the minimum number of operator actions.

Multi-page displays may be used. If so, it shall be possible to page forward or backward. The display shall list alarms in tabular format in order of occurrence.

C.3.9 Events management

C.3.9.1 General

An event is a change of the status of any variable in the process. Typical events are:

– change of status of digital inputs,
– reaching a threshold for analog variables,
– commands from operator, etc.

An event can start or alter a control action.

C.3.9.2 Sequence of events (SOE)

Time resolution is the minimum time by which two events should be separated in order that the corresponding time tags are different. Separating capability is the minimum time by which two events should be separated such that the sequence of their occurrence is determined

correctly. Time resolution cannot be shorter than the separating capability, and it is normally specified.

C.3.9.3 Integration of SOE with third parties systems

If the data processed by the SOE can be accessed by other applications and/or systems, it is necessary to specify them and whether some particular driver or communication interface is required (i.e. OPC alarm and event).

C.3.9.4 Types of events

The types of events are classified according to their sources:

– operator: operator changes such as set points changes, control output changes or controller mode changes. Reactions to alarms, such as acknowledgments;
– alarm: each alarm presents always two events: switching into alarm condition and switching out of alarm condition (sometimes the latter might or might not prompt a reset);
– process: the events are related to the state of the monitored system, such as protecting events, quality changes in the measures, etc.

C.3.10 Historical archiving

C.3.10.1 General

Events can be archived in the historical database, which means recording in a centralised machine a particular signal from the controller where the event was either generated or acquired from a sensor. Only some events should be archived in the historical database. Subclauses C.3.10.2 and C.3.10.3 report the methods for archiving and the specifications to define data that should be archived.

C.3.10.2 Archiving method

The historical database can store events according to different methods:

– cyclically: there is a fixed collection frequency that is used to sample the data;
– on variation: on/off data are stored only when they change their status; analog data are stored when their value changes more than a given threshold;
– on event: data are collected on the basis of a triggering event or interrupt.

The number of events to archive should be defined.

C.3.10.3 Back-up of the archives

The historical database is a critical part of the entire BCS and for such a reason a back-up media should be chosen. The back-up archives are important to restore the data after a disaster or after the corruption of some data.

In order to select the best back-up archive for the historical database, the following features should be defined:

– hardware type of back-up depository;
– expected life span of the back-up;
– need for a software back-up tool that guides the process of intelligent back-up;
– frequency of the back-up (daily, weekly, monthly, etc.);
– format required for the stored data.

C.3.11 Trend and statistics management

C.3.11.1 General

For process or plant supervision and control, HMI should show both instantaneous and recorded values in different format according to process requirements.

C.3.11.2 Features of the trend

The main features defining the trending application are:

– number of traces available per screen/window;
– type of variables to trend;
– minimum/maximum sampling rate;
– the span time or the total capacity of data displayed on the same trend.

C.3.11.3 Analog values trending

The trend of analog value can include the following features:

– current value;
– average;
– minimum;
– maximum;
– standard deviation.

C.3.11.4 Discrete value trending

The trend of discrete value can include the following features:

– current state;
– start state;
– transition count;
– statistics.

C.3.11.5 Trend navigation requirements

The trend system should have some requirements for a comfortable navigation, such as:

– panning: moving “back and forth” along the same time divisions within a much longer trend than fits in a single screen;
– zoom: moving to different time divisions.

In addition to the function of panning and zooming the cursor may have additional functions, such as:

– time/date of placement;
– value/state of intersected traces;
– tags and titles of all traces viewed;
– select area of zoom for more detail.

C.3.12 Communication requirements

Communication plays a key role in a BCS. Different communication networks co-exist in a BCS, each one with specific features and requirements. Usually communication networks may be divided into three or four levels according to the technology used. Figure C.1 schematically shows these alternatives.

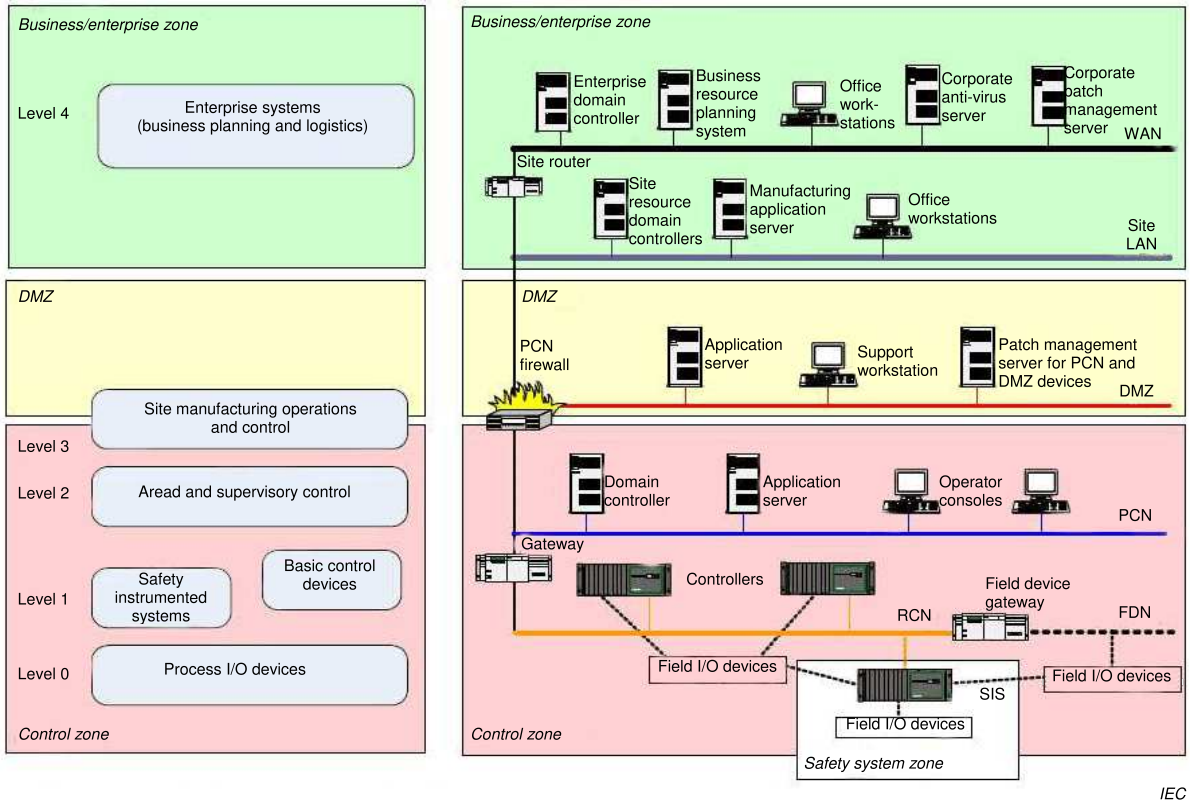


Figure C.1 – Communication networks in a BCS

C.3.13 Fieldbus

According to the IEC 61158, the principal requirements for fieldbuses that should be specified are:

– the physical layer: copper, fiber optic or wireless,
– communication profile (CPF) according to IEC 61784,
– number of devices connected to the network,
– installation in hazardous areas,
– redundancy of the communication medium required,
– maximum distance between the field device and the controller.

C.3.14 Controller network

The requirements for the controller network that should be specified are:

– the type of protocol used,
– the physical layer,
– installation in hazardous areas,
– redundancy of the communication medium required,
– maximum distance of the connection.

C.3.15 Control room network

The requirements for the control room network that should be specified are:

– the type of protocol used,

– the physical layer,
– redundancy of the communication medium required,
– maximum distance of the connection.

C.3.16 External link

The external link allows to put in communication different networks, for example the control room network and the corporate network (refer to Figure C.1).

The user should specify:

– the networks that need the communication link,
– the security level needed,
– the need for a firewall,
– the need for an antivirus.

C.3.17 Communication interfaces

Several communication networks can exist within a BCS, thus it is necessary to define the interfaces between the networks and between different systems.

The user should specify:

– the communication protocol between the networks that exchange data and information;
– the quantity of data exchanged;
– the refresh time required for using valid data;
– the physical medium of connected networks;
– the desired security level.

A communication interface allows to share and pass data and information between different communication systems that use different physical medium and/or different data structure. In this way the data can be moved across the entire BCS communication system and they can be used where they are needed.

C.3.18 Communication with ERP system

Enterprise resource planning (ERP) integrates internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, etc. ERP systems automate this activity with an integrated software application. Its purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders.

The ERP needs to communicate and exchange data with the control system, where the productivity data are generated. ERP systems connect to real-time data and transaction data in a variety of ways:

– direct integration: ERP systems connectivity (communications to control system) as part of their product offered by vendors. This requires the vendors to offer specific support for the control system that their customers operate;
– database integration: ERP systems connect to control system through staging tables in a database. Control systems deposit the necessary information into the database. The ERP system reads the information in the table,
– enterprise appliance transaction modules (EATM): These devices communicate directly with the control system and with the ERP system via methods supported by the ERP

system. EATM can employ a staging table, web services, or system-specific program interfaces (APIs);

– standard protocols: Communication drivers are available for control system and separate products have the ability to log data to staging tables. Standards exist within the industry to support interoperability between software products, the most widely known being OPC,

– security needs shall be reviewed and considered for this ERP system particularly considering that breaches of security may originate in the office (i.e. non-control) part of the network.

C.3.19 Communication with a manufacturing execution system (MES)

An MES is a production scheduling and tracking system used to analyze and report resource availability and status, schedule and update orders, collect detailed execution data such as material usage, labour usage, process parameters, order and equipment status, and other critical information. It accesses bills of material, routing and other data from the base ERP system and is typically the system used for real-time shop floor reporting and monitoring that feeds activity data back to the base system.

The methods for connecting with the MES are:

– direct integration: MES systems connectivity (communications to control system) as part of their product offered by vendors. This requires the vendors to offer specific support for the control system that their customers operate;

– database integration: MES systems connect to the control system through staging tables in a database. Control systems deposit the necessary information into the database. The MES system reads the information in the table;

– standard protocols: Communications drivers are available for control system and separate products have the ability to log data to staging tables. Standards exist within the industry to support interoperability between software products, the most widely known being OPC;

– security needs shall be reviewed and considered for this MES system particularly considering that breaches of security may originate in the office (i.e. non-control) part of the network.

C.3.20 Software simulator

A software simulator is a program that allows the user to observe an operation through simulation without actually running the program.

The simulation software allows testing the system behaviour after a modification or a new configuration without the need of having the real hardware connected. The simulation software allows a better debugging performance in a simulation environment before the downloading of the program or the configuration on the real system.

C.3.21 Simulator of the control logic

The implemented control logic can be tested on the configuration PC or workstation. The simulator allows to test the logic without having the hardware connected. The simulation is useful for checking the overall consistency of the control logic program and the effect of modifications.

C.3.22 On-line debugging

On-line debugging allows checking and correcting a program during its execution even if other programs are running simultaneously. Debug allows detecting and correcting any program faults.

C.3.23 Simulator of the I/O

The I/O simulator allows the simulation of the operation of the I/Os. In this case, it is possible to force the values of the I/Os in order to check a specific logic or control loops.

C.3.24 Remote supervisory functions

A remote computer with the proper trustee rights can supervise the BCS. Remote supervision extends to displays, tags or variables, control-loop setting, alarm acquisition, etc. The user can specify the functions the remote supervision can carry on.

C.3.25 Technology and scope of the BCS

According to today's terminology, the available technologies for BCSs can be selected amongst:

– PLC based;
– soft PLC based;
– DCS;
– SCADA;
– others (to be specified).

The basic function or functions of the required BCS are selected amongst one or more of the following choices:

– supervisory;
– control;
– ESD;
– batch;
– others (to be specified).

C.3.26 Basic architecture

The BCS topology is normally shown in a drawing attached to the technical specification, where all the main components are indicated and named. In case of complex systems, the drawing can be split into several sheets: outline, subsystems, control room layout, etc. Figure C.2 shows an example of a layout for a medium-size BCS.

This standard defines the requirements of the components of the BCS, from field devices to the control room, and the requirements of the interfaces for connecting the BCS to other digital and communication systems of the factory, for example ICT, not within the scope of this standard.

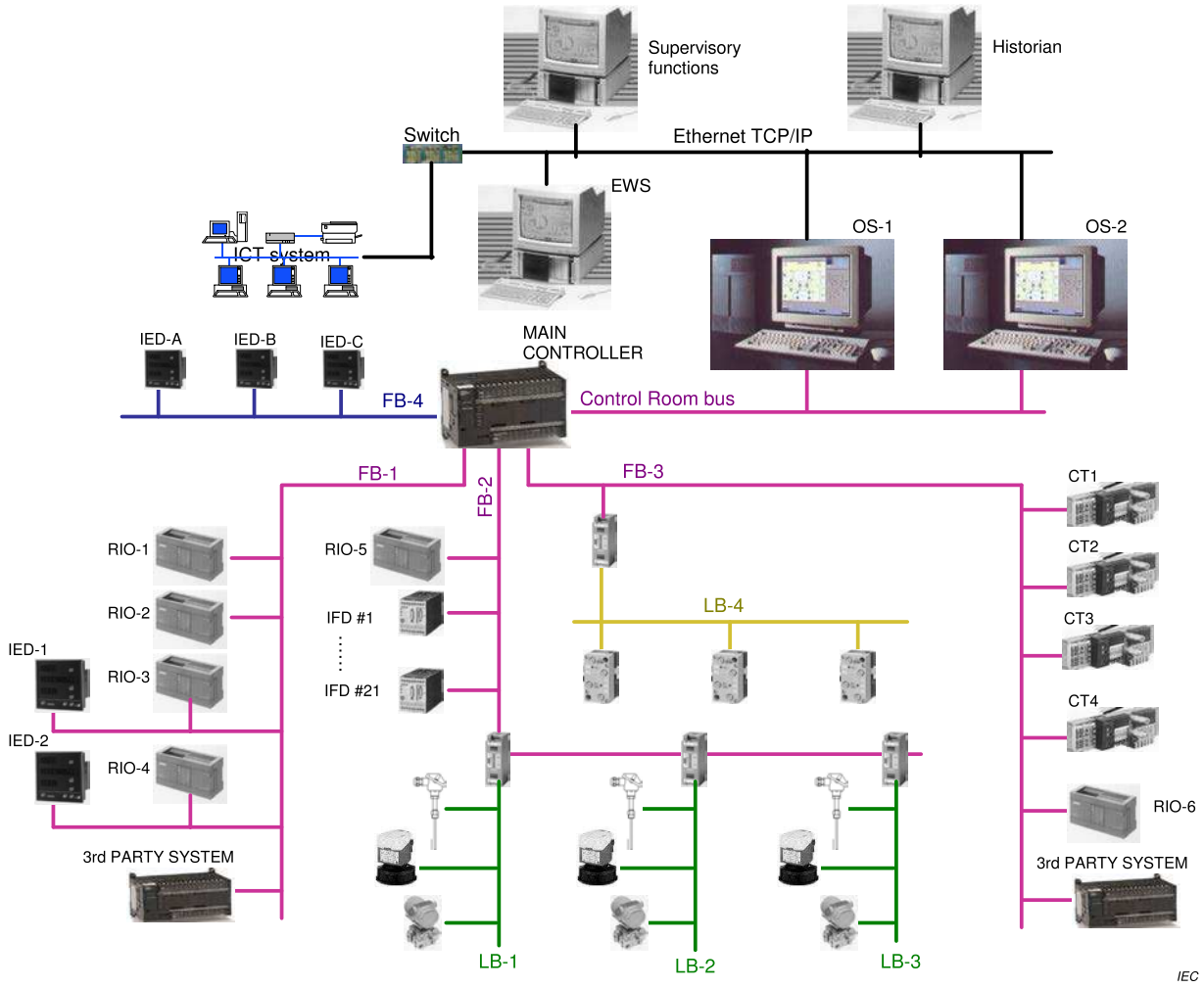


Figure C.2 – Example of a layout drawing

C.4 Configurability

C.4.1 System configuration

The system configuration is the construction of a control system by selecting functional or modular units out of a given set and by defining their interconnections. Configurability of the system defines the extent to which the system facilitates the selection, set-up and arrangement of its modules to perform its mission.

The configuration can be both hardware and software.

The main functionalities for the software configuration of the system are:

– definition of the system architecture by means of the configuration tool;
– inserting software modules;
– selecting and setting parameters;
– selecting options;
– programming;
– compiling and downloading programmes;
– basic engineering.

Some of the software configuration actions might be permissible also if the system is running. Some configuration tools allow the configuration of the entire system even if there is no hardware connected (emulated mode).

The basic functionalities for the hardware configuration of a BCS are:

– inserting modules;
– mounting devices;
– connection by soldering and/or by wiring;
– setting jumpers;
– setting switches;
– inserting printed circuit boards.

Normally, for performing the hardware configuration it is necessary that the system is disabled from process operation.

C.4.2 On-line configuration

If the system supports on-line configuration, then it is possible to run the system configuration procedure while the BCS is running with no loss of functionalities. On-line configuration can have different levels:

– both hardware and software full re-configuration is possible,
– only minor hardware changes are allowed,
– only minor software changes are possible.

On-line configuration is often related to the redundancy policy of the BCS.

C.4.3 Off-line configuration

Off-line configuration means that for setting up the functional parameters of the BCS it is necessary to switch the BCS into off-line, to load the changes, and then to switch the system on-line again, after the validation of the parameter changes.

C.4.4 Configuration in simulation mode

Configuration in simulation mode means that before loading any configuration change in the BCS it is possible to run a simulation of the system with the new parameters for a preventive evaluation of the effect of changes.

C.4.5 Graphical resources

Graphical resources are software tools that support the engineering and the configuration phases. The BCS architecture is drawn starting from a library of devices (click-and-drag) with a graphic tool for defining data exchange and component interconnection. It is also possible to input parameters and functions with graphic procedures (pop-up menus, forms, etc.).

C.5 Flexibility

C.5.1 Spare capacity of the system

C.5.1.1 General

After the final configuration of the system, The BCS should have a spare capacity in order to allow adding functionalities or upgrade the system over time. The spare capacity is installed and available with only the standard configuration.

The desired or needed spare capacity of the system should be specified in the design of the system for the different sub-systems (memory, I/O, terminations, etc.).

C.5.1.2 Spare memory

The spare memory gives the possibility to expand and change the control software in the future. The spare memory is expressed as a percentage of the total available memory installed, and strictly depends on the implemented software applications.

The user should indicate the spare memory needed after the final configuration of the system.

C.5.1.3 Expandability of control room communications

The expandability of communications defines the possibility of adding new communication ports and devices to the control network. The added communication ports can be configured without modifications in the existing software and with no need of re-configuring the entire communication network.

C.5.1.4 Expandability of field communications

Expandability of field communications defines the possibility of adding new communication ports and devices to the field network. The added communication ports can be configured without modifications in the existing software and with no need of re-configuring the entire communication network.

C.5.1.5 Field device expandability

Field device expandability is the possibility of adding new field devices to the existing communication fieldbus(es) or the possibility of adding new field devices to the I/O cards. The maximum number of field devices that can be added to the BCS without any hardware intervention should be indicated, and as a percentage of the existing devices.

C.5.1.6 Available room for BCS expansion

The amount of room that should remain available after the completion of the BCS should be specified. Available room is indicated as a percentage of used space:

– inside the control cubicle, for adding new devices inside,
– in the cabinet room, for adding new control cabinets.

C.5.2 Total number of I/O

The total number of estimated I/O defines the overall size of the BCS. Physical I/O are divided into the conventional analog/digital input/output. If a fieldbus technology is required, the total number of intelligent devices and/or remote input/output devices connected to the BCS is indicated as well.

C.5.3 Number of tags

A tag indicates an elementary piece of information used or produced by the BCS. Tags are often grouped into process objects (transmitters, valves, circuit breakers, etc.) and divided into two categories:

– tags for process control: a limited set of information or commands necessary for process control. For example, the process object “valve” may include the following tags: valve position, open/close status, set-point;
– tags for additional functions, such as device remote setting, diagnostic, alarm setting, etc. These functions are possible only with intelligent devices connected through a fieldbus, and the relevant number of tags may become very high.

C.5.4 Number of control loops

A control loop is based on the use of a software controller with PID functions or similar. The total number of loops gives an idea of the complexity of the system, mainly in terms of software performances. The system should be able to handle the total amount of control loops with the specified time requirements. Advanced controls of special control functions are not to be considered at this point.

C.5.5 System scalability

Scalability is the ability of a system and/or an application to grow incrementally larger without total replacement of hardware or software, and without the need to re-engineer the entire architecture of the system.

C.5.6 System expandability

The system expandability is the possibility of the system to be enlarged without changing the architecture and/or the used equipment. The expandability can be both for the entire system and for each apparatus.

The system expandability means that it is possible to add usable components to the system.

For a component, i.e. a programmable logic controller, expandability means that it is possible to add usable spare part to the component (i.e. the free memory or CPU in a PLC).

Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at http://www.electropedia.org)

[2] IEC 61069-5[3], *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability*

[3] IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

[4] IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

[5] IEC 61297, *Industrial-process control systems – Classification of adaptive controllers for the purpose of evaluation*

[6] IEC 61512 (all parts), *Batch control*

[7] IEC 61784 (all parts), *Industrial communication networks – Profiles*

[8] Dutch Standard Institute NPR 5269, *Industrial-process measurement and control. Basic documentation set for process control installations*

[9] IEC TS 62603-1:2014, *Industrial process control systems – Guideline for evaluating process control systems – Part 1: Specifications*

_____

[3] Second edition to be published simultaneously with this part of IEC 61069.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 3: Évaluation de la fonctionnalité d'un système

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, 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 61069-3 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 1996. 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 61069-3 :1996 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/791/FDIS	65A/800/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, l'IEC 61069 peut être utilisée en tant que guide pour planifier une appréciation et ses méthodes peuvent servir à effectuer les appréciations; l'appréciation des propriétés d'un système fait, en effet, partie intégrante de l'évaluation de ce système.

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

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

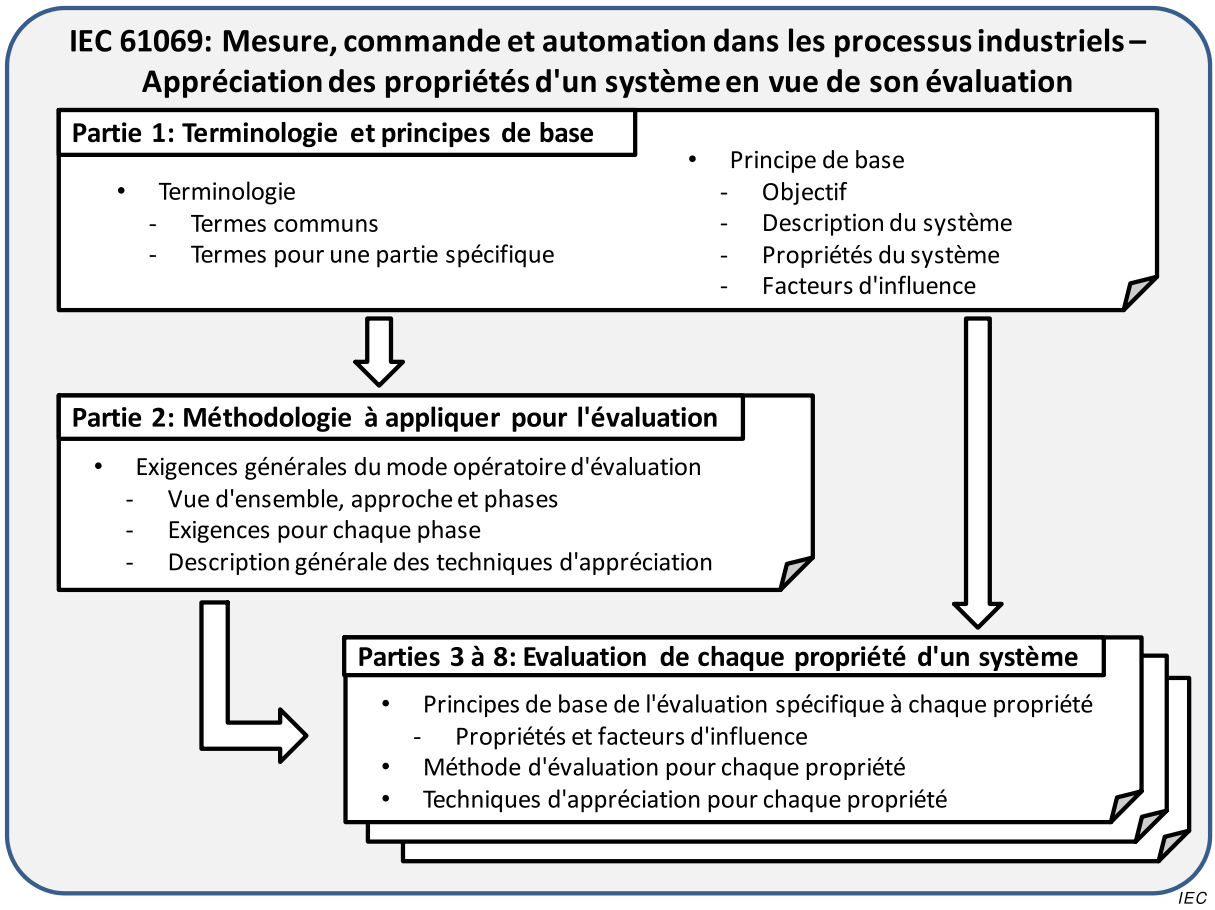


Figure 1 – Structure générale de l'IEC 61069

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

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

Partie 3: Évaluation de la fonctionnalité d'un système

1 Domaine d'application

La présente partie de l'IEC 61069:

– spécifie la méthode d'évaluation détaillée de la fonctionnalité d'un système de commande de base (BCS) reposant sur les principes de base de l'IEC 61069-1 et la méthodologie de l'IEC 61069-2;

– définit la classification de base des propriétés de la fonctionnalité;

– décrit les facteurs ayant une influence sur la fonctionnalité et qui doivent être pris en compte lors de l'appréciation de la fonctionnalité;

– donne des lignes directrices concernant les techniques de sélection à partir d'un ensemble d'options (avec références) pour l'appréciation de la fonctionnalité.

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*

IEC 61069-2:— [2], *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*

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.

---

1 Deuxième édition à paraître simultanément avec la présente partie de l'IEC 61069.

2 Deuxième édition à paraître simultanément avec la présente partie de l'IEC 61069.

4 Principes de base de l'évaluation spécifique à la fonctionnalité

4.1 Propriétés de fonctionnalité

4.1.1 Généralités

Un système est en mesure d'exécuter la mission requise si les fonctions qu'il fournit couvrent cette mission. La mesure dans laquelle ce point est vérifié peut s'exprimer par la propriété de couverture du système.

Dans le cas d'un système conçu pour un ensemble de tâches invariables et figées, la couverture peut entièrement décrire la fonctionnalité du système.

Les tâches requises peuvent toutefois varier pour différentes applications du système ou la mission peut changer ou évoluer au cours du temps en raison de changements dans le processus industriel ou de modifications de la stratégie de commande. Pour y faire face, il convient que le système fournisse des moyens permettant de configurer la sélection ou l'agencement de modules, et qu'il possède une configuration de système assurant une certaine flexibilité pour accepter des additions et modifications.

Pour évaluer totalement la fonctionnalité d'un système, les propriétés du système sont classées de façon hiérarchique.

Les propriétés de fonctionnalité sont classifiées comme indiqué à la Figure 2.

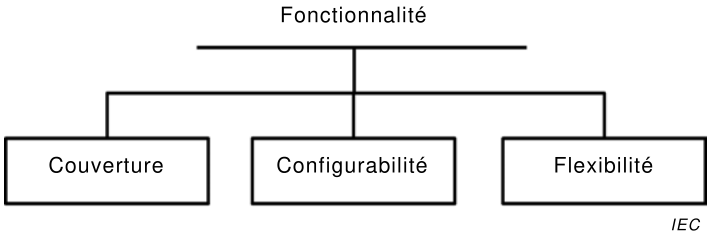


Figure 2 – Fonctionnalité

La fonctionnalité ne peut pas être évaluée directement et ne peut pas être décrite par une seule propriété. La fonctionnalité ne peut être déterminée que par des activités individuelles d'analyse et d'essai de chacune de ses propriétés de fonctionnalité.

Certaines des propriétés de fonctionnalité peuvent être exprimées en termes quantitatifs par une valeur absolue ou relative, d'autres ne peuvent être décrites que de manière qualitative avec quelques éléments quantitatifs.

Lors de l'évaluation de la fonctionnalité d'un système, il convient de prendre en compte la disponibilité des moyens nécessaires au fonctionnement du système.

4.1.2 Couverture

La couverture est déterminée par:

– la gamme des différentes fonctions fournies, en distinguant chacune par son type, sa fréquence d'exécution, son volume de données, etc.;
– la diversité des manières dont les fonctions coopèrent, telles que définies par la configuration du système, pour exécuter la ou les tâches requises;
– le nombre de répliques disponibles de chaque fonction, tel que défini par la manière dont les modules du système fournissent ces fonctions et par la manière dont ces fonctions sont allouées à l'intérieur des modules.

La manière dont les fonctions individuelles sont configurées et associées pour exécuter les tâches peut imposer à chaque fonction des limites interdépendantes. Cela peut également imposer des limites à l'utilisation simultanée de fonctions distinctes lorsque les ressources du système sont partagées.

Il convient de quantifier la couverture du système par un facteur de couverture, qui représente le pourcentage de tâches couvertes par le système par rapport à la totalité des tâches requises par la mission du système. Le cas échéant, il convient de présenter des facteurs de couverture partielle se rapportant à chaque tâche prise individuellement.

Mission du système = n tâches

Facteur de couverture (CF) = tâches couvertes / n tâches

4.1.3 Configurabilité

La configurabilité dépend de l'architecture du système ainsi que de la facilité avec laquelle les modules peuvent être sélectionnés, configurés, agencés et associés pour assembler une ou plusieurs fonctions afin d'exécuter les tâches requises par la mission du système.

Des éléments de configuration peuvent exister à tout niveau du système. La Figure 3 indique des méthodes pour configurer les systèmes. La méthode peut être mise en œuvre par un matériel ou un logiciel.

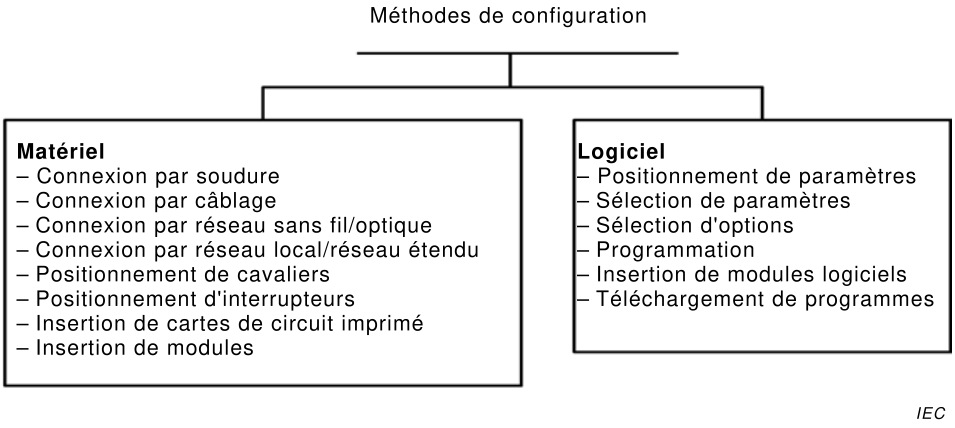


Figure 3 – Méthodes de configuration

Il est également important de garder à l'esprit que les changements de configuration peuvent modifier de manière inattendue les propriétés du système.

Les moyens de configuration font partie du système et sont considérés comme des «fonctions de support» s'ils sont entièrement décrits dans le cahier des spécifications du système.

Dans la pratique, l'activité de configuration d'un système nécessite parfois une connaissance approfondie de l'architecture du système, du comportement des modules et de leurs interfaces. Les moyens de configuration peuvent réduire le besoin d'une telle connaissance.

Suivant le mode de fonctionnement du système («en ligne», «hors ligne», etc.), certaines actions de configuration peuvent ou non être autorisées. Certaines actions (telles que la configuration de module, le changement de connexions d'un module, l'insertion ou le retrait de module, etc.) ne sont possibles que lorsque le système n'a plus d'action sur le processus. La configurabilité ne peut pas être quantifiée par un nombre. Elle peut être décrite de manière qualitative en détaillant les actions et les outils de configuration et en indiquant, pour chacun d'eux, le savoir-faire, les compétences et le temps nécessaires.

4.1.4 Flexibilité

4.1.4.1 Généralités

La flexibilité d'un système dépend des manières dont le système peut être adapté.

La flexibilité du système est d'autant plus grande que le système offre plus de capacité à ajouter, retirer, modifier et/ou réagencer les modules de ce système.

La flexibilité ne peut pas être exprimée par une propriété unique du système.

4.1.4.2 Possibilités de modulation de taille

Un système peut être conçu de telle sorte qu'il soit possible de moduler sa taille. Par exemple, un système peut permettre un accroissement de sa taille (davantage de points d'E/S) ou de ses capacités de communication (davantage d'interfaces de réseau) ou encore du nombre de postes de travail opérateur pris en charge, ou de toute autre manière comptable/mesurable.

La mesure dans laquelle la taille du système peut être modulée peut être évaluée par une analyse de la configuration du système, des fonctions de communication et des ressources partagées.

Les possibilités de modulation de taille peuvent être exprimées par une description qualitative contenant certains éléments quantifiés.

4.1.4.3 Possibilités de diversification des tâches

Un système peut être conçu de telle sorte qu'il soit possible de diversifier la gamme des tâches exécutables.

Les possibilités de diversification des tâches peuvent être évaluées par une analyse de la configuration du système, du degré de modularité, de la spécification des interfaces entre les modules ainsi que du nombre et du domaine d'application des fonctions fournies par les modules individuels.

Les possibilités de diversification des tâches peuvent être exprimées par une description qualitative contenant certains éléments quantifiés.

4.1.4.4 Possibilités d'amélioration des propriétés

Un système peut être conçu de telle sorte qu'il soit possible d'améliorer certaines de ses propriétés.

Les possibilités d'amélioration des propriétés peuvent être évaluées par une analyse de la configuration du système et de la gamme des modules disponibles en conférant des valeurs différentes à une propriété.

Les exemples de mise en œuvre offrant les possibilités les plus importantes d'amélioration des propriétés incluent:

– les modules ayant une mémoire principale plus importante pour permettre une diminution du temps de réponse du fait d'une réduction des transferts de données;
– les modules autorisant un nombre plus important d’itérations de modes opératoires mathématiques pour améliorer la précision d'une valeur calculée;
– l'utilisation de cartes d'entrée ou de sortie mieux protégées contre les perturbations électriques pour accroître la sécurité du système, ou pour accroître les possibilités d'utilisation du système dans des zones situées dans une atmosphère explosive.

Les potentialités d'amélioration de ces propriétés peuvent s'étendre au-delà des exigences formulées dans le cahier des charges du système.

Les possibilités d'amélioration des propriétés peuvent être exprimées par une description qualitative contenant certains éléments quantifiés.

4.2 Facteurs influençant la fonctionnalité

La fonctionnalité d'un système peut être affectée par les facteurs d'influence énumérés en 5.3 de l'IEC 61069-1.

Pour chaque propriété de fonctionnalité d'un système énumérée en 4.1, les facteurs d'influence principaux sont les suivants:

a) La couverture peut être affectée par:

   pas de facteurs d'influence.

b) La configurabilité peut être affectée par:

   1) la licence d'une fonctionnalité spécifique;

   2) l'installation, par exemple tous les modules et les éléments sont en place.

c) Les règles opérationnelles dictées par la mission, la formation du personnel et certaines déficiences de documentation, des manuels et du support technique peuvent gêner l'utilisation complète de la fonctionnalité du système.

5 Méthode d'évaluation

5.1 Généralités

L'évaluation doit être effectuée selon la méthode décrite à l'Article 5 de l'IEC 61069-2:—.

5.2 Définition de l'objectif de l'évaluation

La définition de l'objectif de l'évaluation doit être effectuée selon la méthode décrite en 5.2 de l'IEC 61069-2:—.

5.3 Conception et agencement de l'évaluation

La conception et l'agencement de l'évaluation doivent être effectués selon la méthode décrite en 5.3 de l'IEC 61069-2:—.

La définition du domaine d'application de l'évaluation doit être effectuée selon la méthode décrite en 5.3.1 de l'IEC 61069-2:—.

Le classement des informations détaillées doit être effectué conformément à ce qui est spécifié en 5.3.3 de l'IEC 61069-2:—.

Il convient que les rapports établis conformément à ce qui est spécifié en en 5.3.3 de l'IEC 61069-2:— incluent les éléments suivants en plus de ceux énumérés en 5.3.3 de l'IEC 61069-2:—:

– Aucun élément supplémentaire n'est indiqué.

La mise en forme des informations recueillies doit être effectuée selon la méthode décrite en 5.3.3 de l'IEC 62069-2:—.

La sélection des éléments d'évaluation doit être effectuée selon la méthode indiquée en 5.3.4 de l'IEC 61069-2:—.

Il convient que les spécifications de l'évaluation soient développées conformément à ce qui est spécifié en 5.3.5 de l'IEC 61069-2:—:

La comparaison du cahier des charges du système (CdC) et du cahier des spécifications du système (CdS) doit être effectuée selon la méthode indiquée en 5.3 de l'IEC 61069-2:—.

NOTE 1 Une liste de contrôle du CdC destiné à la fonctionnalité d'un système est fournie en Annexe A.

NOTE 2 Une liste de contrôle du CdS destiné à la fonctionnalité d'un système est fournie en Annexe B.

5.4 Planification du programme d'évaluation

La définition de l'objectif de l'évaluation doit être effectuée selon la méthode décrite en 5.4 de l'IEC 62069-2:—.

Les activités d'évaluation doivent être développées conformément à ce qui est spécifié en 5.4.2 de l'IEC 61069-2:—.

Il convient que le programme définitif d'évaluation précise les points spécifiés en 5.4.3 de l'IEC 61069-2:—.

5.5 Exécution de l'évaluation

L'exécution de l'évaluation doit être conforme à ce qui est spécifié en 5.5 de l'IEC 61069-2:—.

5.6 Rédaction du rapport d'évaluation

La rédaction du rapport d'évaluation doit être conforme à ce qui est spécifié en 5.6 de l'IEC 61069-2:—.

Le rapport doit contenir les informations spécifiées en 5.6 de l'IEC 61069-2:—. De plus, il convient que le rapport d'évaluation aborde également les points suivants:

– informations spécifiées à l'Article 6.

6 Techniques d'appréciation

6.1 Généralités

Plusieurs techniques d'appréciation sont suggérées dans le cadre de l'IEC 61069-3. D'autres méthodes peuvent être appliquées mais, dans tous les cas, il convient que le rapport d'évaluation fasse référence aux documents qui décrivent les techniques utilisées.

Ces techniques d'appréciation sont classées conformément à l'Article 6 de l'IEC 61069-2:—.

Les facteurs ayant une influence sur les propriétés de fonctionnalité du système, comme indiqué en 4.2, doivent être pris en compte.

Les techniques décrites en 6.2, 6.3 et 6.4 sont utilisées pour évaluer les propriétés de fonctionnalité.

Il n'est pas possible d'apprécier la propriété de fonctionnalité en tant qu'entité unique. Il convient plutôt d'étudier séparément chaque propriété de fonctionnalité.

Une fonctionnalité intégrée au système qui n'est pas spécifiée dans le CdC peut être omise dans l'appréciation, mais de telles omissions doivent être enregistrées dans le rapport.

NOTE Un exemple de liste d'éléments d'évaluation est donné dans l'Annexe C.

6.2 Techniques d'appréciation analytique

6.2.1 Couverture

La couverture peut être évaluée en vérifiant analytiquement si le nombre de modules ou d'éléments du système et leurs domaines d'application spécifiés dans le CdS sont en mesure d'exécuter les fonctions requises pour les tâches spécifiées dans le CdC.

Les informations suivantes doivent figurer dans le rapport:

– les tâches et les fonctions de support analysées,
– les fonctions non fournies,
– les déficiences de fonctions découvertes.

6.2.2 Configurabilité

La configurabilité peut être appréciée en énumérant les actions à entreprendre et le temps nécessaire pour configurer, changer ou ajouter une fonction du système afin d'exécuter une tâche dans des circonstances définies, par exemple:

– le savoir-faire et la compétence du personnel concerné;
– les outils utilisés, qui sont fournis par le système ou spécifiés dans le CdS;
– les modes de fonctionnement du système («en ligne», «hors ligne», etc.) pour lesquels chaque action de configuration est autorisée.

6.2.3 Flexibilité

La flexibilité peut être appréciée en effectuant les opérations d'analyse suivantes:

– identification du nombre maximal de répliques fonctionnelles pouvant augmenter la taille du système sans gêner l'exécution correcte des fonctions nécessaires à l'accomplissement des tâches de la mission;
– identification du nombre de fonctions différentes pouvant augmenter la taille du système sans gêner l'exécution correcte des fonctions nécessaires à l'accomplissement des tâches de la mission;
– identification des autres modules et éléments disponibles au catalogue pour améliorer le système avec des valeurs différentes de caractéristiques de fonctionnement, de sûreté de fonctionnement, d'opérabilité et de sécurité du système qu'il est possible d'utiliser sans gêner l'exécution correcte des fonctions nécessaires à l'accomplissement des tâches de la mission.

6.3 Techniques d'appréciation empirique

L'appréciation empirique doit aussi être effectuée pour la couverture, la compatibilité et la flexibilité.

L'appréciation empirique est effectuée pour vérifier le résultat de l'appréciation analytique décrite en 6.2.

6.4 Sujets supplémentaires de techniques d'appréciation

Aucun élément supplémentaire n'est indiqué.

Annexe A
(informative)

Liste de contrôle et/ou exemple de CdC pour la fonctionnalité d'un système

La matrice représentée dans le Tableau A.1 fournit des lignes directrices sur le type d'informations (tâche par tâche et/ou transfert d'information) qu'il convient que le CdC contienne dans le but d'évaluer les caractéristiques de fonctionnement.

Il convient de prêter une attention particulière à vérifier que les moyens de configuration requis et les exigences futures pour le système ont été formulés et quantifiés de manière appropriée, ceci aussi bien au regard des tâches prises individuellement que de la mission d'ensemble du système.

Tableau A.1 – Liste de contrôle du CdC

Propriété	Données, dessins, etc.
Couverture	Tâches requises actuellement et ultérieurement prises en charge par: – le diagramme de mesure et commande du processus, – la description des exigences de mesure et commande en appui de chaque tâche, – les exigences opérationnelles et de surveillance pour chaque tâche, – l'importance de la tâche pour la mission. Environnement comprenant: – un schéma de principe montrant l'emplacement suggéré des points de mesure et commande ainsi que le pupitre / panneau de commande de l'opérateur, etc., – un plan de classification des zones dangereuses, – les contraintes d'espace, d'emplacement, d'accès physique, d'extension.
Configurabilité	Niveau des dispositions requises, par exemple: – fixe, – configurable moyennant certaines contraintes (sous verrouillage, etc.), – librement programmable. Conditions opérationnelles dans lesquelles la configuration est autorisée et/ou requise.
Flexibilité	Extension de la mission envisagée ultérieurement sur plusieurs plans: – reproduction des tâches, – nouvel ensemble de tâches, mesures, sorties, etc., – écrans ou rapports supplémentaires ou plus détaillés. Réalisation progressive ou «en bloc» du projet Evolution envisagée ultérieurement pour les exigences relatives aux propriétés: – amélioration de la sûreté de fonctionnement, – amélioration des caractéristiques de fonctionnement (plus rapide, meilleure précision), – amélioration de l'opérabilité (utilisation d'écrans tactiles, etc.), – nombre maximum d'E/S par I/O par régulateur, – vitesse des tâches, – vitesse de balayage.

Annexe B
(informative)

Liste de contrôle et/ou exemple de CdS pour la fonctionnalité d'un système

B.1 Informations relatives au CdS

Il convient d'effectuer une revue du cahier des spécifications du système afin de s'assurer que les propriétés mentionnées dans le CdC sont détaillées conformément à l'Annexe B de l'IEC 61069-2.

B.2 Points de contrôle de la fonctionnalité d'un système

Il convient de prêter une attention particulière à vérifier que l'on dispose d'informations concernant:

a) les modules et éléments, tant matériels que logiciels, qui supportent chaque fonction;

b) les données quantitatives et/ou qualitatives sur les propriétés de ces modules et éléments, ainsi que la disponibilité de modules et éléments conférant des propriétés différentes;

c) les détails des outils de configuration, leur utilisation et les contraintes qu'ils induisent sur le fonctionnement du système;

d) les moyens fournis par le système qui, dans le système opérationnel complet, aident à l'analyse des propriétés de fonctionnalité. Des exemples de ces moyens incluent les services pour:

   1) dresser la liste de tous les programmes chargés, des modules et éléments d'appui;

   2) calculer la capacité non utilisée dans les mémoires, etc.;

   3) effectuer une analyse statistique de l'utilisation des ressources du système, etc.;

   4) dresser la liste de tous les effets secondaires sur l'une quelconque des autres propriétés du système, pouvant survenir du fait de modifications du système.

Annexe C
(informative)

Exemple de liste d'éléments d'évaluation (informations provenant de l'IEC TS 62603-1)

C.1 Vue d'ensemble

L'Annexe C donne quelques exemples d'éléments d'évaluation relatifs à la présente partie de l'IEC 61069, qui ont été extraits de l'IEC TS 62603-1.

Les classifications des valeurs de propriétés décrites dans le présent document ne sont qu'indicatives.

C.2 Caractéristiques du système

C.2.1 Vue d'ensemble

L'Article C.2 de la norme définit les caractéristiques principales qui influencent la structure et la capacité d'un BCS en termes généraux, avec une attention spéciale sur son intégration et son évolutivité.

C.2.2 Evolutivité du système

L'évolutivité est la capacité d'un système et/ou d'une application à croître progressivement sans un remplacement total du matériel et du logiciel, et sans la nécessité de repenser toute l'architecture du système.

C.2.3 Extensibilité du système

L'extensibilité du système est la possibilité d'étendre le système sans changer l'architecture et/ou l'équipement employé. L'extensibilité peut concerner à la fois le système entier et chaque appareil.

L'extensibilité d'un système permet d'ajouter au système des composants utilisables.

Pour un composant tel qu'un automate programmable, l'extensibilité signifie qu'il est possible d'ajouter une pièce de rechange utilisable aux composants (c'est-à-dire de la mémoire libre ou un processeur dans un automate programmable).

C.2.4 Intégration de sous-systèmes

L'intégration de sous-systèmes requiert un mode opératoire pour associer des modules de composants développés séparément afin qu'ils fonctionnent ensemble en tant que système unique. Un sous-système est un ensemble de composants qui fonctionne dans le cadre d'un système et qui est capable d'effectuer une tâche spécifique au sein d'un système.

Une autre possibilité serait qu'un sous-système ait été fourni par d'autres fournisseurs et fabricants (sous-système tiers).

C.2.5 Documentation automatique

Le BCS génère automatiquement la documentation après la phase de configuration. Les documents peuvent inclure:

– l'architecture du système,
– les paramètres de configuration,
– la liste des matériels,
– les logiciels d'applications,
– le tableau de câblage pour les terminaisons,
– la configuration des câbles et des connexions,
– d'autres éléments.

C.2.6 Langages de programmation pour la commande

C.2.6.1 Généralités

Il convient que la partie commande du système prenne en charge des langages de programmation spécifiques pour la mise en œuvre de la logique de commande. Selon le type des fonctions nécessaires au BCS, un langage de programmation normalisé différent peut être utilisé.

Le terme automate programmable (PLC, Programmable Logic Controller) représente un système électronique à fonctionnement numérique, conçu pour être utilisé dans un environnement industriel, qui se sert d'une mémoire programmable pour le stockage interne des instructions orientées utilisateur pour la mise en œuvre de fonctions spécifiques telles que la logique, le séquencement, la temporisation, le comptage et l'arithmétique. Un PLC peut commander, via des entrées et des sorties numériques ou analogiques, des entrées de compteurs et des sorties à impulsions, différents types de machines ou de processus. Dans un BCS à grande échelle, le terme régulateur est souvent employé avec la même signification. Le PLC et ses périphériques associés sont conçus de manière à pouvoir être intégrés facilement dans un système de commande industriel et être utilisés facilement dans toutes leurs fonctions attendues.

Le terme système-PLC représente une configuration effectuée par l'utilisateur, qui consiste en un régulateur programmable et ses périphériques associés, nécessaire pour le système automatisé prévu. Celle-ci consiste en des unités interconnectées par des câbles ou des connexions pour une installation permanente et par des câbles ou d'autres moyens pour des périphériques portables et transportables.

C.2.6.2 Langages de programmation pour les régulateurs programmables

L'IEC 61131-3 définit un ensemble de langages pour la programmation des PLC et des régulateurs. Les langages de programmation standard sont divisés en deux catégories:

a) les langages graphiques:
   1) Ladder: (LL) est une représentation symbolique qui illustre de façon schématique les fonctions de commande sous la forme de schémas de circuits électriques;
   2) diagramme en blocs fonctionnels (FBD, Function Block Diagram): il permet de faire apparaître les éléments du programme (le PID et les autres algorithmes) sous forme de blocs connectés ensemble comme indiqué dans une présentation visuelle similaire à un diagramme logique;
b) langages textuels:
   1) Liste d'instructions (IL): il s'agit d'un langage de bas niveau similaire à l'assembleur, dans lequel une seule opération, comme le stockage d'une valeur dans un registre, est autorisée par ligne;
   2) Texte structuré (ST): il s'agit d'un langage de haut niveau structuré en blocs, dont la syntaxe ressemble au Pascal. ST permet d'exprimer des instructions complexes faisant intervenir des variables qui représentent un grand nombre de types de données différents.

C.2.6.3 Outil de programmation Diagramme fonctionnel en séquence (SFC, Sequential Function Chart)

En plus des langages de programmation définis dans l'IEC 61131-3, l'outil de programmation SFC autorise une représentation graphique et la structuration du logiciel de commande. SFC est une manière de représenter graphiquement un programme de commande complexe sous la forme d'une suite d'étapes et de transitions.

C.2.6.4 Outil de programmation Diagramme fonctionnel continu (CFC)

Le diagramme fonctionnel continu (CFC) permet de convertir de façon simple des spécifications technologiques en programmes d'automation exécutables: il utilise pour cela des blocs fonctionnels reliés ensemble et configurés individuellement.

Le CFC peut être considéré comme une forme spéciale de FBD. La différence principale entre le CFC et le FBD réside dans le fait qu'il fait aussi apparaître les ressources et les affectations de tâches. Chaque bloc fonctionnel montre le nom de la tâche qui commande son exécution.

Le CFC est principalement utilisé pour montrer la structure de haut niveau des ressources et des programmes.

C.2.6.5 Définition d'un bloc fonctionnel personnalisé

L'IEC 61131-3 définit un ensemble de blocs fonctionnels standard communs à tous les régulateurs programmables. Un bloc fonctionnel est un ensemble d'éléments consistant en:

a) la définition d'une structure de données partitionnée en entrée, sortie et variables internes; et

b) un ensemble d'opérations à effectuer sur les éléments de la structure de données lorsqu'une instance du type de bloc fonctionnel est appelée.

Exemples de blocs fonctionnels standard:

– verrou,

– détection de contours,

– compteur,

– temporisateur.

En plus des blocs fonctionnels standard, il peut être utile de définir des blocs fonctionnels personnalisés déclenchant des fonctions spécifiques. Une fois défini, un bloc fonctionnel personnalisé se comporte comme un bloc standard.

C.2.6.6 Outil de programmation par lots

Le BCS peut prendre en charge l'environnement pour la commande par lots définie dans l'IEC 61512.

C.2.6.7 Logiciel d'exploitation multitâche pour le régulateur

Le logiciel d'exploitation multitâche est une méthode de gestion des ressources du processeur du régulateur qui permet à plusieurs tâches de partager des ressources de traitement communes. La fonction multitâche permet au programmeur d'utiliser la capacité de multiprogrammation du régulateur. Le terme de multiprogrammation désigne une méthode de programmation dans laquelle plusieurs tâches sont en même temps dans un état exécutable.

C.2.6.8 Commande de processus avancée (APC)

L'APC peut se définir comme les stratégies de commande de processus sous-jacentes à des boucles de commande de PID simples. Les APC sont des outils logiciels vendus comme modules supplémentaires qui peuvent être interfacés ou installés dans le BCS. Un APC autorise une meilleure commande et une optimisation du processus, et il utilise normalement des techniques de commande sophistiquées comme: les systèmes experts, la commande par mode glissant, la commande multivariable, etc.

C.2.7 Localisation d'un BCS

La localisation est la capacité d'un BCS à prendre en charge les langues locales pour différentes fonctions, comme:

– la programmation;
– la documentation;
– l'interface homme-machine (IHM).

Les langages et fonctions nécessaires doivent être spécifiés.

C.3 Propriétés de fonctionnalité

C.3.1 Spécifications d'entrée/sortie

Les types d'entrée/sortie considérés sont: E/S analogique conventionnelle (c'est-à-dire 4 mA à 20 mA, 0 V à 10 V, etc.), E/S numérique, compteurs (par exemple les compteurs rapides), sorties à impulsions, E/S Hart et fieldbus. Pour chaque type d'E/S, il convient que l'utilisateur spécifie la résolution, la précision et la répétabilité.

C.3.2 Entrée/sortie conventionnelle

C.3.2.1 Entrée numérique

La spécification des entrées numériques peut inclure:

– la tension d'entrée assignée (c'est-à-dire 24 V en courant continu) et le courant (c'est-à-dire 10 mA);
– le retard de l'entrée (fixe ou variable);
– l'affichage d'état local des entrées;
– l'isolation électrique entre les entrées et entre les entrées et le fond de panier;
– le niveau d'isolation (c'est-à-dire 1 kV en courant continu).

C.3.2.2 Sortie numérique

La spécification de la sortie numérique peut inclure:

– le type de sortie: statique ou relais;
– la charge connectée, c'est-à-dire valves de solénoïdes, contacteurs, lumières, etc.;
– la tension de sortie assignée (c'est-à-dire 24 V en courant continu);
– le courant de sortie assigné (permanent et pendant un court laps de temps);
– l'affichage local des sorties (c'est-à-dire DEL);
– l'isolation électrique entre les entrées et entre les entrées et le fond de panier;
– le niveau d'isolation (c'est-à-dire 1 kV).

C.3.2.3 Entrée analogique

La spécification de l'entrée analogique peut inclure:

– le type des entrées, c'est-à-dire thermocouple, détecteur de températures à résistance (2-3-4 fils), 4 mA à 20 mA;
– la protection de polarité inverse;
– l'isolation électrique entre les entrées et entre les entrées et le fond de panier;
– le niveau d'isolation (c'est-à-dire 500 V en courant continu).

C.3.2.4 Sortie analogique

La spécification de la sortie analogique peut inclure:

– le type de sortie, c'est-à-dire 4 mA à 20 mA, ± 10 V, 0 V à 5 V, etc.;
– la résolution (ou le nombre de bits de conversion);
– l'isolation électrique entre les sorties et entre les sorties et le fond de panier;
– le niveau d'isolation (c'est-à-dire 500 V en courant continu);
– la protection de sortie individuelle avec fusible.

C.3.2.5 Compteurs

Les compteurs sont généralement numériques. On les utilise pour des éléments tels que des totalisateurs de débitmètres.

C.3.2.6 Sorties à impulsions

Les sorties à impulsions sont généralement numériques. Elles sont particulièrement adaptées pour maintenir des éléments tels que des vannes en position fermée en cas de défaillance du BCS. La correction de l'erreur évite également de mettre la sortie à une position inattendue.

C.3.3 Entrée/sortie avec des appareils intelligents

Il est courant d'utiliser des appareils intelligents sur le terrain. Dans ce cas, l'entrée/sortie analogique prend en charge la conversion entre le protocole utilisé pour les appareils intelligents (c'est-à-dire Hart) et le protocole utilisé pour la commande de processus. En plus des données spécifiées pour les E/S analogiques, l'utilisateur spécifie les protocoles utilisés.

C.3.4 Connexion fieldbus avec l'E/S distante

L'utilisateur indique si une connexion fieldbus est employée pour connecter l'E/S distante et les régulateurs. Le fieldbus peut être un fieldbus IEC 61158 normalisé ou un fieldbus propriétaire.

C.3.5 Validation des entrées

Lorsqu'un contact unipolaire bidirectionnel (SPDT, Single Pole Double Throw) est acquis sous la forme de deux entrées numériques, une logique de validation est mise en œuvre pour détecter les états anormaux. De même, l'état hors-plage d'un signal analogique est détecté lorsque le signal monte au-dessus ou descend en dessous de la plage valide.

C.3.6 Entrées spéciales

Des exigences spécifiques pour les entrées, différentes des exigences habituelles, doivent être spécifiées.

C.3.7 Exigences concernant les logiciels

C.3.7.1 Exigences concernant la base de données système

La base de données système fournit les informations nécessaires à différentes transactions (fonctions) système pour l'exécution de leurs tâches. Les données d'entrée proviennent des appareils de terrain (capteurs, émetteurs, commutateurs, etc.) via les interfaces d'acquisition de données du régulateur, des systèmes de commande de supervision (PC, système de commande réparti, DCS (Distributed Command System), PLC), via les liaisons de régulateurs externes, et d'autres régulateurs via des connexions inter-régulateurs. Les données de sortie sont dirigées vers les appareils de commande et d'indication sur le terrain, les systèmes de supervision et les autres régulateurs.

La base de données système est une base de données temps réel, c'est-à-dire qu'elle doit offrir un temps de réponse prévisible pour garantir l'achèvement des transactions critiques dans les temps.

C.3.7.2 Agencement physique de la base de données (mise en œuvre)

La base de données système peut être installée physiquement de deux manières:

– base de données répartie: les données sont réparties sur plusieurs emplacements physiques. La base de données tout entière est commandée par un système de gestion de base de données (SGBD) central qui coordonne tous les fichiers de données;

– base de données concentrée: toutes les données sont stockées dans une base de données centrale, c'est-à-dire que tous les enregistrements sont présents sur une machine unique et accessibles par le système de gestion de base de données (SGBD).

C.3.7.3 Compatibilité avec une base de données externe

Si la base de données système garantit la compatibilité et la connexion avec d'autres bases de données, il est nécessaire de spécifier quelles bases de données ont accès ou sont accessibles à la base de données système.

C.3.7.4 Type de logiciel

Le logiciel de mise en œuvre de la base de données peut être un produit du commerce ou un produit propriétaire. En cas d'exigence ou de contrainte spécifique, il est nécessaire de spécifier le langage de programmation nécessaire pour la base de données. Ce choix est normalement du ressort du fabricant du BCS.

C.3.8 Gestion des alarmes

C.3.8.1 Généralités

Le système de gestion des alarmes du BCS prend en charge la sélection des événements à considérer comme des alarmes, la définition des priorités d'alarme, les procédures d'accusé de réception, etc.

Il convient que la gestion des alarmes soit conçue pour éviter l'affichage d'un flot d'alarmes sur l'interface de l'opérateur. Il convient que la gestion des alarmes soit conçue en respectant les quelques règles suivantes:

– les alarmes simples doivent montrer l'emplacement et l'action recommandée;

– il convient que l'accès aux écrans appropriés soit rapide et adapté, et ne nécessite que la frappe d'un nombre de touches minimum;

– il convient que des techniques de traitement soient mises en œuvre, en particulier pour la définition de priorités et les annonces;

– il convient que les techniques soient faciles à reconfigurer.

C.3.8.2 Types d'alarmes

Différents types d'alarmes peuvent être définis. Les fonctions d'alarme habituelles incluent:

– seuil absolu: un paramètre donné atteint un certain niveau de seuil;
– delta unique: une alarme supplémentaire avertit que le signal continue d'augmenter. Le signal a dépassé un certain pourcentage au-dessus du seuil défini;
– delta répétitif: une alarme est déclenchée à chaque changement sélectionné au-delà de ce qui a été choisi pour l'alarme delta unique;
– vitesse de changement: une alarme est déclenchée en cas de changement rapide de la variable même si aucun seuil n'a été dépassé. La vitesse de changement s'exprime normalement en unités par seconde ou en pourcentage de temps;
– retour à la normale: si nécessaire, l'opérateur a besoin d'être averti lorsqu'un paramètre revient à la normale, pas uniquement lorsque ce paramètre passe en valeur d'alarme;
– délai: certains paramètres sont relativement instables ou fluctuent simplement en continu, comme les pressions ou les débits. Il est souvent utile de définir sur de telles alarmes un délai agissant comme zone d'insensibilité, afin qu'un pic ne déclenche pas une alarme intempestive;
– «arrêt momentané» de l'alarme: la fonction d'«arrêt momentané» de l'alarme déclenche à nouveau l'alarme si la condition persiste au-delà d'un temps déterminé après l'acquittement. Dans certains cas, ce type d'alarme peut être paramétré pour s'acquitter lui-même si la condition disparaît;
– alarme avec hystérésis: une alarme avec hystérésis possède différents seuils dans chaque direction, vers le haut ou vers le bas. Employée de la même manière que le délai, cette zone d'insensibilité réduit les alarmes intempestives dans des fluides actifs dynamiquement.

C.3.8.3 Sévérité de l'alarme

Il convient de signaler tout défaut ou fonctionnement anormal du BCS à l'opérateur, avec une indication de la sévérité de l'alarme. La sévérité de l'alarme indique l'ordre dans lequel il convient que les utilisateurs traitent l'événement relatif aux alarmes des autres sévérités. Les niveaux de sévérité peuvent aider à planifier les activités de maintenance et de réparation et constituent une fonctionnalité importante des messages d'autodiagnostic (alarmes système). La sévérité ne concerne pas les alarmes de processus.

Les niveaux de sévérité peuvent être définis comme suit:

– arrêt: aucune réponse de l'entité ou de l'appareil surveillé;
– élevée (critique): condition d'alarme qui handicape sérieusement le service et requiert une correction immédiate;
– moyenne (conseil): condition d'alarme qui handicape le service, mais pas de façon sérieuse;
– faible (journal): condition d'alarme qui ne handicape pas le service, mais qui doit être corrigée avant de devenir plus grave.

La définition des niveaux de sévérité est à la charge du fabricant du BCS, de même que ses modes opératoires d'affichage.

C.3.8.4 Niveau de priorité d'alarme

La priorité d'une alarme indique l'urgence de la réponse de l'opérateur, par exemple la gravité des conséquences et le temps de réponse admissible. Trois niveaux de priorité sont définis:

– niveau 1: action immédiate de l'opérateur. Mise en danger du personnel, défaillance d'équipement/impact environnemental catastrophique, arrêt de l'unité ou arrêt imminent d'autres unités;

– niveau 2: action rapide de l'opérateur exigée. Arrêt possible de l'unité. Un arrêt partiel a eu lieu. Alarme de priorité d'urgence possible;
– niveau 3: action prompte de l'opérateur exigée. Alarme de haute priorité possible. Comportement non conforme aux spécifications imminent ou perte de production imminente.

Il convient que l'utilisateur indique si le système de gestion des alarmes du BCS doit prendre en charge les niveaux de priorité.

C.3.8.5 Groupement des alarmes

Les alarmes peuvent être organisées en groupes selon des critères géographiques ou fonctionnels. Le groupement d'alarmes doit permettre à l'opérateur de reconnaître rapidement des manifestations caractéristiques dans une suite d'alarmes et de découvrir les zones ou les machines impliquées.

C.3.8.6 Acquittement des alarmes

Il convient que toutes les alarmes soient acquittées par le ou les opérateurs. Pour chaque alarme, selon son groupe, sa sévérité et sa priorité, une suite d'actions indiquant que l'alarme a été reconnue est définie. Différentes séquences d'acquittement peuvent être mises en œuvre.

C.3.8.7 Système d'alarme «intelligent» / masquage des alarmes

Pour réduire l'effort nécessaire à l'opérateur pour comprendre les causes d'un événement anormal, les alarmes qui sont évidentes ou redondantes ne doivent pas être affichées. Le BCS prend en charge un système d'alarme «intelligent» dans lequel des alarmes prédéfinies peuvent être automatiquement dissimulées à l'opérateur dans le cas de conditions particulières de processus ou d'installations.

Il convient que le système fournisse les outils et la capacité d'une configuration facile des alarmes qui sont à «masquer» en fonction de l'état d'une installation ou de la condition d'un processus.

Les alarmes masquées ne sont pas présentées à l'opérateur sur les affichages d'alarmes ou les graphiques de processus standard, mais leur déclenchement est enregistré dans l'historique des alarmes. Il convient qu'un affichage des «alarmes masquées» soit fourni, qui présente toutes les alarmes actuellement masquées à l'opérateur.

C.3.8.8 Annonce des alarmes

L'annonce des alarmes est la capacité du système à prévenir les opérateurs du déclenchement des alarmes. Le processus d'annonce peut, par exemple, inclure:

– l'activation d'une alarme sonore extérieure ou de signaux lumineux;
– l'activation de la carte son interne du PC (par exemple pour lire des fichiers .wav);
– la mise à jour d'un affichage d'alarme avec l'alarme en cours;
– la mise à jour d'un écran de vue d'ensemble des alarmes pour indiquer le déclenchement d'une alarme dans une zone / un affichage de processus spécifique;
– l'impression du message d'alarme sur une imprimante d'alarme;
– tout objet graphique associé au point d'alarme doit changer de couleur ou de forme, apparaître, disparaître, etc. selon la configuration.

C.3.8.9 Listes d'affichages récapitulatifs des alarmes

Un récapitulatif des alarmes peut être utile, et il peut inclure:

– les alarmes de processus actives,
– les alarmes de processus effacées,
– les alarmes de processus acquittées,
– les alarmes système actives,
– les alarmes système effacées,
– les alarmes système acquittées,
– l'historique des alarmes,
– la liste des actions de l'opérateur,
– la liste des alarmes supprimées (verrouillées),
– la liste des alarmes masquées,
– la liste des affichages de fréquences d'alarmes.

L'accès à un écran récapitulatif des alarmes à partir d'un autre écran doit nécessiter un nombre d'actions minimum de la part de l'opérateur.

Des écrans de plusieurs pages peuvent être utilisés. Dans ce cas, il doit être possible de parcourir les pages vers l'avant ou vers l'arrière. L'écran doit afficher les listes d'alarmes en format tabulaire dans l'ordre de déclenchement.

C.3.9 Gestion des événements

C.3.9.1 Généralités

Un événement est un changement d'état d'une variable dans le processus. Les événements courants sont:

– changement d'état d'entrées numériques;
– variables analogiques atteignant un seuil;
– commandes de l'opérateur, etc.

Un événement peut démarrer ou non une action de commande.

C.3.9.2 Séquence d'événements (SOE, Sequence Of Events)

La résolution temporelle est le temps minimum dont il convient de séparer deux événements afin que les repères temporels correspondants soient différents. La capacité de séparation est le temps minimum dont il convient de séparer deux événements pour que la séquence de leur apparition soit déterminée correctement. La résolution temporelle ne peut pas être plus courte que la capacité de séparation, et elle est normalement spécifiée.

C.3.9.3 Intégration de la SOE avec des systèmes tiers

Si les données traitées par la SOE peuvent être accessibles par d'autres applications et/ou systèmes, il est nécessaire de les spécifier, de même que si un pilote ou une interface de communication spécifique est nécessaire (c'est-à-dire alarme et événement OPC (OLE for Process Control)).

C.3.9.4 Types d'événements

Les types d'événements sont classés selon leurs sources:

– opérateur: changements opérateur tels que les changements de points de consigne, les changements de sortie de commande ou les changements de mode de régulateur. Réactions aux alarmes, telles que des acquittements;

– alarme: chaque alarme présente toujours deux événements: basculement dans une condition d'alarme et basculement pour sortir de la condition d'alarme (ce dernier pouvant ou non inviter à effectuer une réinitialisation);
– processus: les événements sont liés à l'état du système surveillé, comme des événements de protection, des changements de qualité dans les mesures, etc.

C.3.10 Archivage

C.3.10.1 Généralités

Les événements peuvent être archivés dans la base de données historique, ce qui revient à enregistrer dans une machine centralisée un signal particulier provenant du régulateur où l'événement a été généré ou acquis par un capteur. Il convient de n'archiver dans la base de données historique que certains événements. Les paragraphes C.3.10.2 et C.3.10.3 présentent les méthodes d'archivage et les spécifications pour définir les données qu'il convient d'archiver.

C.3.10.2 Méthode d'archivage

La base de données historique peut stocker des événements selon différentes méthodes:

– cycliquement: une fréquence de collecte fixe est utilisée pour échantillonner les données;
– en cas de variation: les données activation/désactivation sont stockées uniquement lors d'un changement d'état; les données analogiques sont stockées lorsque leur valeur change au-delà d'un seuil prédéfini;
– en cas d'événement: les données sont collectées sur la base d'un événement déclencheur ou d'une interruption.

Il convient de définir le nombre d'événements à archiver.

C.3.10.3 Sauvegarde des archives

La base de données historique est une partie critique du BCS dans son ensemble et c'est la raison pour laquelle il convient de choisir un support de sauvegarde. Les archives de sauvegarde sont importantes pour restaurer les données après un sinistre ou après que certaines données ont été endommagées.

Pour sélectionner la meilleure archive de sauvegarde pour la base de données historique, il convient de définir les fonctionnalités suivantes:

– type matériel du dépôt de sauvegarde;
– durée de vie attendue de la sauvegarde;
– nécessité d'un outil de sauvegarde logiciel pour guider le processus de sauvegarde intelligente;
– fréquence des sauvegardes (quotidienne, hebdomadaire, mensuelle, etc.);
– format requis pour les données stockées.

C.3.11 Gestion des tendances et des statistiques

C.3.11.1 Généralités

Pour la supervision et la commande de processus et d'installations, il convient que l'interface homme-machine (IHM) montre à la fois les valeurs instantanées et les valeurs enregistrées dans différents formats selon les exigences du processus.

C.3.11.2 Fonctionnalités de la tendance

Les principales fonctionnalités définissant l'application de tendance sont:

– le nombre de traces disponibles par écran/fenêtre;
– le type des variables dont la tendance doit être établie;
– taux minimal/maximal d'échantillonnage;
– l'intervalle temporel ou la capacité totale des données affichées sur la même tendance.

C.3.11.3 Tendance de valeurs analogiques

La tendance de valeurs analogiques peut inclure les fonctionnalités suivantes:

– valeur actuelle,
– moyenne,
– minimum,
– maximum,
– écart-type.

C.3.11.4 Tendance de valeurs discrètes

La tendance de valeurs discrètes peut inclure les fonctionnalités suivantes:

– état actuel,
– état de départ,
– nombre de transitions,
– statistiques.

C.3.11.5 Exigences relatives à la navigation parmi les tendances

Il convient que le système de tendances respecte certaines exigences pour une navigation confortable, telles que les suivantes:

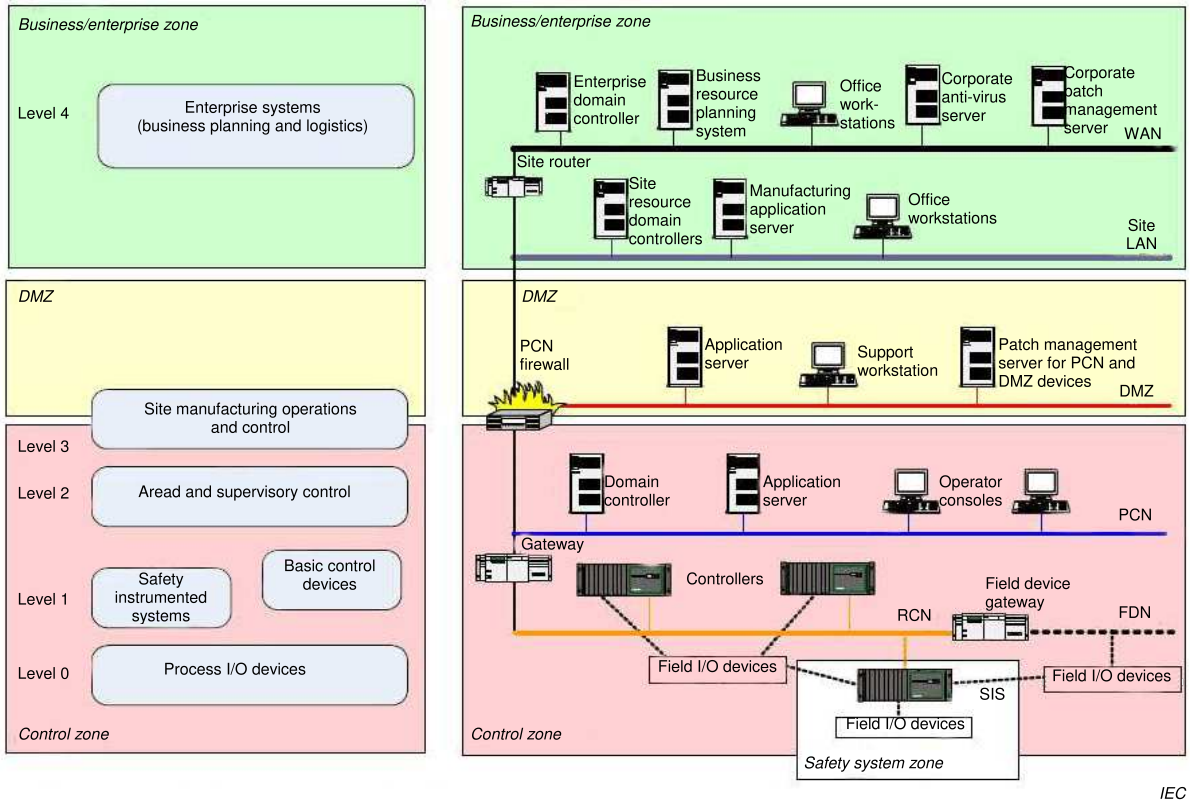
– panoramique: déplacement «vers l'avant et vers l'arrière» le long des mêmes divisions temporelles au sein d'une tendance plus longue qu'un seul écran;
– zoom: passage à des divisions temporelles différentes.

En plus de la fonction de panoramique et de zoom, le curseur peut proposer des fonctions supplémentaires, comme:

– heure/date de positionnement,
– valeur/état des traces d'intersection,
– étiquettes et titres de toutes les traces affichées,
– choix d'une zone de zoom pour des détails supplémentaires.

C.3.12 Exigences relatives à la communication

La communication joue un rôle clé dans un BCS. Différents réseaux de communication coexistent dans un BCS, chacun avec des fonctionnalités et des exigences spécifiques. Les réseaux de communication peuvent être habituellement divisés en trois ou quatre niveaux selon la technologie utilisée. La Figure C.1 présente de façon schématique ces différents choix.



Anglais	Français
Business/enterprise zone	Zone de l'activité/l'entreprise
Level	Niveau
Enterprise systems (business planning and logistics)	Systèmes de l'entreprise (planification de l'activité et logistique)
Enterprise domain controller	Contrôleur de domaine de l'entreprise
Business resource planning system	Systèmes de planification des ressources de l'activité
Office workstations	Postes de travail de bureau
Corporate anti-virus server	Serveur antivirus de l'entreprise
Corporate patch management server	Serveur de gestion de correctifs de l'entreprise
WAN	Réseau étendu (WAN)
Site router	Routeur du site
Site resource domain controllers	Contrôleurs de domaine des ressources du site
Manufacturing application server	Serveur d'applications pour la fabrication
Site LAN	Réseau local (LAN) du site
DMZ	DMZ
PCN firewall	Pare-feu PCN
Application server	Serveur d'applications
Support workstation	Poste de travail de support
Patch management server for PCN and DMZ devices	Serveur de gestion de correctifs pour appareils PCN et DMZ
Site manufacturing operations and control	Opérations et commande relatives à la fabrication sur site
Area and supervisory control	Commande de zones et de supervision

Anglais	Français
Safety instrumented systems	Systèmes dotés d'instruments de sécurité
Basic control devices	Appareils de commande de base
Process I/O devices	Appareils d'E/S du processus
Control zone	Zone de commande
Domain controller	Contrôleur de domaine
Application server	Serveur d'applications
Operator consoles	Consoles d'opérateur
Gateway	Passerelle
Controllers	Régulateurs
RCN	RCN
Field device gateway	Passerelle des appareils de terrain
PCN	PCN
FDN	FDN
Field I/O devices	Appareils d'E/S du terrain
Safety system zone	Zone du système de sécurité

Figure C.1 – Réseaux de communication dans un BCS

C.3.13 Fieldbus

Selon l'IEC 61158, les exigences principales pour les fieldbus qu'il convient de spécifier sont:

– la couche physique: cuivre, fibre optique ou sans fil,
– le profil de communication (CPF, Communication Profile Family) selon l'IEC 61784,
– le nombre d'appareils reliés au réseau,
– l'installation dans des zones dangereuses,
– la redondance exigée pour le support de communication,
– la distance maximale entre l'appareil de terrain et le régulateur.

C.3.14 Réseau des régulateurs

Les exigences pour le réseau des régulateurs qu'il convient de spécifier sont:

– le type de protocole utilisé,
– la couche physique,
– l'installation dans des zones dangereuses,
– la redondance exigée pour le support de communication,
– la distance maximale de la connexion.

C.3.15 Réseau de la salle de commande

Les exigences pour le réseau de la salle de commande qu'il convient de spécifier sont:

– le type de protocole utilisé,
– la couche physique,
– la redondance exigée pour le support de communication,
– la distance maximale de la connexion.

C.3.16 Liaison externe

La liaison externe permet de mettre en communication différents réseaux, par exemple le réseau de la salle de commande et le réseau de l'entreprise (voir Figure C.1).

Il convient que l'utilisateur spécifie:

– les réseaux qui ont besoin de la liaison de communication,
– le niveau de sécurité nécessaire,
– la nécessité d'un pare-feu,
– la nécessité d'un antivirus.

C.3.17 Interfaces de communication

Plusieurs réseaux de communication peuvent exister dans un BCS, et il est donc nécessaire de définir les interfaces entre les réseaux ainsi qu'entre différents systèmes.

Il convient que l'utilisateur spécifie:

– le protocole de communication entre les réseaux qui échangent des données et des informations,
– le volume de données échangées,
– la durée de rafraîchissement exigée pour l'utilisation de données valides,
– le support physique des réseaux connectés,
– le niveau de sécurité souhaité.

Une interface de communication permet de partager et de transmettre des données et des informations entre différents systèmes de communication utilisant différents supports physiques et/ou différentes structures de données. De cette manière, les données peuvent être déplacées dans tout le système de communication du BCS, et être utilisées là où elles sont nécessaires.

C.3.18 Communication avec un système ERP

Le système de planification des ressources d'entreprise (ERP) intègre des informations de gestion internes et externes de toute une entreprise, en englobant les finances/la comptabilité, la fabrication, les ventes et le service, etc. Les systèmes ERP automatisent cette activité avec une application logicielle intégrée. Celle-ci a pour but de faciliter la circulation d'informations entre toutes les fonctions métier au sein de l'entreprise et de gérer les connexions avec les parties concernées extérieures.

L'ERP doit communiquer et échanger des données avec le système de commande, là où les données de productivité sont générées. Les systèmes ERP se connectent à des données temps réel et des données transactionnelles de différentes façons:

– intégration directe: connectivité des systèmes ERP (communications vers le système de commande) du produit offert par leurs fournisseurs. Cela exige de la part du fournisseur une offre de support spécifique pour le système de commande utilisé par ses clients;
– intégration de base de données: les systèmes ERP se connectent à un système de commande par l'intermédiaire de tables de relais dans une base de données. Les systèmes de commande déposent les informations nécessaires dans la base de données. Le système ERP lit les informations dans la table;
– modules de transactions d'appareils d'entreprise (EATM, Enterprise Appliance Transaction Module): Ces appareils communiquent directement avec le système de commande et avec le système ERP via les méthodes prises en charge par le système ERP. Les EATM

peuvent se servir d'une table de relais, de services Web ou d'interfaces de programmation (API, Application Programming Interface) propres au système;

– protocoles standard: Des pilotes de communication sont disponibles pour le système de commande, et des produits séparés ont la possibilité d'historiser des données dans des tables de relais. Des normes existent dans l'industrie pour prendre en charge l'interopérabilité entre les produits logiciels, la plus connue étant OPC;
– il est nécessaire d'examiner et de prendre en compte les besoins en matière de sécurité pour ce système ERP; en particulier, il sera tenu compte du fait que les violations de la sécurité peuvent provenir de la partie bureau du réseau (hors de la partie commande).

C.3.19 Communication avec un système d'exécution de fabrication (MES)

Un MES est un système de planification et de suivi de la production utilisé pour analyser et consigner dans un rapport la disponibilité et l'état des ressources, planifier et mettre à jour les commandes, recueillir des données d'exécution détaillées telles que l'utilisation du matériel, l'utilisation de la main-d'œuvre, les paramètres de traitement, l'état des commandes et des équipements, ainsi que d'autres informations critiques. Il accède aux nomenclatures, au routage et à d'autres données du système ERP de base et constitue le système habituellement utilisé pour la génération de rapports et la surveillance en temps réel d'un espace de vente ainsi que le renvoi des données d'activité au système de base.

Les méthodes de connexion au MES sont les suivantes:

– intégration directe: connectivité des systèmes MES (communications vers le système de commande) du produit offert par leurs fournisseurs. Cela exige de la part du fournisseur une offre de support spécifique pour le système de commande utilisé par ses clients;
– Intégration de base de données: les systèmes MES se connectent au système de commande par l'intermédiaire de tables de relais dans une base de données. Les systèmes de commande déposent les informations nécessaires dans la base de données. Le système MES lit les informations dans la table.
– protocoles standard: Des pilotes de communication sont disponibles pour le système de commande, et des produits séparés ont la possibilité d'historiser des données dans des tables de relais. Des normes existent dans l'industrie pour prendre en charge l'interopérabilité entre les produits logiciels, la plus connue étant OPC.
– il est nécessaire d'examiner et de prendre en compte les besoins pour ce système MES; en particulier, il sera tenu compte du fait que les violations de la sécurité peuvent provenir de la partie bureau du réseau (hors de la partie commande).

C.3.20 Simulateur logiciel

Un simulateur logiciel est un programme qui permet à l'utilisateur d'observer une opération par le biais d'une simulation sans réellement exécuter le programme.

Le logiciel de simulation permet de soumettre à essai le comportement d'un système après une modification ou une nouvelle configuration sans avoir à connecter le matériel véritable. Le logiciel de simulation autorise un meilleur débogage dans un environnement de simulation avant le téléchargement du programme ou la configuration du système réel.

C.3.21 Simulateur de la logique de commande

La logique de commande mise en œuvre peut être essayée sur le PC ou le poste de travail de configuration. Le simulateur permet de soumettre à essai la logique sans connecter de matériel. La simulation est utile pour vérifier la cohérence globale du programme de logique de commande et l'effet des modifications.

C.3.22 Débogage en ligne

Le débogage en ligne permet de vérifier et de corriger un programme pendant son exécution même si d'autres programmes s'exécutent simultanément. Le débogage permet de détecter et de corriger les défauts éventuels des programmes.

C.3.23 Simulateur d'E/S

Le simulateur d'E/S permet de simuler le fonctionnement des E/S. Dans ce cas, il est possible de forcer les valeurs des E/S de manière à vérifier une logique spécifique ou des boucles de commande.

C.3.24 Fonctions de supervision à distance

Un ordinateur distant doté des droits d'administrateur appropriés peut superviser le BCS. La supervision à distance s'étend aux affichages, étiquettes ou variables, au paramétrage des boucles de commande, à l'acquisition d'alarmes, etc. L'utilisateur peut spécifier les fonctions que la supervision à distance peut exécuter.

C.3.25 Technologie et domaine d'application du BCS

Selon la terminologie actuelle, les technologies disponibles pour les BCS peuvent être sélectionnées parmi les suivantes:

– basée sur PLC;
– basée sur PLC logiciel;
– DCS;
– SCADA;
– autres (à spécifier).

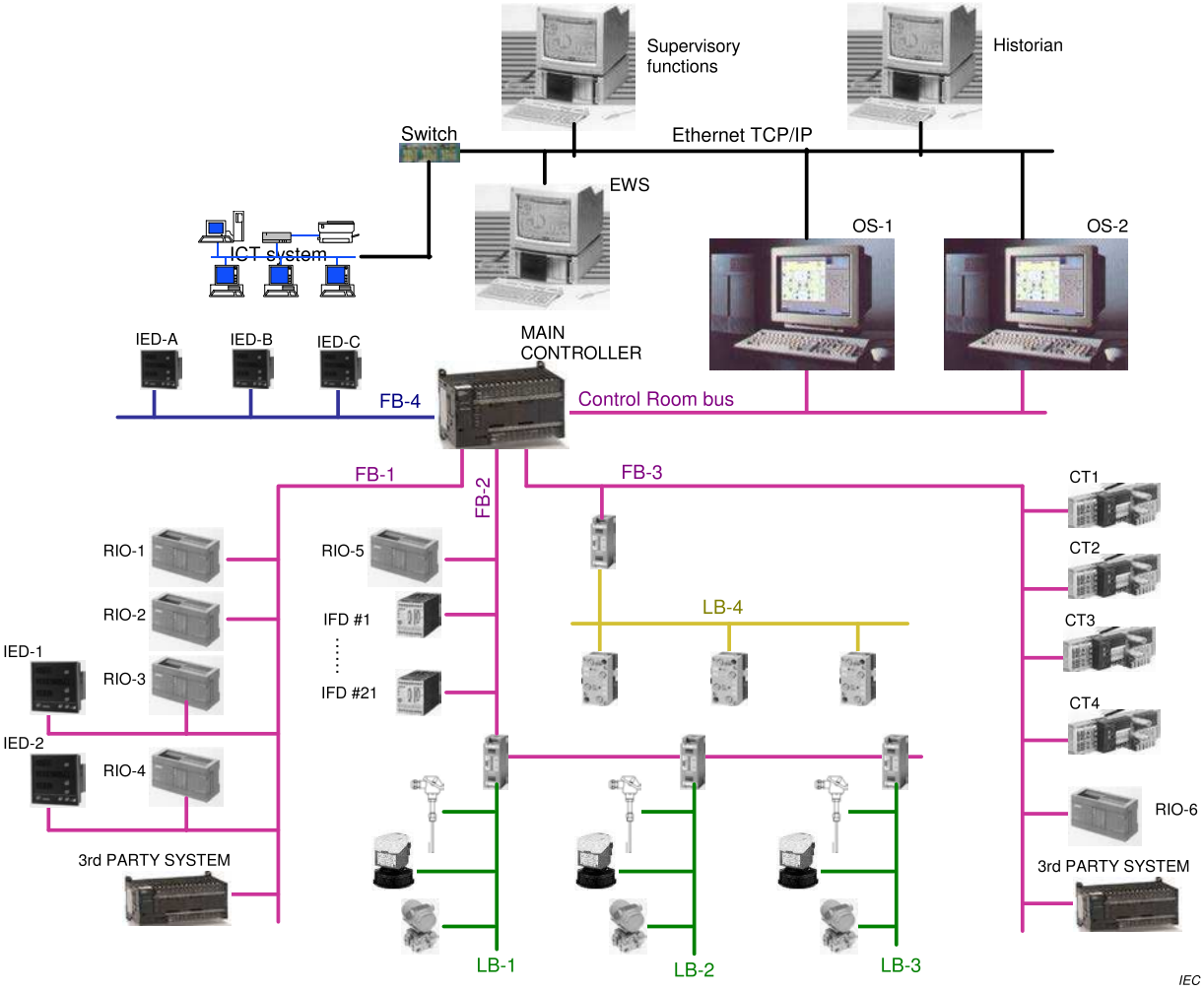
La ou les fonctions de base du BCS nécessaire sont sélectionnées parmi un ou plusieurs des choix suivants:

– supervision;
– commande;
– ESD;
– traitement de lots;
– autres (à spécifier).

C.3.26 Architecture de base

La topologie du BCS est normalement présentée dans un schéma joint à la spécification technique, dans lequel tous les principaux composants sont indiqués et nommés. Dans le cas de systèmes complexes, le schéma peut être scindé en plusieurs feuilles: plan, sous-systèmes, agencement de la salle de commande, etc. La Figure C.2 présente un exemple d'agencement pour un BCS de taille moyenne.

La présente norme définit les exigences pour les composants du BCS, des appareils de terrain à la salle de commande, et les exigences des interfaces pour la connexion du BCS aux autres systèmes numériques et de communication de l'usine, par exemple les systèmes TIC, qui ne sont pas dans le domaine d'application de la présente norme.



Anglais	Français
Supervisory functions	Fonctions de supervision
Historian	Historien
Switch	Commutateur
Ethernet TCP/IP	Ethernet TCP/IP
Main controller	Régulateur principal
ICT system	Système TIC
Control room bus	Bus de la salle de commande
3rd party system	Système tiers

Figure C.2 – Exemple de schéma d'agencement

C.4 Configurabilité

C.4.1 Configuration du système

La configuration du système est la construction d'un système de commande en sélectionnant des unités fonctionnelles ou modulaires dans un ensemble donné et en définissant leurs interconnexions. La configurabilité du système définit la mesure dans laquelle le système facilite la sélection, l'installation et l'agencement de ses modules pour accomplir sa mission.

La configuration peut être à la fois matérielle et logicielle.

Les principales fonctionnalités de la configuration logicielle du système sont:

– la définition de l'architecture du système au moyen de l'outil de configuration;
– l'insertion de modules logiciels;
– la sélection et la définition des paramètres;
– la sélection des options;
– la programmation;
– la compilation et le téléchargement des programmes;
– l'ingénierie de base.

Certaines actions de configuration logicielle peuvent aussi être permises si le système est en fonctionnement. Certains outils de configuration permettent la configuration du système tout entier même si aucun matériel n'est connecté (mode émulé).

Les fonctionnalités de base de la configuration matérielle d'un BCS sont:

– l'insertion de modules;
– le montage d'appareils;
– la connexion par soudure et/ou par câblage;
– le positionnement de cavaliers;
– le positionnement d'interrupteurs;
– l'insertion de cartes de circuit imprimé.

Normalement, pour que la configuration matérielle soit effectuée, il est nécessaire que le système ne soit plus en mode d'exploitation.

C.4.2 Configuration en ligne

Si le système prend en charge la configuration en ligne, il est possible d'exécuter le mode opératoire de configuration du système pendant que le BCS est en fonctionnement sans perte de fonctionnalités. La configuration en ligne peut avoir différents niveaux:

– une reconfiguration totale à la fois matérielle et logicielle est possible;
– seules des modifications matérielles mineures sont possibles;
– seules des modifications logicielles mineures sont possibles.

La configuration en ligne est souvent liée à la politique de redondance du BCS.

C.4.3 Configuration hors ligne

La configuration hors ligne signifie que pour définir les paramètres fonctionnels du BCS, il est nécessaire de basculer le BCS hors ligne, de charger les modifications puis de rebasculer le système en ligne, après la validation des modifications des paramètres.

C.4.4 Configuration en mode simulation

La configuration en mode simulation signifie qu'avant de charger une modification de configuration dans le BCS, il est possible d'effectuer une simulation du système avec les nouveaux paramètres pour apprécier à l'avance l'effet des modifications.

C.4.5 Ressources graphiques

Les ressources graphiques sont des outils logiciels qui viennent en appui des phases d'ingénierie et de configuration. L'architecture du BCS est dessinée à partir d'une bibliothèque d'appareils (cliquer-et-glisser) à l'aide d'un outil graphique afin de définir les échanges de

données et les interconnexions de composants. Il est aussi possible de spécifier des paramètres et des fonctions à l'aide de modes opératoires graphiques (menus déroulants, formulaires, etc.).

C.5 Flexibilité

C.5.1 Capacité de réserve du système

C.5.1.1 Généralités

Après la configuration finale du système, il convient de disposer d'une capacité de réserve pour permettre l'ajout de fonctionnalités ou la mise à niveau du système au fil du temps. La capacité de réserve est installée et disponible uniquement avec la configuration standard.

Il convient que la capacité de réserve du système souhaitée ou nécessaire soit spécifiée dans la conception du système pour les différents sous-systèmes (mémoire, E/S, terminaisons, etc.).

C.5.1.2 Mémoire de réserve

La mémoire de réserve donne la possibilité d'étendre et de modifier le logiciel de commande par la suite. La mémoire de réserve est exprimée en pourcentage de la mémoire disponible totale installée et dépend strictement des applications logicielles mises en œuvre.

Il convient que l'utilisateur indique la mémoire de réserve nécessaire après la configuration finale du système.

C.5.1.3 Extensibilité des communications de la salle de commande

L'extensibilité des communications de la salle de commande définit la possibilité d'ajouter de nouveaux ports de communication et de nouveaux appareils au réseau de commande. Les ports de communication ajoutés peuvent être configurés sans modifications du logiciel existant et sans nécessité de reconfigurer tout le réseau de communication.

C.5.1.4 Extensibilité des communications de terrain

L'extensibilité des communications de terrain définit la possibilité d'ajouter de nouveaux ports de communication et de nouveaux appareils au réseau de terrain. Les ports de communication ajoutés peuvent être configurés sans modifications du logiciel existant et sans nécessité de reconfigurer tout le réseau de communication.

C.5.1.5 Extensibilité des appareils de terrain

L'extensibilité des appareils de terrain est la possibilité d'ajouter de nouveaux appareils de terrain aux fieldbus de communication existants ou la possibilité d'ajouter de nouveaux appareils de terrain aux cartes d'E/S. Il convient d'indiquer le nombre maximum d'appareils de terrain qui peuvent être ajoutés au BCS sans intervention matérielle, et sous la forme du pourcentage des appareils existants.

C.5.1.6 Espace disponible pour les extensions du BCS

Il convient de spécifier l'espace qui doit rester disponible après l'achèvement du BCS. L'espace disponible est indiqué comme pourcentage de l'espace utilisé:

– à l'intérieur de l'armoire de commande, pour l'ajout de nouveaux appareils à l'intérieur;
– dans la salle des armoires, pour l'ajout de nouvelles armoires de commande.

C.5.2 Nombre total d'E/S

Le nombre total d'E/S estimées définit la taille totale du BCS. Les E/S physiques sont divisées en entrées/sorties analogiques/numériques traditionnelles. Si une technologie fieldbus est nécessaire, le nombre total d'appareils intelligents et/ou d'appareils d'entrée/sortie distants connectés au BCS est aussi indiqué.

C.5.3 Nombre d'étiquettes

Une étiquette indique un élément d'information utilisé ou produit par le BCS. Les étiquettes sont souvent regroupées en objets de processus (émetteurs, valves, disjoncteurs, etc.) et divisées en deux catégories:

– étiquettes pour la commande de processus: un ensemble limité d'informations ou de commandes nécessaires à la commande de processus. Par exemple, l'objet de processus «valve» peut inclure les étiquettes suivantes: position de valve, état ouvert/fermé, point de consigne;
– étiquettes pour des fonctions supplémentaires, comme le paramétrage d'appareil à distance, le diagnostic, le paramétrage d'alarme, etc. Ces fonctions sont uniquement possibles avec des appareils intelligents connectés via un fieldbus, et le nombre d'étiquettes concerné peut devenir très élevé.

C.5.4 Nombre de boucles de commande

Une boucle de commande est basée sur l'utilisation d'un régulateur logiciel avec des fonctions PID ou similaires. Le nombre total de boucles donne une idée de la complexité du système, principalement pour les performances logicielles. Il convient que le système soit capable de traiter le nombre total de boucles de commande avec les exigences temporelles spécifiées. Les commandes avancées des fonctions de commande spéciales ne doivent pas être prises en compte à ce stade.

C.5.5 Evolutivité du système

L'évolutivité est la capacité d'un système et/ou d'une application à croître progressivement sans un remplacement total du matériel et du logiciel, et sans la nécessité de repenser toute l'architecture du système.

C.5.6 Extensibilité du système

L'extensibilité du système est la possibilité d'étendre le système sans changer l'architecture et/ou l'équipement employé. L'extensibilité peut concerner à la fois le système entier et chaque appareil.

L'extensibilité d'un système permet d'ajouter au système des composants utilisables.

Pour un composant tel qu'un automate programmable, l'extensibilité signifie qu'il est possible d'ajouter une pièce de rechange utilisable au composant (c'est-à-dire de la mémoire libre ou un processeur dans un automate programmable).

Bibliographie

[1] IEC 60050 (toutes les parties), *Vocabulaire Electrotechnique International* (disponible sur <http://www.electropedia.org>)

[2] IEC 61069-5[3], *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 5: Evaluation de la sûreté de fonctionnement d'un système*

[3] IEC 61131-3, *Automates programmables – Partie 3: Langages de programmation*

[4] IEC 61158 (toutes les parties), *Réseaux de communication industriels – Spécifications des bus de terrain*

[5] IEC 61297, *Systèmes de commande des processus industriels – Classification des régulateurs adaptatifs en vue de leur évaluation*

[6] IEC 61512 (toutes les parties), *Contrôle-commande des processus de fabrication par lots*

[7] IEC 61784 (toutes les parties), *Réseaux de communication industriels – Profils*

[8] Comité de Normalisation Hollandais NPR 5269, *Industrial-process measurement and control. Basic documentation set for process control installations* (disponible en anglais seulement)

[9] IEC TS 62603-1:2014, *Industrial process control systems – Guideline for evaluating process control systems – Part 1: Specifications* (disponible en anglais seulement)

_____

3 Deuxième édition à paraître simultanément avec la présente partie de l'IEC 61069.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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