IEC 61069-5

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 5: Assessment of system dependability

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

IEC 61069-5:2016-06(en-fr)

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de 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 61069-5

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 5: Assessment of system dependability

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-3447-1

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 5: Assessment of system dependability

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61069-5 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1994. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) reorganization of the material of IEC 61069-5:1994 to make the overall set of standards more organized and consistent;
b) IEC TS 62603-1 has been incorporated into this edition.

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

FDIS	Report on voting
65A/793/FDIS	65A/803/RVD

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

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

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

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

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

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

INTRODUCTION

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

Part 1: Terminology and basic concepts

Part 2: Assessment methodology

Part 3: Assessment of system functionality

Part 4: Assessment of system performance

Part 5: Assessment of system dependability

Part 6: Assessment of system operability

Part 7: Assessment of system safety

Part 8: Assessment of other system properties

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

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

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

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

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

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

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

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

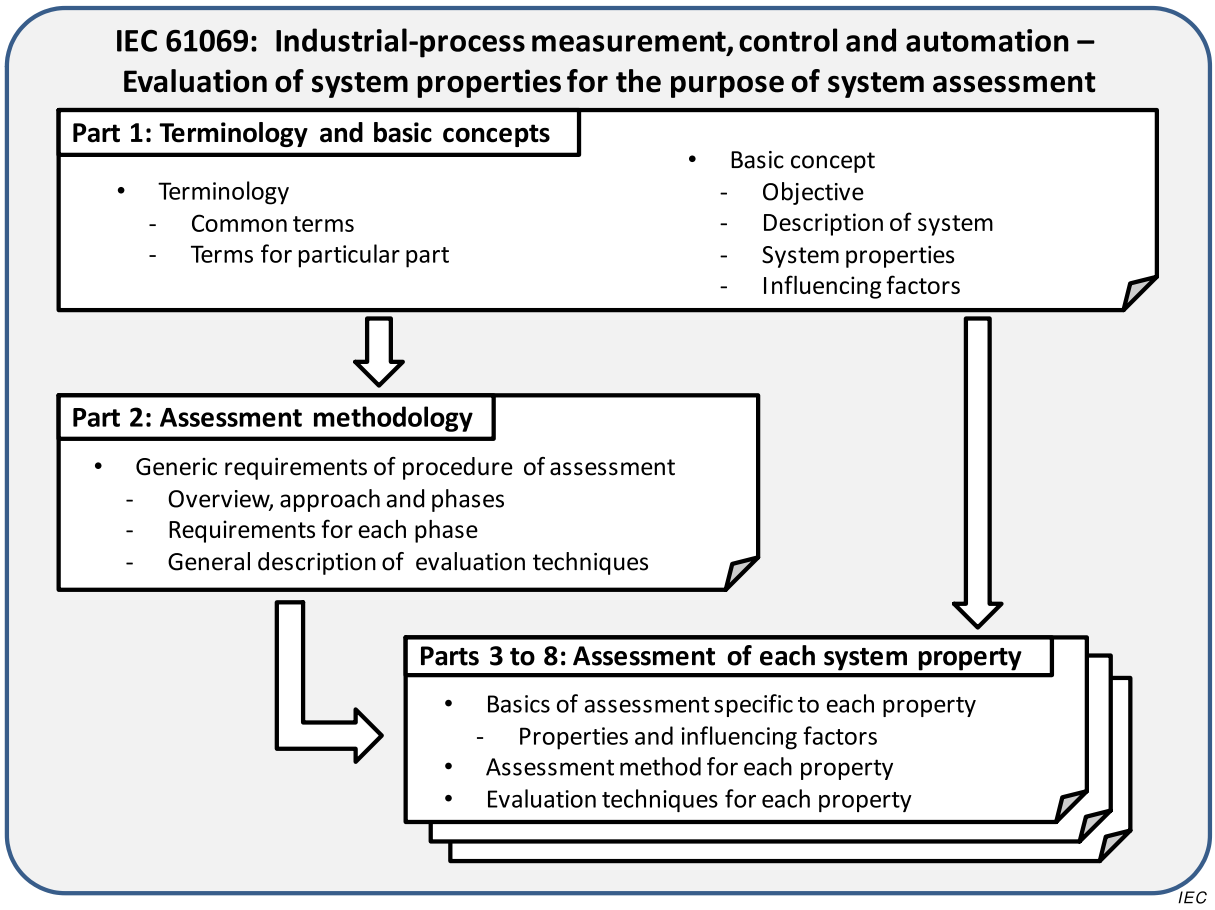

Figure 1 – General layout of IEC 61069

Some example assessment items are integrated in Annex C.

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

Part 5: Assessment of system dependability

1 Scope

This part of IEC 61069:

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

– defines basic categorization of dependability properties,

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

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

2 Normative references

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

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

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

IEC 61069-1:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 1: Terminology and basic concepts*

IEC 61069-2:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

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

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

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

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

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

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

3.1 Terms and definitions

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

3.2 Abbreviated terms, acronyms, conventions and symbols

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

4 Basis of assessment specific to dependability

4.1 Dependability properties

4.1.1 General

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

For a system to be dependable it is necessary that it is ready to perform its functions. However, in practice, when the system is ready to perform its function, this does not mean that it is sure that the functions are performed correctly. In order to cover these two aspects, dependability properties are categorised into the groups and subgroups shown in Figure 2.

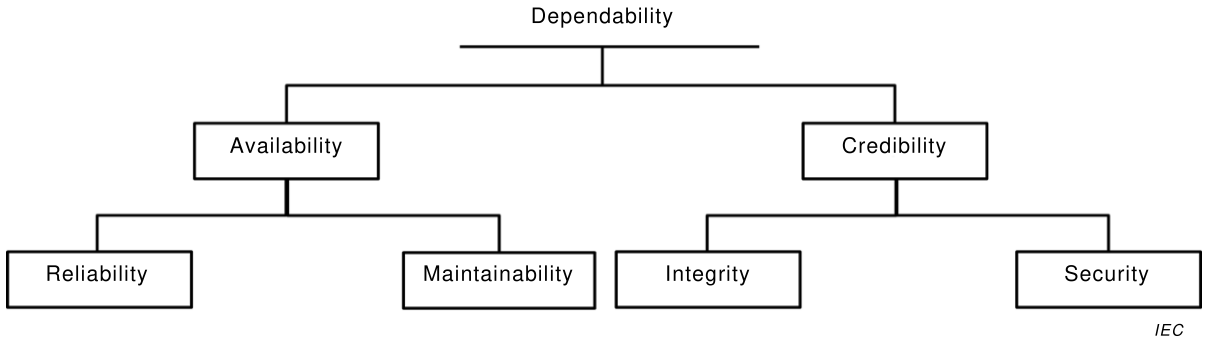

Figure 2 – Dependability

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

The relationship between the dependability properties of the system and its modules is sometimes very complex.

For example:

– if the system configuration includes redundancy, availability property of the system is dependent upon the integrity properties of the redundant modules;
– if the system configuration includes system security mechanisms, security property of the system is dependent upon the availability properties of modules that perform the security mechanism;
– if the system configuration includes modules that check data transferred internally from other parts of the system, then integrity property of the system is dependent upon the security properties of these modules.

When a system performs several tasks of the system, its dependability can vary across those tasks. For each of these tasks, a separate analysis is required.

4.1.2 Availability

Availability of the system is dependent upon the availabilities of the individual modules of the system and the way in which these modules cooperate in performing tasks of the system. The way in which modules of the system cooperate can include functional redundancy (homogeneous or diverse), functional fall-back and degradation. Availability is dependent in practice upon the procedures used and the resources available for maintaining the system. The availability of the system can differ with respect to each of its tasks.

Availability of the system for each task can be quantified in two ways:

A system's availability can be predicted as:

Availability = mean_time_to_failure / (mean_time_to_failure + mean_time_to_restoration)

where:

- "availability" is the availability of the system for the given task;
- "mean_time_to_failure" is the mean of the time from restoration of a system into a state of performing its given task(s) to the time the system fails to do so;
- "mean-time_to_restoration" is the mean of the total time required to restore performance of the given task from the time the system failed to perform that task.

For a system in operation, the availability can be calculated as:

Availability = total_time_the_system_has_been_able_to_perform_the_task / Total_time_the_system_has_been_expected_to_perform_the_task

4.1.3 Reliability

Reliability of a system is dependent upon the reliability of the individual modules of the system and the way in which these modules cooperate in performing task(s) of the system. The way in which these modules cooperate can include functional redundancy (homogeneous or diverse), functional fall-back and degradation.

Reliability of the system can differ with respect to each of its tasks. Reliability can be quantified for individual tasks, with varying degrees of predictive confidence.

The reliability of the individual elements of the system can be predicted using the parts count method (see IEC 62380 and IEC 61069-6). Reliability of the system can then be predicted by synthesis. It should be noted, that for the software modules of systems, there are no reliability prediction methods available that provide high levels of confidence.

Mechanisms to analyse software reliability are described in ISO IEC 25010.

Reliability can be represented by mean time to failure (MTTF) or failure rate.

4.1.4 Maintainability

The maintainability of a system is dependent upon the maintainability of individual elements and structure of elements and modules of the system. The physical structure affects ease of access, replaceability, etc. The functional structure affects ease of diagnosis, etc.

When quantifying the maintainability of a system, all actions required to restore the system to the state where it is fully capable of performing its tasks should be included. This should include actions such as the time necessary to detect the fault, to notify maintenance, to diagnose and remedy the cause, to adjust and check, etc.

The quantification of maintainability should be augmented with qualitative statements by checking the provision for and the coverage of the following items:

The quantification of maintainability should be augmented with qualitative statements by checking the provision for and the coverage of the following items:

– notification of the occurrence of the failures: lights, alert messages, reports, etc.;
– access: ease of access for personnel and for connecting measuring instruments, modularity, etc.;
– diagnostics: direct fault identification, diagnostic tools which have no influence on the system by itself, remote maintenance support facilities, statistical error checking and reporting;
– repairability/replaceability: few restrictions on the replacement of modules while operating (“hot swap” support), modularity, unambiguous identification of modules and elements, minimum need for special tools, minimum repercussions on other elements or modules, when elements or modules are replaced;
– check-out: guided maintenance procedures, minimum check-out requirements.

Maintainability can be represented by mean time to repair (MTTR).

4.1.5 Credibility

The credibility of a system is dependent upon the integrity and security mechanisms implemented as functions performed by the modules of the system.

Credibility mechanisms include:

– a check on
  • correct performance of functions (for example by watchdog, using known data); and/or
  • correct data (for example validity check, parity check, readback, input validation, etc.);
– an action, such as:
  • self-correction;
  • confinement;
  • notification of action, etc.

These mechanisms can be used to provide integrity and/or security.

To analyse the credibility mechanisms, the fault injection techniques described in 6.1 can be used.

Credibility is deterministic and some aspects can be quantified.

4.1.6 Security

The security of a system is dependent upon mechanisms implemented at the boundary of the system to detect and prevent incorrect inputs and unauthorized access. These boundaries can be physical or virtual. See:

– Annex F for more considerations on security, and
– IEC 62443 series.

A security mechanism can be implemented by an element checking the inputs to other elements.

4.1.7 Integrity

The integrity is dependent upon mechanisms implemented at the output elements of the system to check for correct outputs. It also depends upon mechanisms implemented within the system to detect and prevent incorrect transitions of signals or data between parts of the system.

An integrity mechanism is implemented by an element checking the outputs of other elements.

4.2 Factors influencing dependability

The dependability of a system can be affected by the following influencing factors listed in IEC 61069-1:2016, 5.3.

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

– Reliability is influenced by the influencing factors;
  - utilities, the influence is partly predictable using IEC 61709,
  - environment, the influence is partly predictable using IEC 61709,
  - services, due to the handling, storage of parts, etc.
– Maintainability; for the purpose of this standard, maintainability is considered as an intrinsic property of the system itself and is only affected in an indirect way, for example restricted access due to hazardous conditions.
– Availability; when taking into account the human activities necessary to retain the system in, or restore the system to, a state in which the system is capable of performing task(s) of the system, availability is influenced by human behaviour and service conditions (delays in delivery of spare parts, training, documentation, etc.).
– Credibility; the mechanisms (security and integrity) can be affected by intentional or unintentional human actions and by infestations of pests and if these mechanisms share common facilities, such as buses or multitasking processors, they can be influenced by task(s) of the system, the process due to a sudden increase in process activity (for example an alarm burst), etc. and external systems.

In general, any deviations from the reference conditions in which the system is supposed to operate can affect the correct working of the system.

When specifying tests to evaluate the effects of influencing factors, the following standards should be consulted:

– IEC 60068,
– IEC 60801,
– IEC 61000, and
– IEC 61326.

5 Assessment method

5.1 General

The assessment shall follow the method as laid down in IEC 61069-2:2016, 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 61069-2:2016, 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 61069-2:2016, 5.3.

Defining the scope of assessment shall follow the method laid down in IEC 61069-2:2016, 5.3.1.

Collation of documented information shall be conducted in accordance with IEC 61069-2:2016, 5.3.3.

The statements compiled in accordance with IEC 61069-2:2016, 5.3.3 should include the following in addition to the items listed in IEC 61069-2:2016, 5.3.3.

– No additional items are noted

Documenting collated information shall follow the method in IEC 61069-2:2016, 5.3.4.

Selecting assessment items shall follow IEC 61069-2:2016, 5.3.5.

Assessment specification should be developed in accordance with IEC 61069-2:2016, 5.3.6.

Comparison of the SRD and the SSD shall follow IEC 61069-2:2016, 5.3.

NOTE 1 A checklist of SRD for system dependability is provided in Annex A.

NOTE 2 A checklist of SSD for system dependability 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 61069-2:2016, 5.4.

Assessment activities shall be developed in accordance with IEC 61069-2:2016, 5.4.2.

The final assessment program should specify points specified in IEC 61069-2:2016, 5.4.3.

5.5 Execution of the assessment

The execution of the assessment shall be in accordance with IEC 61069-2:2016, 5.5.

5.6 Reporting of the assessment

The reporting of the assessment shall be in accordance with IEC 61069-2:2016, 5.6.

The report shall include information specified in IEC 61069-2:2016, 5.6. Additionally, the assessment report should address the following points:

– No additional items are noted.

6 Evaluation techniques

6.1 General

Within this standard, 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 61069-2:2016, Clause 6.

Factors influencing dependability 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 recommended to assess dependability properties.

Quantitative evaluation can be based on a predictive analysis, calculations, or on tests.

To start the evaluation it is first necessary to analyse the functional and physical structure of the system. Once this is accomplished an analysis of how the tasks are performed by the system should be done.

The structure of the system can be described using functional and physical block diagrams, signal flow diagrams, state graphs, tables, etc.

Failure modes are considered for all elements (hardware and software). Their effects on the dependability of the task(s) of the system, together with the influence of the requirements for maintainability, are determined.

Quantitative evaluations can be performed using one of, or a combination of, the available methods described in 6.2 and 6.3.

The analysis shall include an examination of the manner in which alternative paths through the system are initiated, i.e.:

– in a static manner by changing the system configuration; or
– dynamically, either automatically, for example, by credibility mechanisms or manually, for example, by a keyboard action.

A list of items that shall be considered for the assessment can be found in IEC 60319 and IEC 61709. The analytical techniques, described below, are based on models. Such models can rarely represent the real system exactly, and, even if they can, there can never be 100 % certainty that they do. The evaluation results based on analytical techniques should therefore also state their confidence level.

The dependability of a system is also influenced by errors introduced into the system during the design, specification and manufacturing stages. This holds equally well for the hardware and software of the system. These errors can only be discovered by meticulously checking the proper execution of each function.

In addition, injecting hypothetical faults or errors is a valuable technique in providing an increase in the degree of confidence in the final dependability of the system, as achieved during all stages of the design, specification and manufacturing. These fault injection techniques can be accomplished by using hardware and/or specially designed software. They are used to discover what the overall consequence, to the task(s) of the system, will be.

It should however be recognized that, in practice, the increase in confidence is limited since the number of tests that can be designed and carried out will be constrained by the number of all possible errors and faults that can be thought of and injected.

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

6.2 Analytical evaluation techniques

6.2.1 Overview

This subclause discusses common analytical evaluation techniques: logical analysis (inductive and deductive) and predictive evaluation.

6.2.2 Inductive analysis

At the component or element level the failure modes are identified and for each of these modes the corresponding effect on the dependability of the system task(s) at the next higher level is analysed. The resulting failure effects become the failure modes at the next higher level.

This "bottom-up" approach is a tedious method which finally results in the identification of the effects at all levels of the system of all postulated failure modes.

An appropriate inductive analysis method is described in IEC 60812.

6.2.3 Deductive analysis

Deductive analysis proceeds from a hypothetical failure at the highest level in the system, i.e. the failure of a task, to successively lower levels.

The next tower level is analysed to identify failure modes and associated failures, which would result in the identified failure at the highest level, i.e. the task level.

The analysis is repeated by tracking back through the functional and physical paths of the system until the analysis yields sufficient information in terms of dependability (including maintainability) for the assessment.

The deductive analysis does not give any information on failure modes that are not postulated as events. It is however very time effective for complex systems, for which it is more convenient to describe what is considered a system failure or success, than to consider all the possible failure modes of the constituent elements of the system.

An appropriate deductive analysis method is described in IEC 61025.

6.2.4 Predictive evaluation

A predictive evaluation is based on a qualitative analysis complemented with quantification of the basic reliability (failure rates) of the elements. To quantify the failure rate of the system to perform its task(s), a predictive analysis method is required. An appropriate method is described in IEC 61078.

A reliability block diagram can be constructed almost directly from the functional and physical structure of the system. The method is primarily oriented towards success analysis (two-state) and does not deal effectively with complex repair and maintenance strategies nor with multi-state situations.

Various mathematical tools are available in support of the calculation of the failure rates such as boolean algebra, truth tables and/or path and cut set analysis. To predict quantitatively failure rates of a system to perform its task in a multi-state situation, an analysis method such as described in IEC 61165 may be used.

The Markov analysis method, however, becomes very complex if a large number of system states are to be considered. In such cases it is more effective to apply the Markov analysis to calculate reliability data for subsets of analysis models derived with one of the other analysis methods, such as "fault tree analysis".

Basic quantified failure rate data for the modules and elements used in the above analysis methods can be obtained from field experience or via a calculation method "parts count reliability prediction" using generic data for the components of the modules and elements. The parts count reliability prediction method is described in IEC 61709.

To account for stress levels due to influencing factors, the method described in IEC 61709 and the information listed in Annex A should be used.

The parts count method is based on the assumption that the components are functionally connected in series (worst case estimate). The components of the modules of the system and elements are listed per module or element, stating for each component its type, its appropriate failure rate, the factors influencing the failure rate (part quality, environment, etc.) and the number used.

Alternatively generic failure data may be found in the references contained in Annex E.

For complex systems, such as BCSs, it is impossible in practice to make an accurate predictive assessment of the dependability properties.

The system properties, maintainability, security, and integrity, depend mainly on the features designed into the system, and hence the degree of their existence cannot be calculated in a probabilistic manner. The reliability of the elements used to assure security and integrity shall be considered. The methods used to assess the reliability of these elements may be the same as those used for the elements and modules supporting the primary system functions.

6.3 Empirical evaluation techniques

6.3.1 Overview

To rely solely upon system-level testing to measure reliability and availability for a complex system is neither practical nor cost-effective. In general, complex systems are unique (number of samples equals one). Furthermore, the coverage of such tests will of necessity be severely constrained by the time allowed for the tests. However, for systems which are already in operation such tests provide valuable information.

The actual data obtained in this way is useful for:

– guiding improvement of future designs, structure of system, redesign or replacement of failure prone equipment and software;
– comparison of expected or specified characteristics with actual data;
– generating field data that can be used for future dependability predictions.

Guidance on procedures that shall be followed for defining test can be found in IEC 61070 and IEC 60300-3-2.

The main objective of performing tests on systems is to evaluate the behaviour of a system on the occurrence of a fault (hardware and software) or of an unauthorized or incorrect input (integrity and security).

To observe the behaviour of a system, a representative task or set of tasks shall be defined and for each task those system states that are considered to be a failure shall be defined (for example state of the output(s)). Guidance on the treatment of these tests can be found in IEC 60706-4.

6.3.2 Tests by fault-injection techniques

Prior to testing by fault injection, the system specification should be examined to determine:

– the integrity measures taken to avert the propagation of faults through the system;
– the security measures taken to avert the intrusion of faulty or unauthorized inputs; the diagnostic features provided.

To be time-effective, the design of system tests should be based on a qualitative analysis and, as far as possible, should use the diagnostic features provided by and for the system. Care should be taken that, where these diagnostic features are necessary to provide the system dependability, these themselves should be tested independently.

To test integrity, faults can be injected into module(s), element(s) and/or component(s). Observations are then made to determine if:

– the system outputs fail; and/or
– notice is given of the fault.

To test security, faults can be injected or unauthorized information entered at the system boundaries, i.e. incorrect inputs, human error in operation and/or maintenance activities.

Care should be taken to include some simultaneous tests of both integrity and security. The result of some faults can be the lack of detection of the fault, i.e. an undetectable fault. Therefore care should be taken to include some simultaneous tests of both integrity and security. Annex D lists a number of faults which may be introduced when executing these tests.

6.3.3 Tests by environmental perturbations

Some perturbations of the influencing factors can trigger the security mechanisms.

Therefore, selected influencing factors should be varied around their normal values to test the security mechanisms.

For the selection of the influencing factors refer to 4.2.

6.4 Additional topics for evaluation techniques

No additional items are noted.

Annex A
(informative)

Checklist and/or example of SRD for system dependability

The system requirements document should be reviewed to check that for each of the system tasks the following are clearly stated:

– the relative importance of the task;
– the definition of what is considered to be a failure of the task;
– the criteria of the failure in terms of the dependability properties;
– the operational and operating environment.

The specification of a failure in quantitative or qualitative terms should follow a format defined before the evaluation and assessment begins.

Annex B
(informative)

Checklist and/or example of SSD for system dependability

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 61069-2:2016, Annex B.

B.2 Check points for system dependability

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

– the system functions supporting each task and the modules and elements, both hardware and software, supporting each of these functions;
– the alternative routes supported by the system to perform each task and how these alternative routes are activated;
– credibility mechanisms (security and integrity) provided and how these are supported;
– reliability and availability of each task as well as of the supporting functions, modules and elements;
– maintainability characteristics;
– operational and environmental characteristics and limits of use for the modules and elements.

Annex C
(informative)

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

C.1 Overview

Annex C provides some examples about influencing factors related to this standard which were extracted from IEC TS 62603-1.

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

C.2 Dependability

Dependability cannot be described by a single number. Some of its properties can be expressed as probabilities, other properties are deterministic; some aspects can be quantified, other aspects can only be described in a qualitative way.

When a system performs several tasks of the system, its dependability may vary across those tasks. For each of these tasks, a separate analysis is required.

C.3 Availability

C.3.1 System self-diagnostics

System self-diagnostics allow one to rapidly recognize the failure and thus reduce the mean time to repair. For that reason, assessors should consider the systems self-diagnostic capabilities at all levels of the system.

It could be necessary to implement self-diagnostic routines for the basic components of the BCS, such as the I/O cards or modules, the processor card, the memory cards and the communication links.

The self-diagnostic of field devices should be implemented in the control logic to actuate safety or recovery actions in case of field errors. Self-diagnostic of other components of the BCS are a part of the alarm management system.

C.3.2 Single component fault tolerance and redundancy

C.3.2.1 Overview

Fault tolerance is the built-in capability of a system to provide the continued, correct execution of its assigned function(s) in presence of a hardware or software failure of a single component. In other words, the system is able to perform its mission even after the first failure (hardware or software).

C.3.2.2 Redundancy criteria

When specifying a control system, the effects of component failure should be assessed in relation to the controlled process, and redundancy should be requested accordingly.

Redundancy should cover components that are critical or vital for proper and safe operation of the entire system. When defining redundancy criteria, the following requirements should be addressed, when applicable according to the type of component:

– the type of stand-by, if any,
– the management of the software and data back-up between the redundant components;
– redundancy policy (1-out-of-2, 2-out-of-3, k-out-of-m);
– synchronization of data between the active and the stand-by machines;
– configuration of the active and stand-by machine.

It is particularly useful to examine the availability of fault-tolerance and/or redundancy in:

– power supplies including UPS backup;
– I/O modules;
– I/O networks between I/O modules and controllers;
– controllers;
– control networks linking controls, workstations and other components;
– operator workstations, for example, can replace any workstation;
– servers.

Characteristics of importance include:

– bumpless failover;
– failover time (time when a service is not available);
– failure modes (can some modes of failure cause both the primary and secondary to be lost).

C.3.3 Redundancy methods

C.3.3.1 General

Availability of the system depends upon the availabilities of the individual parts of the system and the way in which these parts cooperate in performing the tasks of the system. The way in which parts cooperate may include:

– functional redundancy (homogeneous or diverse): the redundancy of a specific function can be obtained using the same hardware both for the master and the stand-by (homogeneous) or with independent hardware (diverse). If functional redundancy is available, the first failure does not reduce the functionalities and the performances of the system;
– functional fall-back: is the capacity of returning to a known functional level or mode in case of failure or abnormal operation;
– degradation: in case of failure of a part of the BCS, the performances and the functionalities of the system are reduced. In degraded working condition all the critical functions are properly working.

Availability depends upon the procedures used and the resources available for maintaining the system. Availability requirements are usually expressed as the accumulated down times occurring over a certain period of time. Different availability values are possible for different tasks of the BCS.

In addition to the desired downtime, further special needs, if any, for increasing the availability of some critical functions should be specified in terms of component redundancy.

C.3.3.2 Admissible degraded conditions

Because of faults in the system, the entire system cannot achieve all the functions that represent its mission. If degraded working conditions are admissible, it is possible to keep the process and the system running even if one or more functions abort. It is necessary to identify which are the functions that are not critical for the operation of the system and that can be lost in degraded conditions. The capacity of operating in degraded conditions increases the availability of the BCS.

C.3.3.3 Stand-by configurations

If some critical components are redundant, it is necessary to define the stand-by configuration. Basically, there are two possible stand-by configurations:

– hot stand-by: the primary and the back-up components or systems run simultaneously. Data, if the component should process data, are mirrored to the back-up component in real-time so that the two components are identical. The system can perform a hot swap between the primary and the back-up component without losing any data;
– cold stand-by: in this configuration the back-up component is called up only when the primary component fails. Data, if needed, are mirrored in the back-up component with an update rate lower than in the case of the hot stand-by. This configuration is used for non-critical applications.

Intermediate solutions between hot and cold stand-by may exist, and are sometime referred as “warm stand-by”.

C.3.3.4 Protection action in fail-safe mode

The concept of fail-safe is a protection against the effect of failure of equipment. The fail-safe mode refers to the capacity to switch into a predetermined safe state when a specific malfunction occurs. For performing a fail-safe protection, it is necessary to define the fail-safe devices (i.e. components, systems, control devices, etc.) that are designed so that they set the controlled parameters in a predetermined (safe) condition when a failure is detected.

It should be defined the actions that a fail-safe device implements when it is requested to act as fail-safe device. For example, for a fail-safe valve, the protection action can be the open or the close position.

C.3.3.5 Hot swappable components

Each component of the BCS is hot swappable if it can be removed and substituted while the BCS is operating. The BCS automatically configures the new component as previously configured the removed one. Hot-swap is possible both with faulted components, and with sound ones. The hot swap capability is often required for critical components, whose failure might jeopardize one or more functions of the BCS. For this reason, hot swappable components usually have an installed back-up. The BCS technical specification should indicate the critical components that need a hot swap (if any).

C.4 Reliability

Reliability of a system depends upon the reliability of the individual parts of the system and the way in which these parts cooperate in performing the system task(s). The way in which parts cooperate may include functional redundancy (homogeneous or diverse), functional fallback and degradation. Reliability of the system may differ with respect to each of its tasks. Reliability can be quantified for individual tasks, with varying degrees of predictive confidence. The reliability of the individual hardware parts of the system can be predicted using the parts count method (see IEC 62380). Reliability of the overall system can be calculated by analytical tools and methods (see IEC 61078 and IEC 61025). It should be noted that for the software modules of systems, there are no reliability prediction methods available that provide high levels of confidence.

C.5 Maintainability

C.5.1 General

Maintainability is the ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.

C.5.2 Generation of maintenance requests

The system can generate maintenance requests if the operating status of a component changes. The capacity of generating a maintenance request is a way towards the preventive-predictive maintenance; devices or sub-systems recognize autonomously the need for a repair intervention before failures arise. This capacity is mainly related to intelligent field devices such as analytical instruments, valve positioners, etc.

C.5.3 Strategies for maintenance

Different strategies for maintenance exist, as reported in the following:

– corrective maintenance: response to existing fault and diagnostic messages. Maintenance means here to repair or replace the faulted element;

– preventive maintenance: appropriate maintenance measures are initiated before a failure occurs. Maintenance means here to perform a time-dependant or status-dependant repair or replace policy;

– predictive maintenance: predictive diagnostics for timely detection of potential problems and to determine the remaining service life. Maintenance means here to schedule appropriate repair or substitution interventions based on measured data.

In the definition of the requirements, the requested strategies for maintenance should be defined.

C.5.4 System software maintenance

According to ISO IEC 14764, the software maintenance is the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.

The BCS software maintenance includes the installation of patches, upgrades or new releases of firmware.

The user should require a service of software upgrade from the contractor. This service includes any new release (major or minor, depending on the contract) or patch that is developed by the contractor during the service period.

The software upgrade service can be limited to the sole delivery of the new releases and patches, or can also include the installation of the upgraded software on the system itself.

The contractor should notify the user about the compatibility of all major official operating system patches or security updates with the system. If required, the user should include in the software upgrade service also the installation of the official operating system patches and security updates.

C.6 Credibility

Credibility depends:

– on the ability of the system to provide warning should it fail into a state in which it is not able to perform some or all of its functions correctly (integrity);
– on the ability of the system to reject any incorrect inputs or unauthorized access to the system (security).

C.7 Security

See Annex F.

C.8 Integrity

C.8.1 General

The following C.8.2 to C.8.10 discuss some of the items to investigate with regard to integrity of the data processed by the system.

C.8.2 Hot-swap

Hot-swap for I/O cards or modules should be specified separately, considering the higher stress and rate of failure of these devices.

C.8.3 Module diagnostic

The BCS monitors the operating status of each I/O card or module. Both normal and abnormal operation, e.g. faults or withdrawal, are displayed on the HMI.

C.8.4 Input validation

When a 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.8.5 Read-back function

Analogue and digital outputs of the BCS are sent back to input cards to implement validation logic. For example, this function may be used to verify the emission of open/close commands or the value of emitted set-points.

C.8.6 Forced output

Each digital and/or analogue output is forced to a pre-defined value, singularly settable, in case of faults or abnormal operation.

C.8.7 Monitoring functions

The input cards are designed to detect the most common failures in field, i.e. open or broken circuit.

C.8.8 Controllers

Things to assess include:

– use of error correcting RAM;
– approach to fault-tolerance / redundancy and the resulting data consistency issues, e.g., assurance that no “bad” data can be sent to the field in the event of failure of the primary controller.

C.8.9 Networks

Things to assess include:

– integrity checks on the messages, e.g., error correcting codes;
– timeouts on communications;
– status bits associated “atomically” with value so that application can judge data quality.

C.8.10 Workstations and servers

Things to assess include:

– error correcting RAM.

Annex D
(informative)

Credibility tests

D.1 Overview

The testing by injecting faults into the system provides a useful contribution to assessing the credibility of systems (hardware and software).

These techniques require an in-depth knowledge by the test personnel of the system operation and its physical and functional structure and make it often necessary to access the system physically.

The philosophy behind these tests is the following: a credible system should not fail to perform tasks correctly, despite a failure of an element or an attempt on the system through its boundary.

To test this, faults are created (to test integrity) and/or alternatively a non-authorized or wrong operation is introduced (to test security) and the resulting system behaviour (state of the output(s) and/or signalling reporting provided) is observed.

Below are examples of questions that need to be addressed regarding system behaviour:

– are the outputs driven to or frozen into a predefined position when a fault occurs?
– is the keyboard automatically blocked when a screen is not operating correctly?
– how does the system behave when communication is overloaded?
– is signalization provided by the watchdog, alarm, printing facilities, when a fault is injected?

On the basis of a qualitative analysis, a coordinated approach to the tests should be adopted, starting at board level and moving gradually to the integrated circuit pin level to avoid unnecessary work.

In general, single steady faults are introduced. The types of faults injected are, for example:

– board or module removal;
– opening of board connections (most system failures are due to bad connections);
– opening of IC's pins or forcing them to represent a "logic" 0 or 1.

Special arrangements may be required to be able to perform the tests, such as:

– extender boards with switches;
– clamps;
– special test software.

Depending on the depth of the assessment, the method may be time-consuming, but has the advantage that it is easy to implement and that the test facilities required are relatively inexpensive.

NOTE Care and precaution are taken when implementing these tests in order to avoid damage of some of the elements in the system.

D.2 Injected faults

D.2.1 General

Potential failure modes of the systems are classified in 5.2.3 of IEC 60812:2006.

A number of faults are identified in the following subclauses which may lead to a system failure and can be used for simulation.

D.2.2 System failures due to a faulty module, element or component

System failures may result from faults caused by support capabilities, high temperatures, functional capabilities, such as:

– loss of power of single power supply units;
– loss of power of redundant power supply units (active as well as passive unit);
– loss of power to redundant modules, primary as well as secondary side of the power supply module;
– loss of power to single modules and elements;
– loss of communication buses between modules and elements, single and redundant;
– loss of a module or element;
– loss of power to peripheral equipment (screens, keyboards, printers, disk drives, etc.);
– loss of communication to peripheral equipment;
– open- and short-circuits of power lines, communication buses, address lines, input/output lines.

D.2.3 System failures due to human errors

System failures may result from faults caused by incorrect maintenance operations, reconfiguration, software updates, such as:

– mixing-up redundant bus cables;
– setting incorrect address of modules, elements, etc.;
– inserting printed circuit boards in wrong positions;
– inserting printed circuit boards in upside-down positions;
– inserting connectors in upside-down or reverse positions;
– inserting connectors in wrong positions;
– failing to insert connectors after repair;
– reversing the power connections;
– failing to execute a complete or correct initialization or start-up procedure;
– using the same address twice. etc.

D.2.4 System failures resulting from incorrect or unauthorized inputs into the system through the man-machine interface

System failures may result from faults caused by poor training, ergonomics, confusing user interface such as:

– call-up or use of non-existing or incorrect displays, tag-codes, programs or peripherals;
– creating overflow conditions at keyboard or touch screen by introducing a large number of commands in a short time (n-key roll over);
– use of incomplete codes at call-up of displays, tags, etc.

D.3 Observations

When the above faults are injected, the following questions are asked and the responses recorded.

– Which tasks of the system are affected and how are they affected?
  - Will changes of input signals still be detected in all corresponding modules?
  - Do output signals respond to the correct input signals in all modules? Is data presentation to operators still correct?
  - Will commands from operator's stations still be executed correctly?
  - Is the communication functioning correctly, peer-to-peer, to host computer, to operator's stations, to printer, etc.?
  - Is there a temporary loss of operation in any of the modules?
– Did the system report the fault?
  - Automatically, or within a certain period of time?
  - Automatically, after a periodic test?
  - At which level of the system was the fault reported (operator's stations, other element)?
– Did the system provide protective measures to avoid the occurrence of the failure?
  - Is fault propagation prevented?
  - Does the operation continue via a redundant path?
  - Are the tasks of the system degraded?
  - Is the operation continued via back-up facilities; does this degrade the system task(s)?
  - Does the output reach a predefined level in case of the inability of the system to continue correct operation?
– Is on-line repair possible without affecting the system task(s)?
  - Is a fault reported by providing unambiguous information on the failed part?
  - Can defective part(s) be exchanged without affecting or interrupting the operation of other modules or elements of the system?
  - Is the repaired or spare module or element automatically started and functioning correctly after reinsertion in the system?

D.4 Interpretation of the results

To ease the interpretation of the results, the percentage of induced faults is calculated for which:

– the behaviour is correct;
– the signalization is correct.

Although the data cannot be used in an absolute manner, it is of value in comparative situations.

A similar approach is followed for the availability assessment, where the self-testing coverage is calculated as the percentage of faults detected by self-testing.

Annex E
(informative)

Available failure rate databases

E.1 Databases

The following bibliography is a non-exhaustive list, in no particular order, of sources of failure rate data for electronic and non-electronic components. It should be noted that these sources do not always agree with each other, and therefore care should be taken when applying the data.

IEC TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*, Union Technique de l'Éléctricité et de la Communication (www.ute-fr.com). Identical to RDF 2000/Reliability Data Handbook, UTE C 80-810

Siemens Standard SN 29500, *Failure rates of components, (parts 1 to 14)*; Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.

Telcordia SR-332, Issue 01: May 2001, *Reliability Prediction Procedure for Electronic Equipment,* (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06).

EPRD (RAC-STD-6100)*, Electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.

NNPRD-95 (RAC-STD-6200), *Non-electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.

HRD5, *British Handbook for Reliability Data for Components used in Telecommunication Systems,* British Telecom

Chinese Military/Commercial Standard GJB/z 299B, *Electronic Reliability Prediction*, (http://www.itemuk.com/china299b.html)

ISBN:0442318480, *AT&T reliability manual – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors*, AT&T Reliability Manual, Van Nostrand Reinhold, 1990,.

FIDES:January, 2004, *Reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA*. FIDES is available on request at fides@innovation.net.

IEEE Gold book, *The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems,* provides data concerning equipment reliability used in industrial and commercial power distribution systems. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 IEEE (in the US and Canada) +1 732 981 0060 (outside of the US and Canada), FAX: +1 732 981 9667 e-mail: customer.service@ieee.org.

IRPH ITALTEL, *Reliability Prediction Handbook* – The Italtel IRPH handbook is available on request from: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy. This is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed.

PRISM (RAC / EPRD), The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

E.2 Helpful standards concerning component failure

The following standards contain information with regard to component failure.

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

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

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

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60721-1, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*

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

IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

NOTE See Annex D for further information on failure modes of electrical/electronic components.

Annex F
(informative)

Security considerations

F.1 Physical security

Physical security strives to prevent accidental or delibrate destruction by people with access to the equipment. The proposed BPCS should be assessed for its ability to support physical security.

Common physical security assessment points include:

1) access to open data ports on PCs, for example USB, Ethernet, modems, serial ports, etc;
2) equipment placement, for example in cabinets or on tables;
3) access to material within a cabinet, for example key locks, special tools, or simple unlocked latch;
4) access to data about the enclosed equipment, for example temperatures, humidity, and corrosion;
5) access to rack rooms, for example secured entry, monitored space;
6) controls for data changes through the HMI, for example keylocks.

F.2 Cyber-security

F.2.1 General

Although BCS vendors should provide support for cyber-security (including the elimination of known vulnerabilities), ultimately the responsibility for security in operation falls to the user of the equipment.

ISO IEC 27001 and ISO IEC 27002 provide the basis for all cyber-security standards. ISO IEC 27001:2013, Annex A contains eleven clauses numbered from 5 to 15 which provide an outline of what needs to be done. These clauses are by no means exhaustive and an organization may consider that additional control objectives and controls are necessary.

F.2.2 Security policy

The assessment of the cyber-security capabilities of a system should be done within the context of the user's security policy. The security policy should be incorporated into the systems requirements document described in IEC 61069-2 by reference.

Security policies are created to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

F.2.3 Other considerations

ISO IEC 27001:2013, Clause A.10 lists a number of areas against which the applied system should be assessed. For example, the system should be assessed as to how well it supports:

- business continuity management;
- change management, for example ability to document changes and roll them back;
- segregation of duties (roles) and access (permissions), for example supervisor vs. operator; engineer vs. maintenance;

- system planning and acceptance;
- protection against malicious and mobile code, for example anti-virus, anti-spyware, firewalls, patch management, OS upgrades, whitelists, blacklists, etc;
- back up and restore, for example automatic or manual, full or incremental, local or networked, etc;
- media handling, for example open access to all removable media vs. all media ports locked down vs. intelligent handling (only USBs from certain vendors);
- monitoring, for example intrusion protection, intrusion detection, machine health including update status, etc.;
- access control and user management, for example support for which identifiers (something owned (cards), something known (passwords), or something you are (bio signatures), account management (creation, deletion), etc.;
- network access control, for example documented IP ports, firewalls on the network, Ethernet connections disabled when not specifically required;
- operating system access control, for example control of access to command line utilities;
- the consideration of significantly different OS for the BCS from the office systems in the plant to minimise the risk of viruses functioning;
- application and information access control, for example limiting access to certain process control applications to specific roles and limiting non-process control applications to even fewer people;
- mobile computing and teleworking, for example security of the wireless connection, access to mobile devices, control of the applications on the mobile devices;
- cryptographic controls, for example disk drive encryption, message encryption, etc.
- security in development and support processes, i.e., does the vendor have a define security design lifecycle policy and is it followed;
- technical vulnerability management;
- information security incident management;
- business continuity management;
- compliance with legal requirements.

Bibliography

IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

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

IEC 60050-192:2015, *International Electrotechnical Vocabulary – Part 192: Dependability*

IEC 60068 (all parts), *Environmental testing*

IEC 60605-1:1978, *Equipment reliability testing – Part 1: General requirements*[1]

IEC 60605-2:1994, *Equipment reliability testing – Part 2: Design of test cycles*

IEC 60605-3 (all parts), *Equipment reliability testing – Part 3: Preferred test conditions*[2]

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60605-6:2007, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

IEC 60605-7:1978, *Equipment reliability testing – Part 7: Compliance test plans for failure rate and mean time between failures assuming constant failure rate*[3]

IEC 60706-4, *Guide on maintainability of equipment – Part 4: Section 8: Maintenance and maintenance support planning*[4]

IEC 60801 (all parts), *Electromagnetic compatibility for industrial-process measurement and control equipment*[5]

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61069-6, *Industrial-process, control measurement and automation – Evaluation of system properties for the purpose of system assessment – Part 6: Assessment of system operability*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

---

1 This publication was withdrawn and replaced by IEC 60300-3-5:2001.

2 This series was withdrawn.

3 This publication was withdrawn and replaced by IEC 61124:1978.

4 This publication was withdrawn and replaced by IEC 60300-3-14.

5 This series was withdrawn.

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61165, *Application of Markov techniques*

IEC 61326 (all parts), *Electrical equipment for measurement, control and laboratory use – EMC requirements*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

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

ISO IEC 14764, *Software Engineering – Software Life Cycle Processes – Maintenance*

USA Military Standardization Handbook MIL-HDBK-217 issues A through F, *Reliability prediction of electronic equipment*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

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

AVANT-PROPOS

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

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

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

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

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

Le texte de cette norme est issu des documents suivants:

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

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

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

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

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

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

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

INTRODUCTION

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

Partie 1: Terminologie et principes de base

Partie 2: Méthodologie à appliquer pour l'évaluation

Partie 3: Evaluation de la fonctionnalité d'un système

Partie 4: Evaluation des caractéristiques de fonctionnement d'un système

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

Partie 6: Evaluation de l'opérabilité d'un système

Partie 7: Evaluation de la sécurité d'un système

Partie 8: Evaluation des autres propriétés d'un système

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

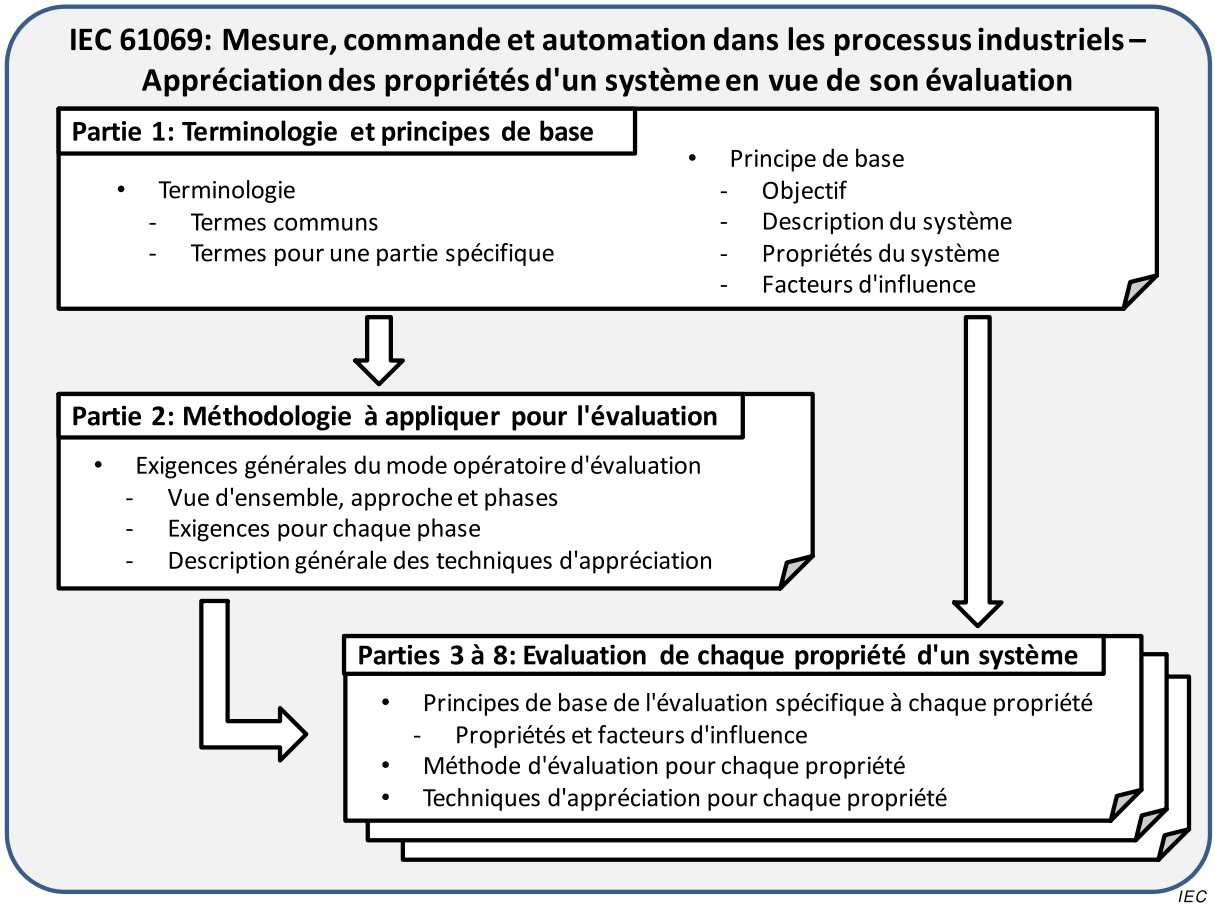

Figure 1 – Structure générale de l'IEC 61069

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

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

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

1 Domaine d'application

La présente partie de l'IEC 61069:

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

– définit la classification de base des propriétés de la sûreté de fonctionnement;

– décrit les facteurs ayant une influence sur la sûreté de fonctionnement et dont il faut tenir compte lors de l'appréciation de la fonctionnalité, et

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

2 Références normatives

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

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

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

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

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

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

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

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

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

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

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

3.1 Termes et définitions

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

3.2 Abréviations, acronymes, conventions et symboles

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

4 Principes de base de l'évaluation spécifique à la sûreté de fonctionnement

4.1 Propriétés de la sûreté de fonctionnement

4.1.1 Généralités

Pour évaluer totalement la sûreté de fonctionnement, les propriétés du système sont classées de façon hiérarchique.

Pour qu'un système soit sûr, il est nécessaire qu'il soit prêt à exécuter ses fonctions. Toutefois, en pratique, lorsque le système est prêt à exécuter ses fonctions, cela ne signifie pas obligatoirement que les fonctions sont correctement exécutées. Pour pouvoir aborder ces deux aspects, les propriétés de sûreté de fonctionnement sont classées en groupes et sous-groupes présentés dans la Figure 2.

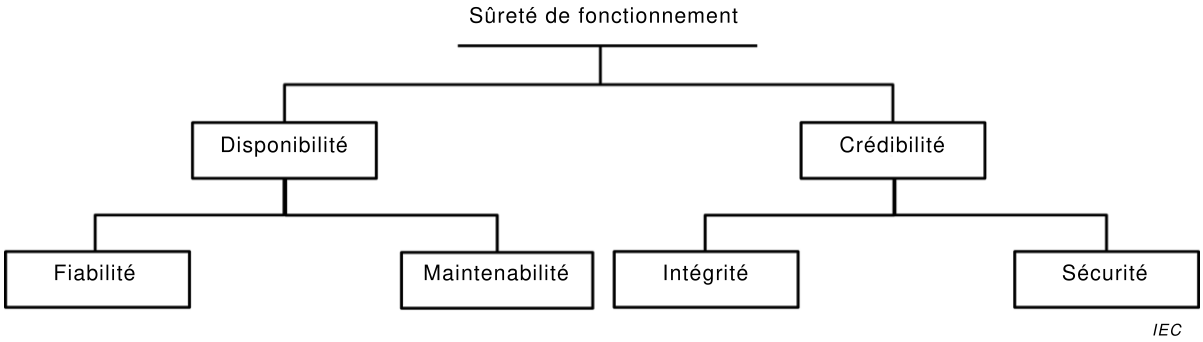

Figure 2 – Sûreté de fonctionnement

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

La relation entre les propriétés de la sûreté de fonctionnement du système et ses modules est parfois très complexe.

Par exemple:

– si la configuration du système comprend une fonction de redondance, la propriété de disponibilité du système dépend des propriétés d'intégrité des modules redondants;

– si la configuration du système inclut des mécanismes de sécurité du système, la propriété de sécurité dépend des propriétés de disponibilité des modules qui exécutent le mécanisme de sécurité;
– si la configuration du système comprend des modules qui assurent la vérification du transfert interne des données provenant des autres composants du système, alors la propriété d'intégrité du système est fonction des propriétés de sécurité de ces modules.

Lorsqu'un système exécute plusieurs tâches du système, sa sûreté de fonctionnement peut varier en fonction de ces tâches. Pour chacune de ces tâches, il est nécessaire de réaliser une analyse indépendante.

4.1.2 Disponibilité

La disponibilité du système est fonction des disponibilités des modules individuels du système et de la manière dont ces modules coopèrent en exécutant les tâches du système. La manière dont les modules du système coopèrent peut inclure une redondance fonctionnelle (homogène ou diversifiée), un mode de secours fonctionnel et un autre dégradé. En pratique, la disponibilité dépend des modes opératoires utilisés et des ressources disponibles pour maintenir le système. La disponibilité du système peut différer pour chacune de ses tâches.

La disponibilité de chaque tâche peut être quantifiée de deux façons.

Il est possible de prévoir la disponibilité du système de la manière suivante:

Disponibilité = durée moyenne avant défaillance / (durée moyenne avant défaillance + durée moyenne de rétablissement)

où:

- la «disponibilité» représente la disponibilité du système pour la tâche donnée;
- la «durée moyenne avant défaillance» représente le délai moyen entre le rétablissement d'un système en état d'exécuter sa ou ses tâche(s) et la défaillance de ce système;
- la «durée moyenne de rétablissement» représente la durée totale nécessaire au rétablissement des performances de la tâche donnée après la défaillance du système.

Pour un système en fonctionnement, il est possible de calculer la disponibilité de la manière suivante:

Disponibilité = durée totale pendant laquelle le système a été capable d'exécuter la tâche / durée totale pendant laquelle on a attendu du système qu'il exécute la tâche

4.1.3 Fiabilité

La fiabilité du système est fonction de la fiabilité des modules individuels du système et de la manière dont ces modules coopèrent en exécutant la ou les tâches du système. La manière dont ces modules coopèrent peut inclure une redondance fonctionnelle (homogène ou diversifiée), un mode de secours fonctionnel et un autre dégradé.

La fiabilité du système peut différer pour chacune de ses tâches. Il est possible de quantifier la fiabilité des tâches individuelles selon des niveaux variables de confiance prévisionnelle.

La fiabilité des composants individuels du système peut être prévue à l'aide de la méthode du dénombrement des composants (voir l'IEC 62380 et l'IEC 61069-6). Il est ensuite possible de prévoir la fiabilité du système au moyen d'une synthèse. Il convient de noter qu'il n'existe actuellement aucune méthode de prévision de la fiabilité des modules logiciels permettant d'obtenir des niveaux élevés de confiance.

Les mécanismes d'analyse de la fiabilité des logiciels sont décrits dans l'ISO IEC 25010.

La fiabilité peut être représentée par la durée moyenne avant défaillance (MTTF) ou par le taux de défaillance.

4.1.4 Maintenabilité

La maintenabilité d'un système est fonction de la maintenabilité des éléments individuels ainsi que de la structure des éléments et des modules du système. La structure physique affecte la facilité d'accès, la remplaçabilité, etc. La structure fonctionnelle affecte la facilité d'exécution du diagnostic, etc.

Lorsque la maintenabilité d'un système est quantifiée, il convient que toutes les actions requises pour rétablir l'état de pleine capacité d'exécution des tâches du système soient incluses. Il convient d'inclure les actions telles que la durée nécessaire pour détecter le défaut, initier une opération de maintenance, diagnostiquer et corriger la cause, régler et vérifier, etc.

Il convient que la quantification de la maintenabilité soit complétée par des rapports qualitatifs relatifs à la fourniture et la couverture des éléments suivants:

Il convient que la quantification de la maintenabilité soit complétée par des rapports qualitatifs relatifs à la fourniture et la couverture des éléments suivants:

– notification de l'occurrence des défaillances: témoins, messages d'alerte, rapports, etc.;
– accès: facilité d'accès du personnel et de la connexion des instruments de mesure, de la modularité, etc.;
– diagnostics: identification directe des défauts, instruments de diagnostic n'ayant aucune influence sur le système à proprement parler, installations de support de maintenance à distance, vérification des erreurs statistiques et rédaction de rapports;
– réparabilité/remplaçabilité: peu de restrictions concernant le remplacement des modules en cours de fonctionnement (support des «échanges à chaud»), modularité, identification claire des modules et des éléments, besoin minimum en outils spéciaux, répercussions minimales sur les autres éléments ou les modules, lors du remplacement des éléments ou des modules;
– vérification: modes opératoires de maintenance guidés, exigences de vérification minimales.

La maintenabilité peut être représentée par la durée moyenne de réparation (MTTR).

4.1.5 Crédibilité

La crédibilité d'un système est fonction des mécanismes d'intégrité et de sécurité mis en œuvre en tant que fonctions exécutables par les modules du système.

Les mécanismes de crédibilité comprennent:

– une vérification:
  - de l'exécution appropriée des fonctions (par exemple par chien de garde, à l'aide de données connues); et/ou
  - de l'exactitude des données (par exemple vérification de la validité, de la parité, collationnement, validation des entrées, etc.);
– une action telle que:
  - l'auto-correction;
  - le confinement;
  - la notification d'actions, etc.

Ces mécanismes peuvent être utilisés pour assurer l'intégrité et/ou la sécurité.

Pour analyser les mécanismes de crédibilité, les techniques d'injection de défauts décrites en 6.1 peuvent être utilisées.

La crédibilité est un concept déterministe et certains de ses aspects peuvent être quantifiés.

4.1.6 Sécurité

La sécurité d'un système est fonction de mécanismes mis en œuvre à la limite du système permettant de détecter et de prévenir les entrées incorrectes et les accès non autorisés. Il peut s'agir de limites physiques ou virtuelles. Voir

– l'Annexe F pour davantage de considérations sur la sécurité, et
– la série IEC 62443.

Un mécanisme de sécurité peut être mis en œuvre par un élément permettant d'assurer la vérification des entrées vers les autres éléments.

4.1.7 Intégrité

L'intégrité est fonction de mécanismes mis en œuvre au niveau des éléments situés en sortie du système, elle permet de vérifier le caractère approprié des sorties. L'intégrité dépend également des mécanismes du système chargés de détecter et de prévenir les transferts incorrects de signaux ou de données entre les composants du système.

Un mécanisme d'intégrité est mis en œuvre par un élément permettant d'assurer la vérification des sorties des autres éléments.

4.2 Facteurs influençant la sûreté de fonctionnement

La sûreté de fonctionnement d'un système peut être affectée par les facteurs d'influence suivants, énumérés en 5.3 de l'IEC 61069-1:2016.

Pour chacune des propriétés de la sûreté de fonctionnement d'un système énumérées en 4.1, les facteurs d'influence principaux sont les suivants.

– La fiabilité est influencée par les facteurs d'influence;
  - les alimentations, l'influence est partiellement prévisible à l'aide de l'IEC 61709;
  - l'environnement, l'influence est partiellement prévisible à l'aide de l'IEC 61709;
  - les services, en raison des activités de manutention, stockage des pièces, etc.
– Maintenabilité; pour les besoins de la présente norme, la maintenabilité est considérée comme une propriété intrinsèque du système à proprement parler, elle peut être affectée uniquement de manière indirecte, par exemple en cas d'accès restreint dû à des conditions dangereuses.
– Disponibilité; selon les activités humaines nécessaires au maintien ou au rétablissement du système dans un état permettant que la ou les tâches soient exécutées, la disponibilité est influencée par le comportement humain et les conditions de service (retard de livraison des pièces de rechange, formation, documentation, etc.).
– Crédibilité; les mécanismes (sécurité et intégrité) peuvent être affectés par des actions humaines délibérées ou accidentelles ainsi que par des infestations d'insectes ravageurs; lorsque ces mécanismes partagent des installations communes telles que les bus ou les processeurs multitâches, ils peuvent être influencés par la ou les tâches du système, par le processus en raison d'une augmentation soudaine de l'activité (par exemple une avalanche d'alarmes), etc. et par les systèmes externes.

De manière générale, tout écart par rapport aux conditions de référence dans lesquelles un système est censé fonctionner peut affecter le fonctionnement correct de ce système.

Lors de la spécification des essais permettant d'apprécier les effets des facteurs d'influence, il convient de consulter les normes suivantes:

– l'IEC 60068,
– l'IEC 60801,
– l'IEC 61000,
– l'IEC 61326.

5 Méthode d'évaluation

5.1 Généralités

L'évaluation doit être effectuée selon la méthode décrite à l'Article 5 de l'IEC 61069-2:2016.

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 61069-2:2016.

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 61069-2:2016.

La définition du domaine d'application de l'évaluation doit être effectuée selon la méthode décrite en 5.3.1 de l'IEC 61069-2:2016.

Le classement des informations détaillées doit être effectué conformément à ce qui est spécifié en 5.3.3 de l'IEC 61069-2:2016.

Il convient que les rapports établis conformément à ce qui est spécifié en en 5.3.3 de l'IEC 61069-2:2016 incluent les éléments suivants, en plus de ceux énumérés en 5.3.3 de l'IEC 61069-2:2016,

– Aucun élément supplémentaire n'est indiqué.

La mise en forme des informations recueillies doit être effectuée selon la méthode décrite en 5.3.4 de l'IEC 61069-2:2016.

La sélection des éléments d'évaluation doit être effectuée selon la méthode indiquée en 5.3.5 de l'IEC 61069-2:2016.

Il convient de développer les spécifications de l'évaluation conformément à ce qui est spécifié en 5.3.6 de l'IEC 61069-2:2016.

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 61069-2:2016.

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

NOTE 2 Une liste de contrôle du CdS destinée à la sûreté de fonctionnement 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 61069-2:2016.

Les activités d'évaluation doivent être développées conformément à ce qui est spécifié en 5.4.2 de l'IEC 61069-2:2016.

Il convient que le programme définitif d'évaluation précise les points spécifiés en 5.4.3 de l'IEC 61069-2:2016.

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 61069-2:2016.

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 61069-2:2016.

Le rapport doit contenir les informations spécifiées en 5.6 de l'IEC 61069-2:2016. De plus, il convient que le rapport d'évaluation aborde également les points suivants:

– aucun élément supplémentaire n'est indiqué.

6 Techniques d'appréciation

6.1 Généralités

Plusieurs techniques d'appréciation sont suggérées dans le cadre de la présente norme. 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 61069-2:2016.

Les facteurs influençant les propriétés de la sûreté de fonctionnement, comme indiqué en 4.2, doivent être pris en compte.

Les techniques données en 6.2, 6.3 et 6.4 sont recommandées pour évaluer les propriétés de la sûreté de fonctionnement.

L'appréciation quantitative peut être fondée sur l'analyse prévisionnelle, le calcul ou les essais.

Pour débuter l'appréciation, il est d'abord nécessaire d'analyser la structure fonctionnelle et physique du système. Ensuite, il convient d'effectuer une analyse de la manière dont les tâches sont exécutées par le système.

La structure du système peut être décrite à l'aide de diagrammes en bloc fonctionnels et physiques, de diagrammes de flux des signaux, de graphiques d'état, de tableaux, etc.

Les modes de défaillance sont pris en compte pour tous les éléments (matériel et logiciel). Leurs effets sur la sûreté de fonctionnement de la ou des tâches du système et l'influence des exigences de maintenabilité sont déterminés.

Il est possible d'effectuer des appréciations quantitatives au moyen d'une ou de plusieurs des méthodes décrites en 6.2 et 6.3.

L'analyse doit inclure un examen de la manière dont les chemins alternatifs sont initiés dans le système, par exemple:

– d'une manière statique en modifiant la configuration du système;
– de manière dynamique, par un moyen automatique, par exemple par le biais de mécanismes de crédibilité ou par un moyen manuel, par exemple par une action du clavier.

Une liste des éléments dont il doit être tenu compte pour l'évaluation peut être consultée dans l'IEC 60319 et l'IEC 61709. Les techniques analytiques décrites ci-dessous sont fondées sur des modèles. De tels modèles peuvent rarement représenter le système réel avec précision, et même si c'était le cas, la certitude ne peut jamais être de 100 %. Il convient donc que les résultats de l'appréciation basés sur les techniques analytiques soient indiqués avec leur niveau de confiance.

La sûreté de fonctionnement d'un système est également influencée par les erreurs introduites dans le système au cours des étapes de conception, de spécification et de fabrication. Ceci est valable tant pour les éléments matériels que pour les éléments logiciels du système. Ces erreurs peuvent être révélées uniquement par une vérification méticuleuse de l'exécution de chacune des fonctions.

En outre, l'introduction de défauts ou d'erreurs hypothétiques constitue une technique pertinente d'augmentation du niveau de confiance de la sûreté de fonctionnement du système, tel qu'obtenu lors de toutes les étapes de la conception, de la spécification et de la fabrication. Ces techniques d'introduction de défauts peuvent être réalisées à l'aide de matériel et/ou d'un logiciel spécialement conçu. Elles peuvent être employées pour révéler quelle sera la conséquence globale par rapport aux tâches du système.

Il convient toutefois de reconnaître qu'en pratique, l'augmentation du niveau de confiance est limitée en raison du fait que le nombre d'essais pouvant être conçus et mis en œuvre est restreint par la quantité de tous les défauts et erreurs potentiels pouvant être introduits.

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

6.2 Techniques d’appréciation analytique

6.2.1 Vue d'ensemble

Le présent paragraphe traite des techniques d'appréciation analytique les plus courantes: analyse logique (inductive et déductive) et prévisionnelle.

6.2.2 Analyse inductive

Les modes de défaillance sont identifiés au niveau des composants ou des éléments, et pour chacun de ces modes, l'effet correspondant sur la sûreté de fonctionnement de la ou des tâches est analysé au niveau supérieur suivant. Les effets de défaillance qui en résultent constituent les modes de défaillance du niveau supérieur suivant.

Cette approche ascendante est une méthode fastidieuse, aboutissant à l'identification des effets de tous les modes de défaillance hypothétiques à tous les niveaux du système.

Une méthode d'analyse inductive appropriée est décrite dans l'IEC 60812.

6.2.3 Analyse déductive

L'analyse déductive part d'une défaillance hypothétique au plus haut niveau du système, par exemple la défaillance d'une tâche, et progresse vers les niveaux successivement inférieurs.

Le niveau suivant est analysé pour identifier les modes de défaillance et les défaillances associées, pour aboutir à la défaillance identifiée au niveau le plus élevé, par exemple le niveau de la tâche.

L'analyse est répétée par retraçage au moyen des chemins physiques et fonctionnels du système jusqu'à ce que l'analyse produise suffisamment d'informations en termes de sûreté de fonctionnement (y compris la maintenabilité) pour permettre l'évaluation.

L'analyse déductive ne fournit aucune information sur les modes de défaillance qui ne sont pas présumés comme étant des évènements. Il s'agit toutefois d'une méthode très efficace en termes de temps pour les systèmes complexes pour lesquels il est plus pratique de décrire ce qui est considéré comme une défaillance ou une réussite du système plutôt que de tenir compte de tous les modes de défaillance possibles des éléments du système.

Une méthode d'analyse déductive appropriée est décrite dans l'IEC 61025.

6.2.4 Appréciation prévisionnelle

Une appréciation prévisionnelle est fondée sur une analyse qualitative complétée par une quantification de la fiabilité de base (taux de défaillance) des éléments. Pour quantifier le taux de défaillance du système dans l'exécution de ses tâches, une méthode d'analyse prévisionnelle est requise. Une méthode appropriée est décrite dans l'IEC 61078.

Il est possible d'élaborer un diagramme de fiabilité presque directement à partir de la structure fonctionnelle et physique du système. La méthode s'oriente principalement vers l'analyse de la stabilité (deux états) et n'aborde pas précisément les stratégies complexes de maintenance et de réparation, ni les situations impliquant plusieurs états.

Divers outils mathématiques sont disponibles pour le calcul des taux de défaillance tels que l'algèbre de Boole, les tables de vérité et/ou l'analyse des chemins et des coupes. Pour prévoir de manière quantitative les taux de défaillance d'un système à exécuter ses tâches dans une situation impliquant plusieurs états, une méthode d'analyse telle que celle décrite dans l'IEC 61165 peut être employée.

La méthode des chaînes de Markov devient très complexe dès qu'il s'agit de tenir compte d'un grand nombre d'états du système. Dans de tels cas, il est plus efficace d'utiliser les chaînes de Markov pour calculer les données de fiabilité des sous-ensembles des modèles d'analyse dérivés avec l'une des autres méthodes d'analyse telle que l'«analyse par arbre de défaillance».

Les données du taux de défaillance quantifié de base des modules et des éléments, utilisées dans les méthodes d'analyse mentionnées ci-dessus, peuvent être obtenues à partir de l'expérience dans des conditions de fonctionnement, ou par une méthode de calcul de «prévision de la fiabilité par le dénombrement des composants» à l'aide de données génériques pour les composants des modules et des éléments. La méthode de prédiction de la fiabilité par le dénombrement des composants est décrite dans l'IEC 61709.

Pour apprécier les niveaux de contrainte dus aux facteurs d'influence, il convient de suivre la méthode décrite dans l'IEC 61709 et d'utiliser les informations mentionnées dans l'Annexe A.

La méthode de dénombrement des composants est fondée sur l'hypothèse selon laquelle les composants sont fonctionnellement connectés en série (estimation de la pire hypothèse). Les composants des modules du système et les éléments sont énumérés par module ou par élément, indiquant le type, le taux de défaillance approprié, les facteurs influençant la défaillance (qualité de la pièce, environnement, etc.) et le nombre utilisé pour chaque composant.

Il est également possible de consulter les données de défaillance générales dans les références contenues en Annexe E.

Pour les systèmes complexes tels que les BCS, il n'est, en pratique, pas possible de réaliser une évaluation prévisionnelle précise des propriétés de la sûreté de fonctionnement.

Les propriétés du système, la maintenabilité, la sécurité et l'intégrité dépendent essentiellement des fonctionnalités dont dispose le système et, par conséquent, leur degré d'existence ne peut pas être calculé de manière probabiliste. La fiabilité des éléments utilisés pour assurer la sécurité et l'intégrité doit être prise en compte. Les méthodes utilisées pour évaluer la fiabilité de ces éléments peuvent être les mêmes que celles employées pour les éléments et les modules de soutien des fonctions primaires du système.

6.3 Techniques d'appréciation empirique

6.3.1 Vue d'ensemble

Le fait de ne compter que sur les essais au niveau du système pour mesurer la fiabilité et la disponibilité d'un système complexe est peu pratique et peu rentable. D'une manière générale, les systèmes complexes sont uniques (le nombre d'échantillons est égal à un). De plus, la réalisation de tels essais est nécessairement très limitée par la durée de ces essais. Toutefois, dans le cas de systèmes déjà en fonctionnement, de tels essais fournissent des informations précieuses.

Les données réelles ainsi obtenues permettent:

– d'orienter l'amélioration des futures conceptions, de la structure du système, de la reconception ou du remplacement du matériel et du logiciel susceptible de subir une défaillance;
– de comparer les caractéristiques attendues ou spécifiées avec les données réelles;
– de générer des données dans des conditions de fonctionnement, pouvant être utilisées pour les futures prévisions de la sûreté de fonctionnement.

Des documents d'orientation sur les modes opératoires qui doivent être suivis pour définir l'essai peuvent être consultés dans l'IEC 61070 et l'IEC 60300-3-2.

L'objectif principal des essais sur les systèmes est d'apprécier le comportement d'un système en cas de défaillance (matérielle ou logicielle) ou d'une entrée incorrecte ou non autorisée (intégrité et sécurité).

Pour observer le comportement d'un système, une tâche représentative ou un ensemble de tâches doit être défini et, pour chaque tâche, les états du système considérés comme des défaillances doivent être également définis (par exemple l'état de la ou des sorties). Il est possible de consulter des documents d'orientation sur le traitement de ces essais dans l'IEC 60706-4.

6.3.2 Essais par techniques d'introduction de défauts

Avant de procéder aux essais par introduction de défauts, il convient d'examiner les spécifications du système pour déterminer:

– les mesures relatives à l'intégrité ayant été prises pour éviter la propagation des défauts dans le système;
– les mesures relatives à la sécurité ayant été prises pour éviter l'intrusion d'entrées anormales ou non autorisées; les fonctionnalités de diagnostic fournies.

Pour être efficaces en termes de temps, il convient que les essais réalisés sur le système soient fondés sur une analyse qualitative et, dans la mesure du possible, qu'ils utilisent les fonctionnalités de diagnostic fournies par et pour le système. Il convient de prêter une attention particulière au fait que ces fonctionnalités de diagnostic sont nécessaires pour assurer la sûreté de fonctionnement du système; il convient de les soumettre à essai de manière indépendante.

Pour vérifier l'intégrité, il est possible d'introduire des défauts dans les modules, les éléments et/ou les composants. Les constatations permettent ensuite de déterminer si:

– les sorties du système sont défaillantes; et/ou
– le défaut est signalé.

Pour vérifier la sécurité, il est possible d'introduire des défauts ou d'entrer des informations non autorisées aux limites du système, c'est-à-dire des entrées incorrectes, une erreur humaine en cours de fonctionnement et/ou des activités de maintenance.

Il convient de veiller à inclure des essais simultanés d'intégrité et de sécurité. Le résultat de certains défauts peut s'avérer être une absence de détection du défaut, c'est-à-dire un défaut indétectable. Il convient donc de veiller à inclure des essais simultanés d'intégrité et de sécurité. L'Annexe D contient une liste des défauts pouvant être introduits lors de l'exécution de ces essais.

6.3.3 Essais par perturbations affectant l'environnement

Certaines perturbations des facteurs d'influence peuvent déclencher les mécanismes de sécurité.

Il convient par conséquent de faire varier les facteurs d'influence sélectionnés autour de leur valeur normale pour soumettre à essai les mécanismes de sécurité.

Pour la sélection des facteurs d'influence, voir 4.2.

6.4 Sujets supplémentaires de techniques d'appréciation

Aucun élément supplémentaire n'est indiqué.

Annexe A
(informative)

Liste de contrôle et/ou exemples de CdC pour la sûreté de fonctionnement d'un système

Il convient d'effectuer une revue du cahier des charges du système afin de s'assurer que pour chacune des tâches du système, les éléments suivants sont clairement indiqués:

– l'importance relative de la tâche;
– la définition de ce qui est considéré comme une défaillance de la tâche;
– les critères de défaillance en termes de propriétés de sûreté de fonctionnement;
– l'environnement opérationnel et d'exploitation.

Il convient que la spécification d'une défaillance en termes quantitatifs ou qualitatifs respecte un format défini avant le début de l'appréciation et de l'évaluation.

Annexe B
(informative)

Liste de contrôle et/ou exemples de CdS pour la sûreté de fonctionnement 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 61069-2:2016.

B.2 Points de contrôle de la sûreté de fonctionnement

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

– les fonctions du système qui supportent chaque tâche, ainsi que les modules et les éléments (matériels ou logiciels) qui soutiennent chacune de ces fonctions;

– les cheminements alternatifs supportés par le système pour exécuter chaque tâche et la manière dont ces cheminements alternatifs sont activés;

– les mécanismes de crédibilité (sécurité et intégrité) fournis et la manière dont ils sont supportés;

– la fiabilité et la disponibilité de chaque tâche ainsi que celles des fonctions, des modules et des éléments qui les supportent;

– les caractéristiques de maintenabilité;

– les caractéristiques opérationnelles et relatives à l'environnement ainsi que leur limite d'utilisation pour les modules et les éléments.

Annexe C
(informative)

Un 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 norme, qui ont été extraits de l'IEC TS 62603-1.

Les classifications des valeurs de propriétés décrites dans la présente norme ne sont qu'indicatives.

C.2 Sûreté de fonctionnement

La sûreté de fonctionnement ne peut pas être décrite par un seul chiffre. Certaines de ses propriétés peuvent être exprimées comme des probabilités, les autres propriétés sont de type déterministe; il est possible de quantifier certains aspects et certains autres ne peuvent être décrits que de manière qualitative.

Lorsqu'un système exécute plusieurs tâches du système, sa sûreté de fonctionnement peut varier en fonction de ces tâches. Pour chacune de ces tâches, il est nécessaire de réaliser une analyse indépendante.

C.3 Disponibilité

C.3.1 Autodiagnostics du système

Les autodiagnostics du système permettent d'identifier rapidement la défaillance et de réduire la durée moyenne de réparation. C'est pour cette raison qu'il convient que l'évaluateur tienne compte des capacités d'autodiagnostic des systèmes à tous les niveaux du système.

Il peut être nécessaire de mettre en œuvre des routines d'autodiagnostic pour les composants de base du BCS, tels que les modules ou les cartes d'E/S, la carte du processeur, les cartes mémoire et les liaisons de communication.

Il convient que la fonction d'autodiagnostic des appareils de terrain soit mise en œuvre dans la logique de commande pour initier les actions de sécurité ou de recouvrement en cas d'erreurs en conditions de fonctionnement. L'autodiagnostic des autres composants du BCS fait partie du système de gestion des alarmes.

C.3.2 Redondance et tolérance aux anomalies d'un composant unique

C.3.2.1 Vue d'ensemble

La tolérance aux anomalies est constituée de la capacité intégrée d'un système à assurer une exécution correcte et continue des fonctions qui lui sont assignées en présence d'une défaillance matérielle ou logicielle d'un seul composant. En d'autres termes, le système est capable d'accomplir sa mission même après la première défaillance (matérielle ou logicielle).

C.3.2.2 Critères de redondance

Lors de la spécification d'un système de commande, il convient que les effets de la défaillance d'un composant soient évalués par rapport au processus commandé, et que la redondance soit requise en conséquence.

Il convient que la redondance couvre les composants critiques ou essentiels au fonctionnement sûr et approprié de l'ensemble du système. Lors de la définition des critères de redondance, il convient de satisfaire aux exigences suivantes, si elles sont applicables au type de composant:

– le type de veille, le cas échéant;
– la gestion de la sauvegarde du logiciel et des données entre les composants redondants;
– la politique de redondance (1 parmi 2, 2 parmi 3, k parmi m);
– la synchronisation des données entre les machines actives et celles en veille;
– la configuration de la machine active et de celles en veille.

Il est particulièrement pertinent d'examiner la disponibilité de la tolérance aux anomalies et/ou la redondance dans:

– l'alimentation, y compris les systèmes d'alimentation sans coupure (ASC);
– les modules d'E/S;
– les réseaux d'E/S entre les modules d'E/S et les régulateurs;
– les régulateurs;
– les réseaux de commande qui relient les commandes, les postes de travail et les autres composants;
– les postes de travail opérateur, par exemple, peuvent remplacer n'importe quel poste de travail;
– les serveurs.

Les caractéristiques importantes comprennent:

– le basculement sans à-coups;
– la durée de basculement (durée d'indisponibilité d'un service);
– les modes de défaillance (certains modes de défaillances peuvent-ils provoquer à la fois la perte des fonctions primaires et secondaires).

C.3.3 Méthodes de redondance

C.3.3.1 Généralités

La disponibilité du système est fonction des disponibilités des composants individuels du système et de la manière dont ces composants coopèrent en exécutant les tâches du système. La manière dont les composants coopèrent peut inclure:

– la redondance fonctionnelle (homogène ou diverse): la redondance d'une fonction spécifique peut être obtenue en utilisant le même matériel pour le matériel maître et celui en veille (homogène) ou avec du matériel indépendant (divers). Si la redondance fonctionnelle est disponible, la première défaillance ne réduit pas les fonctionnalités ni les caractéristiques de fonctionnement du système;
– le mode de secours fonctionnel: exprime la capacité de revenir à un mode ou un niveau fonctionnel minimum en cas de défaillance ou de fonctionnement anormal;
– le mode dégradé: en cas de défaillance d'un composant du BCS, les caractéristiques de fonctionnement et les fonctionnalités du système sont réduites. En conditions de fonctionnement dégradé, toutes les fonctions critiques s'exécutent correctement.

La disponibilité dépend des modes opératoires utilisés et des ressources disponibles pour maintenir le système. Les exigences de disponibilité sont généralement exprimées comme étant les durées cumulées d'indisponibilité survenues au cours d'une période donnée. Il est possible que les valeurs de disponibilité soient différentes pour les diverses tâches du BCS.

En plus de la durée d'indisponibilité souhaitée, il convient de spécifier d'autres besoins spéciaux, le cas échéant, en termes de redondance des composants de sorte à augmenter la disponibilité de certaines fonctions critiques.

C.3.3.2 Conditions dégradées admissibles

En raison de la présence de défauts dans le système, l'ensemble du système ne peut pas exécuter toutes les fonctions constituant sa mission. Si des conditions de fonctionnement dégradées sont admissibles, il est possible de laisser le processus et le système s'exécuter même en cas d'interruption d'une ou de plusieurs fonctions. Il est nécessaire d'identifier les fonctions qui ne sont pas indispensables au fonctionnement du système et qu'il est possible de perdre en conditions dégradées. La capacité de fonctionnement en conditions dégradées augmente la disponibilité du BCS.

C.3.3.3 Configurations de veille

Si certains composants critiques sont redondants, il est nécessaire de définir la configuration de veille. Fondamentalement, il existe deux configurations de veille:

– la reprise immédiate: les systèmes ou composants primaires et de secours tournent simultanément. Les données, s'il convient que le composant traite des données, sont copiées vers le composant de secours en temps réel de sorte que les deux composants soient identiques. Le système peut exécuter un échange à chaud entre le composant primaire et le composant de secours sans aucune perte de données;
– la reprise graduelle: dans cette configuration, le composant de secours est appelé uniquement en cas de défaillance du composant primaire. Les données, si nécessaire, sont copiées dans le composant de secours avec une fréquence de mise à jour inférieure à celle de la reprise immédiate. Cette configuration est utilisée dans les applications non critiques.

Il peut exister des solutions intermédiaires situées à mi-chemin entre la reprise immédiate et graduelle, qui sont parfois désignées par «reprise intermédiaire».

C.3.3.4 Action de protection en mode sécurité intégrée

Le concept de sécurité intégrée constitue une protection contre l'effet d'une défaillance sur le matériel. Le mode de sécurité intégrée désigne la capacité de basculer vers un état de sécurité prédéterminé lorsqu'un dysfonctionnement spécifique se produit. Pour réaliser une protection à sécurité intégrée, il est nécessaire de définir les appareils à sécurité intégrée (c'est-à-dire les composants, systèmes, appareils de commande, etc.) qui sont conçus pour définir les paramètres commandés en condition prédéterminée (de sécurité) lorsqu'une défaillance est détectée.

Il convient de définir les actions qu'un appareil à sécurité intégrée met en œuvre lorsqu'il est amené à agir comme tel. Par exemple, dans le cas d'une vanne à sécurité intégrée, l'action de protection peut correspondre à la position d'ouverture ou de fermeture.

C.3.3.5 Composants échangeables à chaud

Chaque composant du BCS est échangeable à chaud s'il peut être retiré et substitué en cours de fonctionnement du BCS. Le BCS configure automatiquement le nouveau composant avec la même configuration que le composant retiré. L'échange à chaud est possible pour les composants défectueux ou en bon état. La capacité d'échange à chaud est souvent requise pour les composants critiques dont la défaillance est susceptible de compromettre une ou plusieurs des fonctions du BCS. C'est la raison pour laquelle les composants échangeables à

chaud disposent généralement d'une unité de sauvegarde installée. Il convient que les spécifications techniques du BCS indiquent les composants critiques nécessitant un échange à chaud (le cas échéant).

C.4 Fiabilité

La fiabilité du système est fonction de la fiabilité des composants individuels du système et de la manière dont ces composants coopèrent en exécutant les tâches du système. La manière dont ces composants coopèrent peut inclure une redondance fonctionnelle (homogène ou diversifiée), un mode fonctionnel dégradé et de secours. La fiabilité du système peut différer pour chacune de ses tâches. Il est possible de quantifier la fiabilité des tâches individuelles selon des niveaux variables de confiance prévisionnelle. La fiabilité des composants matériels individuels du système peut être prévue à l'aide de la méthode du dénombrement des composants (voir l'IEC 62380). La fiabilité de l'ensemble du système peut être calculée par le biais de méthodes et d'outils analytiques (voir l'IEC 61078 et l'IEC 61025). Il convient de noter qu'il n'existe actuellement aucune méthode de prévision de la fiabilité des modules logiciels permettant d'obtenir des niveaux élevés de confiance.

C.5 Maintenabilité

C.5.1 Généralités

La maintenabilité désigne l'aptitude d'un élément, dans des conditions données d'utilisation, à être maintenu ou rétabli dans un état lui permettant d'exécuter une fonction requise, lorsque la maintenance est réalisée dans des conditions données et au moyen de modes opératoires et de ressources énoncés.

C.5.2 Génération de requêtes de maintenance

Le système peut générer les requêtes de maintenance si le statut de fonctionnement d'un composant est modifié. La capacité à générer une requête de maintenance s'inscrit dans une démarche de maintenance préventive-prévisionnelle; les appareils ou les sous-systèmes reconnaissent le besoin d'une intervention de réparation de manière autonome, avant que la défaillance ne survienne. Cette capacité est principalement reliée aux appareils de terrain intelligents tels que les instruments analytiques, les positionneurs de vanne, etc.

C.5.3 Stratégies de maintenance

Il existe différentes stratégies de maintenance, telles qu'indiquées ci-dessous:

– la maintenance corrective: pour répondre aux messages de défaut et de diagnostic existants. La maintenance désigne ici la réparation ou le remplacement des éléments défectueux;

– la maintenance préventive: des mesures de maintenance appropriées sont initiées avant qu'une défaillance ne survienne. La maintenance désigne ici la réalisation d'une réparation liée au temps ou au statut, ou bien une politique de remplacement;

– la maintenance prévisionnelle: diagnostics prévisionnels destinés à la détection opportune de problèmes potentiels permettant de déterminer la durée de vie en service restante. La maintenance désigne ici la planification appropriée d'une réparation ou d'interventions de substitution fondées sur des données mesurées.

Dans la définition des exigences, il convient de définir les stratégies de maintenance requises.

C.5.4 Maintenance du logiciel du système

Selon l'ISO IEC 14764, la maintenance du système est désignée par la modification d'un produit logiciel après livraison pour corriger les défauts, améliorer les caractéristiques de

fonctionnement ou d'autres attributs, ou pour adapter le produit à un environnement ayant subi des modifications.

La maintenance du logiciel d'un BCS inclut l'installation des correctifs, des mises à niveau ou des nouvelles versions du micrologiciel.

Il convient que l'utilisateur dépose une demande de service de mise à niveau du micrologiciel auprès du fournisseur. Ce service inclut toutes les nouvelles versions (majeures ou mineures, selon le contrat) ou les correctifs développés par le contractant au cours de la période du service.

Le service de mise à niveau du logiciel peut être uniquement restreint à la livraison des nouvelles versions et des correctifs, ou bien il peut également inclure l'installation du logiciel mis à niveau sur le système lui-même.

Il convient que le contractant informe l'utilisateur de la compatibilité avec le système de tous les correctifs majeurs officiels dédiés au système d'exploitation ou des mises à jour de sécurité. Si nécessaire, il convient que l'utilisateur inclue également dans le service de mise à niveau du logiciel, l'installation des correctifs officiels dédiés au système d'exploitation et des mises à jour de sécurité.

C.6 Crédibilité

La crédibilité est fonction de:

– l'aptitude du système à fournir des alertes en cas de panne mettant le système dans un état d'impossibilité d'exécution correcte de certaines ou de toutes ses fonctions (intégrité);
– l'aptitude du système à rejeter toute entrée incorrecte ou tout accès non autorisé au système (sécurité).

C.7 Sécurité

Voir l'Annexe F.

C.8 Intégrité

C.8.1 Généralités

Les Paragraphes C.8.2 à C.8.10 suivantes abordent certains des éléments de recherche relatifs à l'intégrité des données traitées par le système.

C.8.2 Echange à chaud

Il convient que l'échange à chaud des cartes ou modules d'E/S soit spécifié à part, en tenant compte du niveau de contrainte plus élevé et du taux de défaillance de ces appareils.

C.8.3 Diagnostic des modules

Le BCS surveille l'état de fonctionnement de chaque carte d'E/S ou module. En conditions normales et anormales, par exemple en cas de défaut ou de retrait, l'état s'affiche sur l'interface homme-machine (IHM).

C.8.4 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.8.5 Fonction de collationnement

Les sorties analogiques et numériques du BCS sont envoyées vers les cartes d'entrée pour mettre en œuvre la logique de validation. Par exemple, cette fonction peut être utilisée pour vérifier l'émission des commandes ouvert/fermé ou la valeur des points de consigne émis.

C.8.6 Sortie forcée

Chaque sortie numérique et/ou analogique est forcée à une valeur prédéfinie et réglable en cas de défaut ou de fonctionnement anormal.

C.8.7 Fonctions de surveillance

Les cartes d'entrée sont conçues pour détecter les défaillances les plus courantes sur le terrain, c'est-à-dire un circuit ouvert ou interrompu.

C.8.8 Régulateurs

Les éléments à évaluer incluent:

– l'utilisation de mémoire à accès direct (RAM, Random-Access Memory) dédiée à la correction d'erreurs;
– l'approche par rapport à la tolérance aux anomalies / la redondance et les questions liées à la cohérence des données résultantes, par exemple l'assurance qu'aucune «mauvaise» donnée ne peut être émise vers le terrain en cas de défaillance du régulateur primaire.

C.8.9 Réseaux

Les éléments à évaluer incluent:

– les vérifications d'intégrité des messages, par exemple les codes de correction d'erreur;
– les temporisations de communications;
– les bits d'état «atomiquement» associés à la valeur de sorte que l'application puisse juger de la qualité des données.

C.8.10 Postes de travail et serveurs

Les éléments à évaluer incluent:

– la mémoire RAM de correction d'erreurs.

Annexe D
(informative)

Essais de crédibilité

D.1 Vue d'ensemble

Les techniques consistant à introduire des défauts dans le système pour le soumettre à essai contribuent utilement à l'évaluation de la crédibilité des systèmes (matériels et logiciels).

Ces techniques exigent que le personnel d'essai ait une connaissance approfondie du fonctionnement du système et de sa structure physique et fonctionnelle car il est souvent nécessaire d'accéder physiquement au système.

Les principes qui sous-tendent ces essais sont les suivants: il convient qu'un système crédible exécute ses tâches correctement, même en cas de défaillance d'un élément ou de tentative d'entrée erronée aux limites de ce système.

Pour soumettre ce système à essai, des défauts sont créés (pour vérifier l'intégrité) et/ou une opération non autorisée ou incorrecte est introduite (pour vérifier la sécurité) et le comportement du système résultant (état de la ou des sorties et/ou génération d'un rapport de signalisation) est observé.

Des exemples de questions relatives au comportement du système et auxquelles il faut répondre figurent ci-dessous.

– les sorties sont-elles acheminées ou gelées dans une position prédéfinie lorsqu'une défaillance se produit?
– le clavier se bloque-t-il automatiquement lorsque l'écran ne fonctionne pas correctement?
– comment le système se comporte-t-il lorsque le processus de communication est surchargé?
– la signalisation est-elle générée par exemple par la fonction de chien de garde, d'alarme ou les installations d'impression lorsqu'un défaut est introduit?

Sur la base d'une analyse qualitative, il convient qu'une approche coordonnée des essais débutant au niveau de la carte et progressant vers le niveau de la broche du circuit intégré soit adoptée pour éviter un travail inutile.

D'une manière générale, des défauts uniques et réguliers sont introduits. Le type de défaut introduit comprend, par exemple:

– le retrait d'une carte ou d'un module;
– l'ouverture des connexions à la carte (la plupart des défaillances du système sont dues à de mauvaises connexions);
– l'ouverture des broches du circuit intégré (CI) ou le fait de leur imposer une représentation logique de 0 ou 1.

Des dispositions spéciales peuvent être nécessaires à la mise en œuvre des essais telles que:

– des cartes d'extension équipées de commutateurs;
– des attaches;
– un logiciel d'essai spécial.

Selon la profondeur de l'évaluation, la méthode peut s'avérer être longue, mais l'avantage réside dans le fait que sa mise en œuvre est simple et que les installations d'essai nécessaires sont relativement peu coûteuses.

NOTE Des précautions sont prises lors de la mise en œuvre de ces essais, afin d'éviter d'endommager certains des éléments du système.

D.2 Défauts introduits

D.2.1 Généralités

Les modes de défaillance potentiels des systèmes sont classés en 5.2.3 de l'IEC 60812:2006.

Un certain nombre de défauts pouvant conduire à une défaillance du système sont identifiés dans les paragraphes suivants, ils peuvent être utilisés lors des simulations.

D.2.2 Défaillances du système dues à un module, un élément ou un composant défectueux

Les défaillances du système peuvent résulter de défauts causés par les aptitudes du support, des températures élevées, des aptitudes fonctionnelles, telles que:

– perte de puissance des unités d'alimentation uniques;
– perte de puissance des unités d'alimentation redondantes (unités actives et unités passives);
– perte de puissance des modules redondants, du côté primaire et secondaire du module d'alimentation;
– perte de puissance vers les modules et éléments uniques;
– perte des bus de communication entre les modules et les éléments uniques et redondants;
– perte d'un module ou d'un élément;
– perte de puissance d'un équipement périphérique (écran, clavier, imprimantes, disques, etc.);
– perte de la communication vers un équipement périphérique;
– circuits ouverts et courts-circuits sur les lignes d'alimentation, bus de communication, lignes d'adresse, lignes d'entrée/sortie.

D.2.3 Défaillances du système dues à des erreurs humaines

Les défaillances du système peuvent résulter de défauts causés par des opérations de maintenance incorrectes, une reconfiguration, des mises à jour du logiciel telles que:

– la confusion des câbles de bus redondants;
– la définition d'adresse incorrecte pour des modules, des éléments, etc.;
– l'insertion des cartes de circuit imprimé dans une mauvaise position;
– l'insertion des cartes de circuit imprimé dans le mauvais sens;
– l'insertion des connecteurs à l'envers ou dans le mauvais sens;
– l'insertion des connecteurs dans une mauvaise position;
– la non-insertion des connecteurs après réparation;
– l'inversion des connexions électriques;
– l'échec de l'exécution d'une initialisation complète ou correcte ou du mode opératoire de démarrage;
– la même adresse utilisée deux fois, etc.

D.2.4 Défaillances du système résultant d'entrées incorrectes ou non autorisées dans le système par le biais de l'interface homme-machine

Les défaillances du système peuvent résulter de défauts causés par une mauvaise formation, l'ergonomie, une interface utilisateur peu claire, telle que:

– appel ou utilisation d'affichages, de codes étiquettes, de programmes ou de périphériques inexistants ou incorrects;
– création de conditions de débit excessif au niveau du clavier ou de l'écran tactile par l'introduction d'un grand nombre de commandes en un court laps de temps (enchaînement de n touches);
– utilisation de codes incomplets au niveau de l'appel des affichages, des étiquettes, etc.

D.3 Observations

Une fois les défauts ci-dessus introduits, les questions suivantes sont posées et les réponses enregistrées.

– Quelles tâches du système sont affectées et dans quelle mesure le sont-elles?
  - Les changements de signaux d'entrée sont-ils encore détectés dans tous les modules correspondants?
  - Les signaux de sortie répondent-ils aux signaux d'entrée correspondants dans tous les modules? La présentation des données aux opérateurs est-elle toujours correcte?
  - Les commandes provenant des postes des opérateurs sont-elles encore exécutées correctement?
  - La communication fonctionne-t-elle correctement, de grappe à grappe, vers l'ordinateur hôte, vers les postes des opérateurs, vers l'imprimante, etc.?
  - L'un des modules présente-t-il une perte de fonctionnement temporaire?
– Le système a-t-il signalé le défaut?
  - Automatiquement ou dans un certain laps de temps?
  - Automatiquement, après un essai périodique?
  - A quel niveau du système le défaut a-t-il été consigné (postes des opérateurs, autre élément)?
– Le système a-t-il fourni des mesures de protection pour éviter l'occurrence de la défaillance?
  - La propagation du défaut a-t-elle été empêchée?
  - Le fonctionnement se poursuit-il par le biais d'un chemin redondant?
  - Les tâches du système sont-elles dégradées?
  - Le fonctionnement se poursuit-il par le biais des installations de secours; cela dégrade-t-il la ou les tâches du système?
  - La sortie atteint-elle un niveau prédéfini en cas d'incapacité du système à poursuivre un fonctionnement correct?
– La réparation en ligne est-elle possible sans affecter la ou les tâches du système?
  - Le défaut est-il consigné sous la forme d'informations claires relatives au composant défectueux?
  - Le ou les composants défectueux peuvent-ils être remplacés sans affecter ou interrompre le fonctionnement des autres modules ou éléments du système?
  - Le module ou l'élément réparé ou de rechange a-t-il démarré automatiquement et a-t-il fonctionné correctement après son insertion dans le système?

D.4 Interprétation des résultats

Pour simplifier l'interprétation des résultats, le pourcentage de défauts introduits est calculé, correspondant aux défauts pour lesquels:

– le comportement est correct;
– la signalisation est correcte.

Bien que les données ne puissent pas être utilisées d'une manière absolue, leur valeur est significative pour les situations de comparaison.

Une approche similaire est suivie pour l'évaluation de la disponibilité dans laquelle la couverture de l'essai automatique est calculée en pourcentage de défauts détectés par l'essai automatique.

Annexe E
(informative)

Bases de données disponibles sur les taux de défaillance

E.1 Bases de données

La bibliographie suivante est une liste non exhaustive, sans ordre particulier, des sources des données relatives aux taux de défaillance des composants électroniques et non électroniques. Il convient de noter que ces sources ne s'accordent pas toujours les unes avec les autres, il convient donc d'utiliser les données avec précaution.

IEC TR 62380, *Reliability data handbook Universal model for reliability prediction of electronics components, PCBs and equipment*, Union Technique de l'Electricité et de la Communication (www.ute-fr.com) (disponible en anglais seulement). Identique à la norme RDF 2000/Reliability Data Handbook, UTE C 80-810 (disponible en anglais seulement)

Siemens Standard SN 29500, *Failure rates of components, (parties 1 à 14)*; Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich (disponible en anglais seulement).

Telcordia SR-332, version 01: mai 2001, *Reliability Prediction Procedure for Electronic Equipment,* (telecom-info.telcordia.com), (Bellcore TR-332, version 06) (disponible en anglais seulement).

EPRD (RAC-STD-6100), *Electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (disponible en anglais seulement).

NNPRD-95 (RAC-STD-6200), *Non-electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (disponible en anglais seulement).

HRD5, *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (disponible en anglais seulement)

Norme chinoise militaire/commerciale GJB/z 299B, *Electronic Reliability Prediction,* (http://www.itemuk.com/china299b.html) (disponible en anglais seulement)

ISBN:0442318480, *AT&T reliability manual – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors,* AT&T Reliability Manual, Van Nostrand Reinhold, 1990 (disponible en anglais seulement).

FIDES: janvier 2004, *Guide de données de fiabilité développé par un consortium d'industriels français sous la supervision du DoD français, la DGA*. Le guide FIDES est disponible sur demande à l'adresse fides@innovation.net.

IEEE Gold book, *L'IEEE Gold book, IEEE recommended practice for the design of reliable, industrial and commercial power systems* (disponible en anglais seulement), fournit des données concernant la fiabilité du matériel utilisé dans les systèmes de répartition électrique industriels et commerciaux. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., téléphone: +1 800 678 IEEE (aux Etats-Unis et au Canada) +1 732 981 0060 (en dehors des Etats-Unis et au Canada), fax: +1 732 981 9667, e-mail: customer.service@ieee.org.

IRPH ITALTEL, *Reliability Prediction Handbook* (disponible en anglais seulement). Le guide Italtel IRPH est disponible sur demande auprès de: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italie. Il s'agit de la version des

entreprises du secteur de la télécommunication italien de la norme CNET RDF. Les normes sont fondées sur le même ensemble de données avec des modifications apportées à certains facteurs et modes opératoires.

PRISM (RAC / EPRD), Le logiciel PRISM est disponible à l'adresse ci-dessous, il est également compris dans de nombreux produits logiciels de fiabilité disponibles dans le commerce: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

E.2 Normes utiles concernant la défaillance des composants

Les normes suivantes contiennent des informations relatives à la défaillance des composants.

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

IEC 60300-3-5, *Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques*

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

IEC 60706-3, *Maintenabilité de matériel – Partie 3: Vérification et recueil, analyse et présentation des données*

IEC 60721-1, *Classification des conditions d'environnement – Partie 1: Agents d'environnement et leurs sévérités*

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

IEC 62061:2005, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

NOTE Voir l'Annexe D pour davantage d'informations concernant les modes de défaillance des composants électriques / électroniques.

Annexe F
(informative)

Considérations liées à la sécurité

F.1 Sécurité physique

La sécurité physique vise à empêcher la destruction accidentelle ou délibérée par des personnes ayant accès au matériel. Il convient d'évaluer la capacité du système de commande de processus de base (BPCS, Basic Process Control System) à assurer la sécurité physique.

Les points d'évaluation de la sécurité physique les plus courants incluent:

1) l'accès aux ports de données ouverts des PC, par exemple USB, Ethernet, modems, ports série, etc.;
2) l'emplacement du matériel, par exemple dans des armoires ou sur des tables;
3) l'accès aux éléments situés à l'intérieur d'une armoire, par exemple systèmes de verrouillage, outils spéciaux, ou simple loquet déverrouillé;
4) l'accès aux données relatives au matériel sous enveloppe, par exemple les températures, l'humidité et la corrosion;
5) l'accès aux salles contenant les bâtis, par exemple une entrée sécurisée, un espace sous surveillance;
6) les commandes de modification des données par l'IHM, par exemple les systèmes de verrouillage.

F.2 Cybersécurité

F.2.1 Généralités

Il convient que les vendeurs de BCS fournissent un support de cybersécurité (comprenant l'élimination des vulnérabilités notoires); toutefois la responsabilité finale de la sécurité dans les conditions de fonctionnement incombe à l'utilisateur du matériel.

L'ISO IEC 27001 et l'ISO IEC 27002 donnent les bases de toutes les normes relatives à la cybersécurité. L'Annexe A de l'ISO IEC 27001:2013 contient 11 Articles numérotés de 5 à 15, qui fournissent un aperçu de ce qu'il faut effectuer. Ces Articles ne sont nullement exhaustifs et il est possible qu'un organisme puisse estimer que d'autres objectifs de contrôle et des vérifications supplémentaires sont nécessaires.

F.2.2 Politique de sécurité

Il convient que l'évaluation des capacités de cybersécurité d'un système soit effectuée dans le cadre de la politique de sécurité de l'utilisateur. Il convient que la politique de sécurité soit intégrée au cahier des charges du système décrit dans l'IEC 61069-2 par référence.

Les politiques de sécurité sont conçues pour fournir une orientation de gestion et un soutien à la sécurité des informations conformes aux exigences du secteur et aux dispositions légales et réglementaires.

F.2.3 Autres considérations

L'Article A.10 de l'ISO IEC 27001:2013 énumère un certain nombre de domaines pour lesquels il convient d'évaluer le système. Par exemple, il convient d'évaluer la mesure dans laquelle le système assure:

- la gestion de la continuité des opérations;
- la gestion des modifications, par exemple la capacité à documenter les modifications et les annuler;
- la répartition des fonctions (rôles) et des accès (autorisations), par exemple le superviseur par rapport à l'opérateur, l'ingénieur par rapport à la maintenance;
- la planification et l'acceptation du système;
- la protection contre les codes mobiles et malveillants, par exemple antivirus, anti-espion, pare-feu, gestion des correctifs, mise à niveau du système d'exploitation, listes noires, listes blanches, etc.;
- la sauvegarde et la restauration, par exemple automatique ou manuelle, complète ou incrémentielle, locale ou en réseau, etc.;
- le traitement des médias, par exemple l'accès ouvert à tous les médias amovibles, le verrouillage de tous les ports de médias ou une gestion intelligente (uniquement les appareils USB de certains vendeurs);
- la surveillance, par exemple la protection contre les intrusions, la détection des intrusions, l'état de la machine y compris le statut des mises à jour, etc.;
- le contrôle des accès et la gestion des utilisateurs, par exemple un élément d'identification comme un objet détenu (cartes), une information connue (mots de passe), ou ce qui caractérise une personne (identification biométrique), la gestion des comptes (création, suppression), etc.;
- le contrôle des accès en réseau, par exemple ports IP documentés, pare-feu sur le réseau, connexions Ethernet désactivées lorsqu'elles ne sont pas spécifiquement exigées;
- le contrôle des accès au système d'exploitation, par exemple le contrôle de l'accès aux utilitaires de ligne de commande;
- la possibilité d'avoir pour le BCS un système d'exploitation sensiblement différent de celui des systèmes de bureau de l'installation, afin de réduire au maximum le risque de la présence de virus actifs;
- le contrôle des accès aux applications et aux informations, par exemple la restriction de l'accès à certaines applications de commande du processus à des rôles spécifiques et la restriction des applications de commande non liées au processus à un nombre de personnes encore plus restreint;
- l'informatique mobile et le télétravail, par exemple la sécurité de la connexion sans fil, l'accès aux appareils mobiles, la commande des applications sur les appareils mobiles;
- les contrôles cryptographiques, par exemple le chiffrement des disques et des messages, etc.;
- la sécurité en termes de développement et de processus de support, par exemple le vendeur dispose-t-il d'une politique définie de cycle de vie de la conception de la sécurité, et cette politique est-elle suivie;
- la gestion de la vulnérabilité technique;
- la gestion des incidents de sécurité relatifs aux informations;
- la gestion de la continuité des opérations;
- la conformité avec les exigences légales.

Bibliographie

IEC 60300-3-1:2003, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*

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

IEC 60050-192:2015, *Vocabulaire Electrotechnique International – Partie 192: Sûreté de fonctionnement*

IEC 60068 (toutes les parties), *Essais d'environnement*

IEC 60605-1:1978, *Essais de fiabilité des équipements – Partie 1: Prescriptions générales*[1]

IEC 60605-2:1994, *Essais de fiabilité des équipements – Partie 2: Conception des cycles d'essai*

IEC 60605-3 (toutes les parties), *Essais de fiabilité des équipements – Partie 3: Conditions d'essais préférentielles*[2]

IEC 60605-4:2001, *Essais de fiabilité des équipements – Partie 4: Méthodes statistiques de distribution exponentielle – Estimateurs ponctuels, intervalles de confiance, intervalles de prédiction et intervalles de tolérance*

IEC 60605-6:2007, *Essais de fiabilité des équipements – Partie 6: Tests pour la validité et l'estimation du taux de défaillance constant et de l'intensité de défaillance constante*

IEC 60605-7:1978, *Essais de fiabilité des équipements – Partie 7: Plans d'échantillonnage pour confirmer le taux de défaillance et la moyenne des temps de bon fonctionnement dans l'hypothèse d'un taux de défaillance constant*[3]

IEC 60706-4, *Guide de maintenabilité du matériel – Partie 4: Section 8: Planification de la maintenance et de la logistique de maintenance*[4]

IEC 60801 (toutes les parties), *Compatibilité électromagnétique pour les matériels de mesure et de commande dans les processus industriels*[5]

IEC 60812:2006, *Techniques d'analyse de la fiabilité du système – Procédures d'analyse des modes de défaillance et de leurs effets (AMDE)*

IEC 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

IEC 61025:2006, *Analyse par arbre de panne (AAP)*

IEC 61069-6, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 6: Evaluation de l'opérabilité d'un système*

---

1 Cette publication a été supprimée et remplacée par l'IEC 60300-3-5:2001.

2 Cette série a été supprimée.

3 Cette publication a été supprimée et remplacée par l'IEC 61124:1978.

4 Cette publication a été supprimée et remplacée par l'IEC 60300-3-14.

5 Cette série a été supprimée.

IEC 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

IEC 61123, *Essais de fiabilité – Plans d'essai de conformité pour une proportion de succès*

IEC 61165, *Applications des techniques de Markov*

IEC 61326 (toutes les parties), *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 62443 (toutes les parties), *Industrial communication networks – Network and system security* (disponible en anglais seulement)

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

ISO IEC 14764, *Ingénierie du logiciel – Processus du cycle de vie du logiciel – Maintenance*

Recueil de normes militaires américaines MIL-HDBK-217, version A à F, *Reliability prediction of electronic equipment* (disponible en anglais seulement)

_____

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