# NORME INTERNATIONALE

# INTERNATIONAL STANDARD

**CEI**
**IEC**
**61069-5**

Première édition
First edition
1994-12



**Mesure et commande dans les processus industriels –**
**Appréciation des propriétés d'un système en vue de son évaluation –**

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

**Industrial-process measurement and control –**
**Evaluation of system properties for the purpose of system assessment –**

**Part 5:**
Assessment of system dependability

Numéro de référence
Reference number
CEI/IEC 61069-5: 1994

## Numéros des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

## Publications consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

## Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- **«Site web» de la CEI***
- **Catalogue des publications de la CEI**
  Publié annuellement et mis à jour régulièrement
  (Catalogue en ligne)*
- **Bulletin de la CEI**
  Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

## Terminologie, symboles graphiques et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International* (VEI).

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique,* la CEI 60417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles,* et la CEI 60617: *Symboles graphiques pour schémas.*

* Voir adresse «site web» sur la page de titre.

## Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

## Consolidated publications

Consolidated versions of some IEC publications including amendments are available. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

## Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available in the IEC catalogue.

Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
  Published yearly with regular updates
  (On-line catalogue)*
- **IEC Bulletin**
  Available both at the IEC web site* and as a printed periodical

## Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary* (IEV).

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams.*

* See web site address on title page.

# NORME INTERNATIONALE

# INTERNATIONAL STANDARD

**CEI**
**IEC**
**61069-5**

Première édition
First edition
1994-12



**Mesure et commande dans les processus industriels –**
**Appréciation des propriétés d'un système en vue de son évaluation –**

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

**Industrial-process measurement and control –**
**Evaluation of system properties for the purpose of system assessment –**

**Part 5:**
Assessment of system dependability



International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http: //www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE V

*Pour prix, voir catalogue en vigueur*
*For price, see current catalogue*

# SOMMAIRE

# CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

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

### AVANT-PROPOS

1) La CEI (Commission Electrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.

2) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparés par les comités d'études où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.

3) Ces décisions constituent des recommandations internationales publiées sous forme de normes, de rapports techniques ou de guides et agréées comme telles par les Comités nationaux.

4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.

La Norme internationale CEI 1069-5 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de la CEI: Mesure et commande dans les processus industriels.

Le texte de la présente partie est issu des documents suivants:

| DIS | Rapport de vote |
|---|---|
| 65A(BC)37 | 65A/166/RVD |

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

Les annexes A, B, C et D sont données uniquement à titre d'information.

La figure 1 indique les relations entre la présente partie et les autres parties de la CEI 1069, ainsi que la position relative de la présente partie dans la norme.

La partie 1 fournit un guide complet et, en tant que tel, est destinée à constituer une publication autonome.

La partie 2 détaille la méthodologie d'évaluation.

Les parties 3 à 8 fournissent un guide pour l'évaluation de groupes spécifiques de propriétés.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

## Part 5: Assessment of system dependability

### FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international cooperation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of the IEC on technical matters, prepared by technical committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

3) They have the form of recommendations for international use published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.

4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.

International Standard IEC 1069-5 has been prepared by sub-committee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

| DIS | Report on voting |
|---|---|
| 65A(CO)37 | 65A/166/RVD |

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

Annexes A, B, C and D are for information only.

The relation of this part to the other parts of IEC 1069 and the relative place of this part within the standard is shown in figure 1.

Part 1 provides the overall guidance and as such is intended as a stand-alone publication.

Part 2 details the assessment methodology.

Parts 3 to 8 provide guidance on the assessment of specific groups of properties.

La division des propriétés en différentes parties numérotées de 3 à 8 a été choisie afin de regrouper les propriétés apparentées.

La CEI 1069 comprend les parties suivantes, présentées sous le titre général: *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation:*

Partie 1: Considérations générales et méthodologie

Partie 2: Méthodologie à appliquer pour l'évaluation

Partie 3: Evaluation de la fonctionnalité d'un système *(à l'étude)*

Partie 4: Evaluation des caractéristiques de fonctionnement d'un système *(à l'étude)*

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

Partie 6: Evaluation de l'opérabilité d'un système *(à l'étude)*

Partie 7: Evaluation de la sécurité d'un système *(à l'étude)*

Partie 8: Evaluation de propriétés d'un système qui ne sont pas liées à sa tâche même *(à l'étude)*

The division of properties in parts 3 to 8 have been chosen so as to group together related properties.

IEC 1069 consists of the following parts, under the general title: *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment:*

Part 1: General considerations and methodology
Part 2: Assessment methodology
Part 3: Assessment of system functionality *(under consideration)*
Part 4: Assessment of system performance *(under consideration)*
Part 5: Assessment of system dependability
Part 6: Assessment of system operability *(under consideration)*
Part 7: Assessment of system safety *(under consideration)*
Part 8: Assessment of non-task-related system properties *(under consideration)*

# INTRODUCTION

La présente partie de la CEI 1069 traite de la méthode qu'il convient d'utiliser pour évaluer la sûreté de fonctionnement des systèmes de mesure et de commande des processus industriels. 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 (c'est-à-dire dans toutes les conditions d'influence) de toutes les propriétés du système qui contribuent à remplir la mission ou l'ensemble des missions spécifiques considérées. Cela étant rarement réalisable dans la pratique, la démarche qui guidera l'évaluation d'un système consiste à:

– identifier les points critiques des propriétés du système qui sont concernées pour l'accomplissement de la mission;

– planifier l'appréciation des propriétés concernées du système avec un effort rentable pour les différentes propriétés.

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, on ne peut évaluer le système; toutefois il est toujours possible de spécifier et de réaliser des appréciations (comme défini dans la CEI 1069-1) qui pourront servir lors d'évaluations menées par d'autres. Dans ce cas, on peut utiliser la norme en tant que guide pour planifier une appréciation et suivre ses procédures pour effectuer les appréciations; l'appréciation des propriétés d'un système fait en effet partie intégrante de l'évaluation de ce système.

# INTRODUCTION

This part of IEC 1069 deals with the method which should be used to assess the dependability of industrial-process measurement and control systems. Assessment of a system is the judgement, based on evidence, of the system's suitability for a specific mission or class of missions.

To obtain total evidence would require a complete (i.e. under all influencing conditions) evaluation 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:

- to identify the criticality of each of the relevant system properties;

- to plan for evaluation of the relevant system properties with a cost-effective dedication of effort to the various properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of 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 (as defined in IEC 1069-1) can still be specified and be carried out for use in assessments performed by others. In such cases, the standard can be used as a guide for planning an evaluation and it provides procedures for performing evaluations, since evaluations are an integral part of assessment.

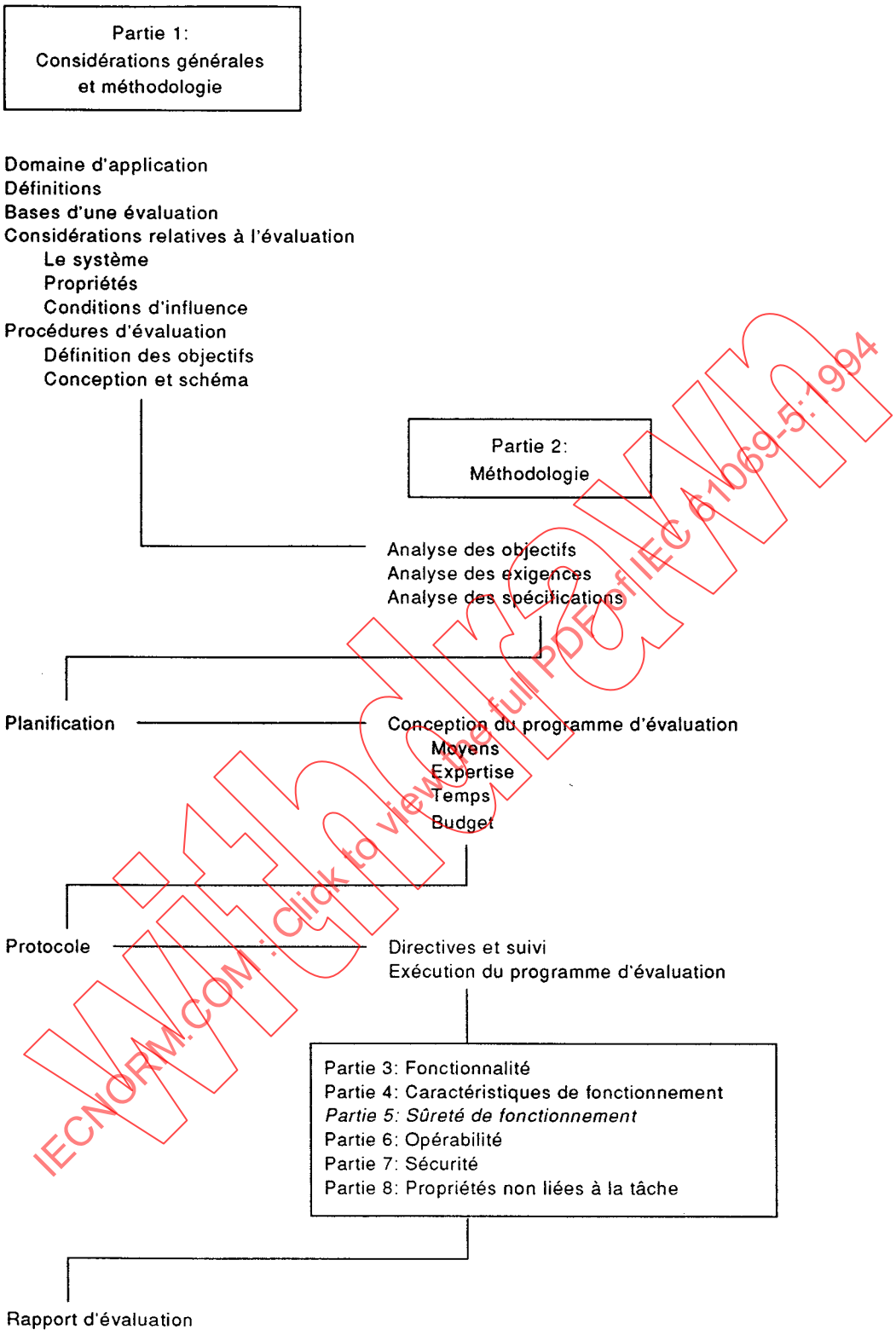





**Figure 1 – Disposition d'ensemble de la CEI 1069**

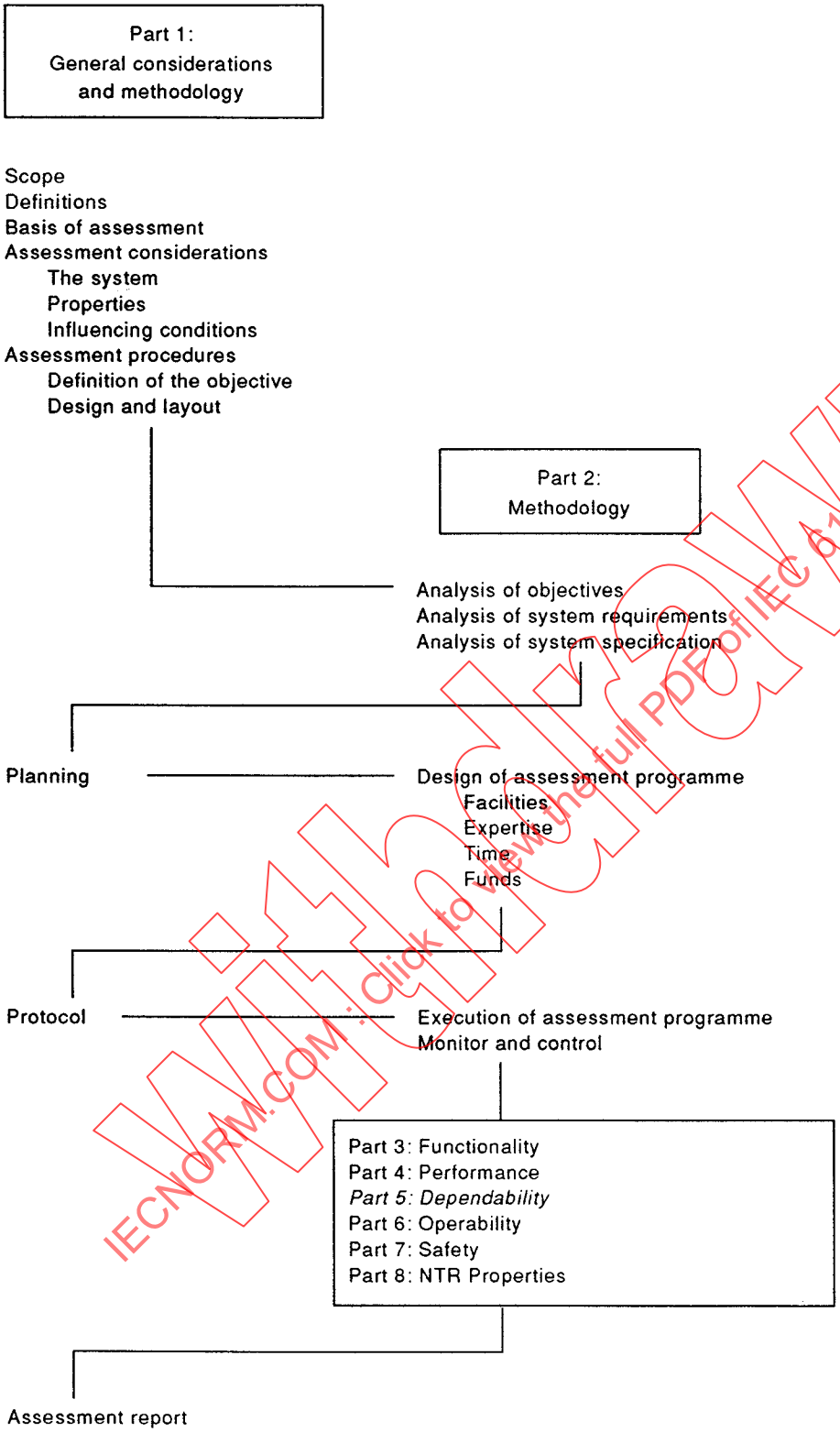





**Figure 1 – General layout of IEC 1069**

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

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

### 1 Domaine d'application

La présente partie de la CEI 1069 décrit en détails la méthode à utiliser pour évaluer de manière systématique la sûreté de fonctionnement d'un système de mesure et de commande des processus industriels.

La méthodologie d'évaluation détaillée dans la CEI 1069-2 est appliquée afin d'obtenir le programme d'évaluation de la sûreté de fonctionnement.

Les propriétés composantes de la sûreté de fonctionnement sont analysées et les critères à prendre en compte lorsque l'on évalue la sûreté de fonctionnement sont décrits.

### 2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de la CEI 1069. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente partie de la CEI 1069 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 50(191): 1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 68: *Essais d'environnement*

CEI 300-3-2: 1993, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 2: Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation.*

CEI 706-4: 1992, *Guide de maintenabilité de matériel – Partie 4 – Section 8: Planification de la maintenance et de la logistique de maintenance*

CEI 801: *Compatibilité électromagnétique pour les matériels de mesure et de commande dans les processus industriels*

CEI 812: 1985, *Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 863: 1986, *Présentation des résultats de la prévision des caractéristiques de fiabilité, maintenabilité et disponibilité*

CEI 1000: *Compatibilité électromagnétique (CEM)*

CEI 1025: 1990, *Analyse par arbre de panne (AAP)*

CEI 1069-1: 1991, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Considérations générales et méthodologie*

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

## Part 5: Assessment of system dependability

### 1 Scope

This part of IEC 1069 describes in detail the method to be used to systematically assess the dependability of industrial-process measurement and control systems.

The assessment methodology detailed in IEC 1069-2 is applied to obtain the dependability assessment programme.

The subsidiary dependability properties are analyzed, and criteria to be taken into account when assessing dependability are described.

### 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 1069. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties making agreements based on this part of IEC 1069 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 50(191): 1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 68: *Environmental testing*

IEC 300-3-2: 1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field.*

IEC 706-4: 1992, *Guide on maintainability of equipment – Part 4 – Section 8: Maintenance and maintenance support planning*

IEC 801: *Electromagnetic compatibility for industrial-process measurement and control equipment*

IEC 812: 1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 863: 1986, *Presentation of reliability, maintainability and availability predictions*

IEC 1000: *Electromagnetic compatibility (EMC)*

IEC 1025: 1990, *Fault tree analysis (FTA)*

IEC 1069-1: 1991, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology*

CEI 1069-2: 1993, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 2: Méthodologie à appliquer pour l'évaluation*

CEI 1070: 1991, *Procédures d'essais de conformité pour la disponibilité en régime établi*

CEI 1078: 1991, *Techniques d'analyse de la sûreté de fonctionnement – Méthode du diagramme de fiabilité*

CEI 1132: 199x, *Prédiction des taux de défaillance des éléments ayant une structure série* (en préparation)

CEI 1165: 199x, *Application des techniques markoviennes* (en préparation)

## 3 Définitions

Pour les besoins de la présente partie de la CEI 1069, les définitions suivantes s'appliquent.

Les définitions marquées d'un * sont identiques à celles données dans la CEI 50(191). Afin d'assurer la cohérence de la compréhension des définitions dans toutes les parties de la CEI 1069, ces définitions sont commentées dans les notes à la fin de cet article.

3.1 **sûreté de fonctionnement**: Mesure dans laquelle on peut se fier à un système pour qu'il exécute exclusivement et correctement une tâche dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée.

3.2 **fiabilité***: Aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné.

3.3 **maintenabilité***: Dans des conditions données d'utilisation, aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits.

3.4 **disponibilité***: Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données à un instant donné, ou pendant un intervalle de temps donné, en supposant que les moyens nécessaires sont fournis.

3.5 **intégrité**: Assurance fournie par un système que les tâches seront accomplies correctement à moins que le système ne prévienne que l'un quelconque de ses états pourrait conduire à une situation contraire.

3.6 **sûreté**: Assurance fournie par un système de sa capacité de refuser toute entrée incorrecte ou tout accès non autorisé.

3.7 **crédibilité**: Mesure dans laquelle un système est capable de reconnaître et signaler son état et de résister à des entrées incorrectes ou des accès non autorisés.

NOTE – Pour les besoins de la présente norme, il est entendu que:

– «une entité» est un système de mesure et de commande des processus industriels;

– «une fonction requise» est une tâche. Dans le cas d'une appréciation, il faut comprendre «tâche» comme «tâche du système». Tâche et fonction sont définies en 2.2.4 et 2.2.5 de la CEI 1069-1.

IEC 1069-2: 1993, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

IEC 1070: 1991, *Compliance test procedures for steady-state availability*

IEC 1078: 1991, *Analysis techniques for dependability – Reliability block diagram method*

IEC 1132: 199x, *Failure rate prediction of items having a series structure* (in preparation)

IEC 1165: 199x, *Application of Markov techniques* (in preparation)

## 3 Definitions

For the purpose of this part of IEC 1069 the following definitions apply.

The definitions marked with an * are identical with those given in IEC 50(191). In order that the definitions are understood consistently throughout all parts of IEC 1069, these definitions are commented upon in notes at the end of this clause.

3.1 **dependability:** The extent to which a system can be relied upon to perform exclusively and correctly a task under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

3.2 **reliability*:** The ability of an item to perform a required function under given conditions for a given time interval.

3.3 **maintainability*:** 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.

3.4 **availability*:** The ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided.

3.5 **integrity:** The assurance provided by a system that the tasks will be performed correctly unless notice is given of any state of the system, which could lead to the contrary.

3.6 **security:** The assurance provided by a system that any incorrect input, or unauthorized access is denied.

3.7 **credibility:** The extent to which a system is able to recognize and signal the state of the system and to withstand incorrect inputs or unauthorized access.

NOTE – For the purpose of this standard, it is understood that:

– "an item" is an industrial-process measurement and control system;

– "a required function" is a task. In case of an evaluation, a "task" should be understood as a "system task". Task and function are defined in 2.2.4 and 2.2.5 of IEC 1069-1.

## 4 Propriétés de sûreté de fonctionnement

### 4.1 *Généralités*

Pour qu'un système soit sûr en ce qui concerne son fonctionnement, il est nécessaire qu'il soit prêt à accomplir ses fonctions. On aborde ici la question de la disponibilité qui dépend de la fréquence des défaillances du système (fiabilité) et du temps nécessaire à restaurer le système (maintenabilité).

Toutefois, quand dans la pratique le système est prêt à accomplir ses fonctions, cela ne signifie pas que l'on soit sûr que ces fonctions soient accomplies correctement.

On aborde ici la question de la crédibilité qui dépend:

– de la capacité du système à émettre une alarme s'il passe dans un état où il n'est plus capable d'accomplir correctement tout ou partie de ses fonctions (intégrité);

– de la capacité du système à rejeter toute entrée incorrecte ou accès non autorisé (sûreté).

Pour évaluer la sûreté de fonctionnement d'un système il est donc nécessaire d'identifier et d'évaluer les composantes qui déterminent la sûreté de fonctionnement.

La figure 2 indique les relations entre la sûreté de fonctionnement et ses composantes.

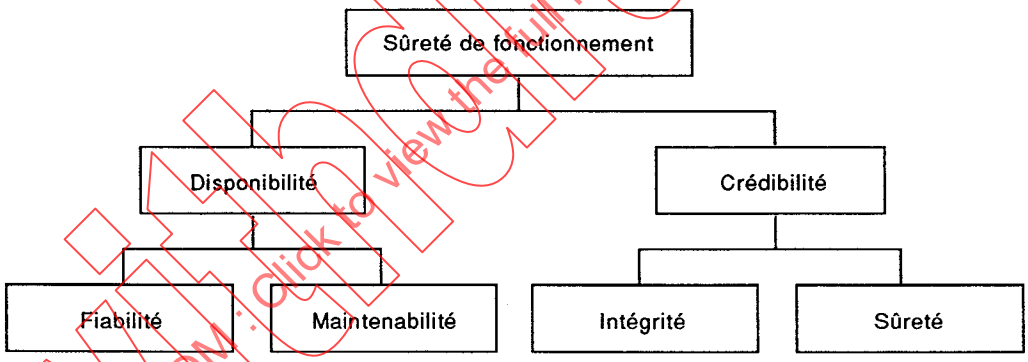



**Figure 2 – Hiérarchie en matière de sûreté de fonctionnement**

### 4.2 *Sûreté de fonctionnement*

La sûreté de fonctionnement ne peut pas être évaluée directement. Il est nécessaire d'évaluer individuellement chacune des propriétés composantes.

Chaque propriété composante dépend de l'organisation architecturale des modules du système et des propriétés de sûreté de fonctionnement de ces modules.

Le rapport entre la sûreté de fonctionnement du système et les composantes de sûreté de fonctionnement des modules peut être très complexe.

Chaque propriété composante au niveau système peut dépendre de plusieurs propriétés composantes au niveau module.

## 4 Dependability properties

### 4.1 *General*

For a system to be dependable it is necessary that it is ready to perform its functions. This is an availability issue and depends on the frequency of the system failures (reliability) and the time necessary to restore the system (maintainability).

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.

This is a credibility issue, which 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).

To assess the dependability of a system, it is therefore necessary to identify and assess the subsidiary properties that determine the dependability.

The relation between dependability and its subsidiary properties is shown in figure 2.

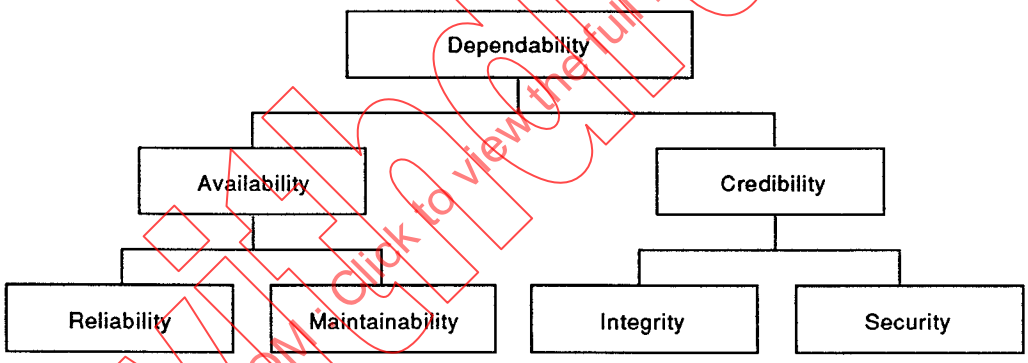



**Figure 2 – Dependability hierarchy**

### 4.2 *Dependability*

Dependability cannot be assessed directly. It is necessary to assess each subsidiary property individually.

Each subsidiary property is dependent upon the architectural arrangement of the system modules and the dependability properties of these modules.

The relation of subsidiary dependability properties of these modules to the dependability of the system may be very complex.

Each subsidiary property at the system level may be dependent upon several subsidiary properties at the module level.

Par exemple:

– si l'architecture du système inclut de la redondance, la disponibilité du système dépend des propriétés d'intégrité des modules redondants;

– si l'architecture inclut des mécanismes de sûreté du système, la sûreté du système dépend des propriétés de disponibilité des modules qui accomplissent ces mécanismes de sûreté;

– si l'architecture inclut des modules qui vérifient les données transférées à l'intérieur depuis d'autres parties du système, l'intégrité du système dépend des propriétés de sûreté de ces modules.

La sûreté de fonctionnement ne peut être décrite par un seul nombre. Certaines de ses composantes peuvent être exprimées sous forme de probabilités; d'autres composantes sont déterministes, certains aspects peuvent être quantifiés; d'autres aspects ne peuvent qu'être décrits de manière qualitative.

Lorsqu'un système exécute plusieurs tâches, sa sûreté de fonctionnement peut être différente d'une tâche à l'autre. Pour chacune de ces tâches, une analyse distincte est nécessaire.

4.3 *Disponibilité*

La disponibilité du système dépend de la disponibilité des parties prises individuellement et de la manière dont ces parties coopèrent pour exécuter les tâches attribuées au système. La manière dont ces parties coopèrent peut inclure une redondance fonctionnelle (homogène ou diversifiée), un repli et une dégradation fonctionnels. Dans la pratique, la disponibilité dépend des procédures suivies et des moyens disponibles pour maintenir le système. La disponibilité d'un système peut être différente pour chacune de ses tâches. Pour chaque tâche, la disponibilité d'un système peut être quantifiée de deux manières.

4.3.1 Pour prédire la disponibilité du système, la disponibilité peut être calculée comme suit:

$$\text{disponibilité} = \frac{\text{temps moyen jusqu'à la défaillance}}{(\text{temps moyen jusqu'à la défaillance} + \text{durée moyenne de panne})}$$

où

– «disponibilité» est la disponibilité du système pour la tâche donnée.

– «temps moyen jusqu'à la défaillance» est la moyenne des temps comptés depuis la remise du système dans un état où il peut accomplir la ou les tâches données jusqu'à l'instant où le système n'est plus en mesure de le faire.

– «durée moyenne de panne» est la moyenne du temps total nécessaire pour remettre le système en état d'accomplir la tâche donnée, partant de l'instant où le système n'a plus été en mesure d'accomplir cette tâche.

4.3.2 Pour un système en fonctionnement, la disponibilité peut être calculée comme suit:

$$\text{disponibilité} = \frac{\text{temps total durant lequel le système a été capable d'accomplir la tâche}}{\text{temps total durant lequel le système aurait dû accomplir la tâche}}$$

For example:

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

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

4.3 *Availability*

Availability of the system is dependent upon the availabilities of the individual parts of the system and the way in which these parts cooperate in performing the system tasks. The way in which parts cooperate may 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 may differ with respect to each of its tasks. Availability of the system for each task can be quantified in two ways.

4.3.1 To predict the availability of a system, its availability can be calculated as:

$$\text{availability} = \frac{\text{mean time to failure}}{(\text{mean time to failure} + \text{mean time to restoration})}$$

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.

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

$$\text{availability} = \frac{\text{total time the system has been able to perform the task}}{\text{total time the system has been expected to perform the task}}$$

4.4 *Fiabilité*

La fiabilité d'un système dépend de la fiabilité des parties prises individuellement constituant le système et de la manière dont ces parties coopèrent pour accomplir la ou les tâches du système. La manière dont ces parties coopèrent peut inclure une redondance fonctionnelle (homogène ou diversifiée), un repli et une dégradation fonctionnels.

La fiabilité d'un système peut être différente pour chacune de ses tâches. La fiabilité peut être quantifiée pour chaque tâche prise individuellement et l'on peut en extrapoler divers niveaux de confiance.

La fiabilité des parties matérielles individuelles constituant le système peut être prédite en utilisant la méthode du décompte des parties. La fiabilité du système peut ensuite être prédite par synthèse. Il convient de noter que pour les modules logiciels des systèmes il n'existe aucune méthode prédictive apportant des niveaux de confiance élevés.

Les mécanismes pour analyser la fiabilité du logiciel sont décrits en 4.6 du projet de comité CEI 56 (Secrétariat)319: *Analyse des exigences de fiabilité et de maintenabilité du logiciel* (à l'étude), listé en annexe D.

4.5 *Maintenabilité*

La maintenabilité d'un système dépend de la maintenabilité des parties élémentaires et de la structure matérielle et fonctionnelle du système. La structure matérielle influence la facilité d'accès, les possibilités de remplacement, etc. La structure fonctionnelle affecte la facilité de diagnostic, etc.

Lorsque l'on quantifie la maintenabilité d'un système, il convient de prendre en compte toutes les actions nécessaires pour remettre le système dans l'état où il est totalement en mesure d'exécuter ses tâches. Il faut donc inclure des éléments tels que les temps nécessaires pour détecter la panne, pour lancer l'action de maintenance, pour effectuer le diagnostic et remédier à la cause, pour effectuer les réglages et vérifications, etc.

La quantification de la maintenabilité doit être complétée par des éléments qualitatifs en vérifiant jusqu'à quel point les critères suivants sont remplis:

– signalisation des défaillances: voyants, messages d'alarme, comptes rendus, etc.;

– accès: facilité d'accès pour le personnel et pour brancher des instruments de mesure, modularité, etc.;

– diagnostics: identification précise de la panne, outils de diagnostic n'ayant pas d'influence sur le système, moyens d'aide au diagnostic à distance, analyse statistique d'erreur et compte rendu;

– possibilités de réparation/de remplacement: modularité, identification non ambiguë des modules et éléments, besoin minimal d'outils spéciaux et, lorsque les éléments ou les modules sont remplacés, répercussion minimale sur les autres éléments ou modules;

– vérification finale: procédures claires de maintenance, exigences minimales de vérification finale.

4.6 *Crédibilité*

La crédibilité d'un système dépend des mécanismes d'intégrité et de sûreté mis en oeuvre en tant que fonctions exécutées par les éléments du système.

Un mécanisme d'intégrité est mis en oeuvre par un élément qui vérifie les sorties d'autres éléments.

### 4.4 *Reliability*

Reliability of a system is dependent 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 fall-back 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. 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 analyze software reliability are described in 4.6 of IEC Committee draft 56(Secretariat)319: *Software reliability and maintainability requirements analysis* (under consideration), listed in annex D.

### 4.5 *Maintainability*

The maintainability of a system is dependent upon the maintainability of individual parts and the physical and functional structure 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 shall 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:

- 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: 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.

### 4.6 *Credibility*

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

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

Un mécanisme de sûreté est mis en oeuvre par un élément qui vérifie les entrées d'autres éléments.

Les mécanismes de crédibilité comprennent:

a) une vérification de

   – l'exécution correcte des fonctions (par exemple, par chien de garde ou en utilisant des données connues); et/ou

   – l'exactitude des données (par exemple, vérification de validité, de parité, etc.);

b) une action, telle que:

   – l'autocorrection;

   – le confinement;

   – la signalisation d'une action, etc.

Ces mécanismes peuvent être utilisés pour conférer intégrité et/ou sûreté.

Pour analyser les mécanismes de crédibilité, on peut utiliser les techniques d'injection de pannes décrites en 8.3.2.2.

La crédibilité est une propriété déterministe et certains aspects peuvent être quantifiés.

### 4.7 *Sûreté*

La sûreté d'un système dépend des mécanismes mis en oeuvre à la limite du système pour détecter des entrées incorrectes et des accès non autorisés et y parer.

La sûreté est une propriété déterministe et certains aspects peuvent être quantifiés.

### 4.8 *Intégrité*

L'intégrité dépend des mécanismes mis en oeuvre sur les éléments de sortie du système pour vérifier que les sorties sont correctes. Elle dépend également des mécanismes mis en oeuvre dans le système pour détecter et éviter des transitions incorrectes de signaux ou de données entre les parties du système. Ces mécanismes internes sont des mécanismes d'intégrité ou de sécurité au niveau des parties constitutives chacune d'entre elles pouvant être considérée individuellement en tant que système.

L'intégrité est une propriété déterministe et certains aspects peuvent être quantifiés.

## 5 Examen critique du cahier des charges du système

Il convient d'effectuer un examen critique du cahier des charges du système afin de s'assurer qu'y figurent toutes les tâches que doit accomplir le système ainsi que les exigences de sûreté de fonctionnement et que ces éléments sont détaillés conformément à la manière décrite dans la CEI 1069-2.

Si une mission a des implications sur la sécurité du processus et si le système doit accomplir des tâches liées à la sécurité, il convient de consulter le projet de comité CEI 65A (Secrétariat)123: *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables* (à l'étude), listé en annexe D, afin de vérifier la cohérence des exigences concernant le système.

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

Credibility mechanisms include:

a) a check on
   - correct performance of functions (e.g. by watchdog, using known data); and/or
   - correct data (e.g. validity check, parity check, etc.);

b) an action, such as:
   - self-correction;
   - confinement;
   - notification of action, etc.

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

To analyze the credibility mechanisms, the fault injection techniques described in 8.3.2.2 can be used.

Credibility is deterministic and some aspects can be quantified.

### 4.7 *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.

Security is deterministic and some aspects can be quantified.

### 4.8 *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. These internal mechanisms are integrity or security mechanisms with respect to the associated parts, each of which may be considered as a system by itself.

Integrity is deterministic and some aspects can be quantified.

## 5 Review of the system requirements document

The system requirements document should be reviewed to check that all the tasks to be performed by the system and the dependability requirements have been addressed and are listed in the manner described in IEC 1069-2.

If a mission has process safety implications and the system is required to perform safety related tasks, IEC committee draft 65A(Secretariat)123: *Functional safety of electrical/ electronic/programmable electronic system* (under consideration), listed in annex D, should be consulted to check the consistency of the system requirements.

L'efficacité de l'évaluation de la sûreté de fonctionnement dépend beaucoup de la clarté de l'expression des exigences, et les résultats de cette évaluation dépendent de ce qui est pris en compte en tant que défaillance.

Pour cette raison le cahier des charges doit être revu afin de vérifier que pour chacune des tâches attribuées au système, les éléments suivants sont clairement exprimés:

- l'importance relative de la tâche;
- la définition de ce qui est pris en compte en tant que défaillance de la tâche;
- les critères de défaillance dans les termes des propriétés de sûreté de fonctionnement;
- les conditions de fonctionnement et d'environnement.

La spécification d'une défaillance en termes quantitatifs ou qualitatifs sera mise en forme conformément au projet de comité CEI 56 (Secrétariat)318: *Guide pour spécifier les caractéristiques de sûreté de fonctionnement* (à l'étude), listé en annexe D.

Lorsque les caractéristiques de sûreté de fonctionnement sont influencées par les facteurs humains, il convient que ceux-ci soient décrits correctement et quantifiés (si possible) afin de permettre une évaluation appropriée de leur influence.

Pour montrer que les informations nécessaires ont été fournies, il faut examiner les exigences en matière de sûreté de fonctionnement à la fois à la lumière de chacune des tâches individuelles et de la mission d'ensemble du système.

L'annexe A fournit à titre indicatif le type de prescriptions et de mise en forme de la documentation que devrait contenir le cahier des charges du système afin de permettre l'évaluation des propriétés de sûreté de fonctionnement.

## 6 Examen critique du cahier des spécifications du système

Il convient d'effectuer un examen critique du cahier des spécifications du système afin de s'assurer que les propriétés de sûreté de fonctionnement pour chacune des tâches requises sont détaillées conformément à la manière décrite dans la CEI 1069-2.

Il convient de porter une attention particulière pour vérifier que l'on dispose d'informations sur:

- les fonctions du système qui supportent chaque tâche et les modules et éléments, tant matériels que logiciels, qui supportent chacune de ces fonctions;
- les différents chemins possibles pour exécuter chaque tâche, et la manière dont ces différents chemins sont activés;
- les mécanismes de crédibilité (sûreté et intégrité) fournis et la manière dont ces mécanismes sont supportés;
- la fiabilité et la disponibilité de chaque tâche de même que des fonctions, modules et éléments qui les supportent;
- les caractéristiques de maintenabilité;
- les conditions de fonctionnement et d'environnement ainsi que les limites d'utilisation des modules et éléments.

L'annexe B fournit à titre indicatif le type de spécifications et de mise en forme de la documentation que devrait contenir le cahier des spécifications du système afin de permettre l'évaluation des propriétés de sûreté de fonctionnement.

The effectiveness of the dependability assessment is strongly dependent upon the comprehensiveness of the statement of requirements, and its results on what is considered to be a failure.

For this reason the system requirements document shall 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 the format given in IEC committee draft 56(Secretariat)318: *Guide on specifying dependability characteristics* (under consideration), listed in annex D.

Where the dependability characteristic is influenced by human factors, these should be properly described and quantified (if possible) to permit the proper assessment of their influence.

To establish that the necessary information has been provided, the dependability requirements shall be considered both in relation to individual tasks and in relation to the total system mission.

Annex A gives guidance on the type of information and documentation format the system requirements document should give to enable the dependability properties to be assessed.

## 6 Review of the system specification document

The specification document should be reviewed to check that the dependability properties for each of the required tasks are listed as described in IEC 1069-2.

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 B gives guidance on the type of information and documentation format the system specification document should give to enable the dependability properties to be assessed.

## 7 Procédure d'évaluation

### 7.1 *Généralités*

L'évaluation doit suivre la procédure décrite dans l'article 7 de la CEI 1069-2.

Il faut exprimer clairement l'objectif de l'évaluation. Des indications sont données en 4.1 de la CEI 1069-1.

Il convient que les informations contenues dans le cahier des charges (CdC) et le cahier des spécifications (CdS) du système soient complètes et précises afin de permettre l'évaluation de la sûreté de fonctionnement. Si, au cours de l'une quelconque des phases de l'évaluation certaines informations sont manquantes ou incomplètes, les rédacteurs du cahier des charges et du cahier spécifications du système doivent être consultés pour répondre à des questions spécifiques afin d'obtenir les informations complémentaires requises.

Une liste détaillée des éléments à prendre en compte pour l'évaluation se trouve dans la CEI 863.

### 7.2 *Analyse du cahier des charges et du cahier des spécifications du système*

#### 7.2.1 *Classement des informations détaillées*

Pour l'évaluation de la sûreté de fonctionnement, les informations doivent être extraites du cahier des charges (CdC) et du cahier des spécifications (CdS) du système comme cela est décrit en 7.2 de la CEI 1069-2.

Les propriétés de sûreté de fonctionnement requises pour chacune des tâches doivent être extraites du cahier des charges en termes quantitatifs/qualitatifs, en mentionnant les conditions qui répondent aux exigences de sûreté de fonctionnement.

Chaque tâche doit être décrite en fonction de ses entrées, de ses sorties et de son fonctionnement.

Pour chaque entrée, il convient de noter:

- les états acceptables et les états de sortie acceptables correspondants;
- les états non acceptables et les actions qui sont alors exigées.

Pour chaque sortie, il convient de noter:

- les états acceptables;
- les états non acceptables et les actions qui sont alors exigées.

Pour chacune des tâches, il convient d'exprimer clairement les éléments suivants:

- ce qui est pris en compte en tant que défaillance;
- la fréquence d'occurrence admise;
- les actions devant être entreprises;
- le temps maximal accordé pour rétablir la tâche;
- autant que possible, les conditions d'influence décrites dans la CEI 1069-1.

## 7 Assessment procedure

### 7.1 *General*

The assessment should follow the procedure as laid down in clause 7 of IEC 1069-2.

The objective of the assessment shall be clearly stated. Guidance is given in 4.1 of IEC 1069-1.

The information given in the system requirements document (SRD) and the system specification document (SSD) should be complete and precise to enable the assessment of the dependability. If at any phase of the assessment information is missing or incomplete, the originators of the system requirements document and the system specification document should be consulted with specific questions to obtain the required further information.

A list of items to be considered for the assessment can be found in IEC 863.

### 7.2 *Analysis of the system requirements document and system specification document*

#### 7.2.1 *Collation of documented information*

For the purpose of the assessment of dependability, information shall be extracted from the system requirements document (SRD) and the system specification document (SSD) as described in 7.2 of IEC 1069-2.

The dependability properties required for each of the tasks shall be extracted from the system requirements document in quantitative/qualitative terms, noting the influencing conditions under which these dependabilities are required.

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

For each input, notes should be made of:

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

For each output, notes should be made of:

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

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

- what constitutes a failure;
- permissible frequency of occurrence;
- action to be taken;
- maximum time allowed to restore the task;
- as far as applicable, influencing conditions as described in IEC 1069-1.

Toutes les informations concernant les données et les exigences de sûreté de fonctionnement fournies pour le système doivent être écrites en regard des exigences correspondantes et confrontées à ces dernières, de manière à relever des éléments précis et concis sur les points suivants:

- les limites fonctionnelles du système;
- points sur lesquels le système ne répond pas aux exigences;
- fonctions fournies pour exécuter les tâches requises et différents chemins liant les fonctions pour venir en soutien de la ou des tâches requises;
- l'allocation des fonctions fournies aux modules et aux éléments du système, chacun accompagné des données relatives à ses propriétés de sûreté de fonctionnement;
- les connaissances déjà disponibles et le niveau de détail jusqu'où il convient d'évaluer les propriétés de sûreté de fonctionnement.

L'analyse doit inclure un examen de la manière dont sont ouverts les différents chemins à travers le système, c'est-à-dire:

- de manière statique en changeant la configuration du système; ou
- de manière dynamique, soit automatiquement au moyen d'un mécanisme de crédibilité par exemple, soit manuellement au moyen d'une action sur un clavier par exemple.

7.2.2 *Conditions d'influence*

La sûreté de fonctionnement d'un système peut être affectée par les conditions d'influence suivantes données en 4.4 de la CEI 1069-1:

- la tâche imposée au système, par exemple une surcharge du système, etc.;
- le processus relié au système, par exemple des perturbations électriques;
- les systèmes extérieurs connectés au système, par exemple des perturbations électriques, etc.;
- les alimentations (air, électricité, etc.) du système, par exemple des variations de tension;
- l'environnement dans lequel est placé le système; humidité, température, etc.

Pour chacune des composantes de la sûreté de fonctionnement, les conditions d'influence de premier ordre sont les suivantes.

a) La fiabilité est influencée par les conditions d'influence:

- les sources d'alimentation dont l'influence est partiellement prévisible en utilisant le projet de comité CEI 56(Secrétariat)383: *Utilisation des données de taux de panne requises pour l'évaluation de la fiabilité du matériel électronique – Conditions de référence – Modèles sous contrainte en vue de leur conversion* (à l'étude), listé en annexe D;
- l'environnement dont l'influence est partiellement prévisible en utilisant le projet de comité CEI 56 (Secrétariat)383, listé en annexe D;
- les services en raison de la manutention et du stockage des pièces, etc.

b) La maintenabilité; dans l'objectif de cette norme, la maintenabilité est considérée comme une propriété intrinsèque du système lui-même et ne peut être affectée que de manière indirecte, par exemple une restriction d'accès due à des conditions dangereuses.

All information on the dependability requirements and the dependability data provided for the system shall be drawn together and cross-related, to compile precise and concise statements of the following:

- the functional boundaries of the system;
- items for which the system does not comply with the requirements;
- functions provided to perform the required tasks and alternative data paths linking the functions to support the required task(s);
- the allocation of the functions provided to the system modules and elements, each with data of their dependability properties;
- the global pre-knowledge available and extent to which the dependability properties should be assessed.

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.

7.2.2 *Influencing conditions*

The dependability of a system can be affected by the following influencing conditions listed in 4.4 of IEC 1069-1:

- the task imposed on the system, e.g. system overload, etc.;
- the process connected to the system, e.g. electrical noise;
- the external systems connected to the system, e.g. electrical noise, etc.;
- the utilities (air, electricity, etc.) serving the system, e.g. voltage variations;
- the environment in which the system is placed; humidity, temperature, etc.

For each of the dependability properties the primary influencing conditions are as follows.

a) Reliability is influenced by the influencing conditions:

- utilities, the influence is partly predictable using IEC committee draft 56(Secretariat)383: *Use of failure rate data intended for reliability prediction of components in electronic equipment – Reference conditions – Stress models for their conversion* (under consideration), listed in annex D;
- environment, the influence is partly predictable using IEC committee draft 56(Secretariat)383 listed in annex D;
- services, due to the handling, storage of parts, etc.

b) 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, e.g. restricted access due to hazardous conditions.

c) La disponibilité; lorsque l'on tient compte des activités humaines nécessaires pour maintenir le système, ou remettre le système, en état d'exécuter la ou les tâches qui lui sont attribuées, la disponibilité est influencée par le comportement humain et les conditions de service (retard dans la fourniture de pièces détachées, formation, documentation, etc.).

d) La crédibilité; les mécanismes de crédibilité (sûreté et intégrité) peuvent être influencés par des actions humaines intentionnelles ou non, et si ces mécanismes partagent des ressources communes, telles que des bus ou des processeurs multitâches, ils peuvent être influencés par la ou les tâches attribuées au système, le processus en raison d'une augmentation soudaine de l'activité du processus (par exemple une avalanche d'alarmes), etc. et les systèmes extérieurs.

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

Lorsque l'on spécifie des essais pour apprécier les effets des conditions d'influence, il convient de consulter les normes CEI suivantes:

- série CEI 68;
- série CEI 801;
- série CEI 1000.

7.2.3 *Mise en forme des informations recueillies*

Il y a lieu de mettre les informations recueillies suivant les indications ci-dessus sous une forme permettant leur manipulation lors de la conception du programme d'évaluation.

Les dispositions présentées dans les annexes A et B sont des exemples possibles de mise en forme des informations.

7.3 *Conception du programme d'évaluation*

7.3.1 *Comparaison du cahier des charges et du cahier des spécifications du système*

La première étape pour concevoir le programme d'évaluation est d'analyser les informations recueillies dans les CdC et CdS, obtenues en 7.2.

En comparant le CdC et le CdS, on établit une liste «tâche par tâche» de l'ensemble des fonctions, modules, éléments et autres moyens proposés pour répondre aux exigences de sûreté de fonctionnement.

Chaque entrée de cette liste est un sujet potentiel d'évaluation.

Chaque sujet potentiel d'évaluation doit être examiné afin de décider jusqu'à quel point ce sujet doit faire l'objet d'une appréciation en vue d'obtenir l'augmentation désirée du niveau de confiance.

7.3.2 *Sujets d'évaluation*

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

- importance de la tâche vis-à-vis de la mission;
- niveau de confiance préexistant basé sur une connaissance préalable, qui peut elle-même s'appuyer sur la réussite du système dans des missions similaires ou identiques, l'expérience acquise avec le constructeur, l'expérience d'utilisateurs avec le même type de système ou des systèmes comparables;

c) 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 the system task(s), availability is influenced by human behaviour and service conditions (delays in delivery of spare parts, training, documentation, etc.).

d) Credibility; the mechanisms (security and integrity) can be affected by intentional or unintentional human actions, and if these mechanisms share common facilities, such as buses or multitasking processors, they can be influenced by system task(s), the process due to a sudden increase in process activity (e.g. 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 conditions, the following IEC standards should be consulted:

- IEC 68;
- IEC 801;
- IEC 1000.

7.2.3 *Documenting collated information*

The information collated as stated above should be documented in a form that can be manipulated for the purpose of designing the assessment programme.

The layouts shown in annexes A and B are examples of the way the information can be documented.

7.3 *Designing the assessment programme*

7.3.1 *Comparison of the system requirements document and system specification document*

The first step in designing the assessment programme is to analyze the information collected from the SRD and SSD obtained in 7.2.

By comparing the SSD and the SRD, a "task-by-task" list is constructed of all the proposed functions, modules, elements and other means provided to achieve the dependability requirements.

Each entry in this list is a potential assessment item.

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

7.3.2 *Assessment items*

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

- importance of the task to the mission;
- existing level of confidence based upon prior knowledge, which may be based on prior success of the system in similar or identical missions, experience with the manufacturer, the experience of users with the same system type or comparable systems;

– la maturité du système basée sur le degré d'innovation dans la conception du système, le nombre de systèmes de référence en fonctionnement, le degré de normalisation des éléments, des interfaces, du logiciel système et du langage de programmation. De telles normes peuvent être internationales, nationales ou d'entreprise;

– le niveau d'interdépendance des différentes fonctions, le nombre des interfaces, la réutilisation de la même fonction dans différentes tâches;

– des contraintes techniques telles que la taille, le poids, la disponibilité des sources d'alimentation, la commande de l'environnement d'essai.

7.3.3 *Activités d'évaluation*

La liste des activités d'évaluation est alors obtenue en complétant chacun des sujets de la liste réduite suivant les indications de 7.3.2 par:

– le type d'analyse et d'essai requis;

– les connaissances et la compétence requises pour exécuter chaque analyse et/ou essai;

– les contraintes sur le planning de l'évaluation en raison des effets permanents que peuvent avoir certains essais;

– la disponibilité du personnel choisi;

– les outils et les services requis pour exécuter les analyses et les essais;

– l'estimation du coût et du temps pour chaque analyse et essai;

– un niveau de priorité pour chacune des activités d'évaluation.

En fonction des critères exprimés en 7.3.1 et 7.3.2, il peut être nécessaire d'envisager plusieurs techniques d'appréciation qui se complètent mutuellement.

La liste des «activités d'évaluation» sera combinée avec les listes similaires établies pour l'évaluation des autres propriétés afin d'aboutir à un programme d'évaluation global pour le système.

7.4 *Programme d'évaluation*

Le programme final d'évaluation doit au moins spécifier et/ou mentionner les points suivants:

– une analyse déductive et qualitative de la sûreté de fonctionnement du système, telle que décrite en 8.2;

– les critères à prendre en compte tels qu'indiqués en 7.2;

– les activités d'évaluation obtenues en 7.3.3;

– les modes de défaillance à analyser et/ou apprécier et les effets résultants attendus;

– les mécanismes d'intégrité et de sûreté existant dans le système;

– l'augmentation recherchée du niveau de confiance;

– le planning d'évaluation prenant en compte les effets permanents que les essais peuvent entraîner.

– the maturity of the system based on the degree of novelty of the system, the number of reference systems in operation, the degree of standardization for devices, interfaces, operating system and programming language. Such standards may be international, national or proprietary;

– the level of interdependency of different functions, the number of interfaces, re-use of same function in different tasks;

– technical constraints such as size, weight, availability of utilities, control of the test environment.

7.3.3 *Assessment activities*

The list of assessment activities is subsequently obtained by augmenting each of the items of the reduced list obtained in 7.3.2 with:

– type of analysis and test required;

– knowledge and skill required to perform each analysis and/or test;

– constraints on the assessment schedule due to permanent effects that tests may have;

– availability of the selected personnel;

– tools and utilities required to perform the analysis and tests;

– estimation of cost and time for each analysis and test;

– priority level for each of the assessment activities.

Depending on the criteria formulated as in 7.3.1 and 7.3.2, it may be necessary to consider several evaluation techniques, which are mutually supplementary.

The "assessment activities" list will be used in conjunction with similar lists established for the assessment of the other properties to arrive at an overall assessment programme for the system.

7.4 *Assessment programme*

The final assessment programme should specify and/or list at least the following points:

– a deductive qualitative dependability analysis of the system as described in 8.2;

– the criteria to be taken into account as given in 7.2;

– the assessment activities obtained in 7.3.3;

– the failure modes to be analyzed and/or evaluated and the resulting effects expected;

– the integrity and security mechanisms provided in the system;

– the required increase in confidence level;

– the assessment schedule taking account of the permanent effects that tests may cause.

## 8 Techniques d'appréciation

### 8.1 *Généralités*

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

On peut retenir des techniques analytiques en se basant uniquement sur la documentation du système, ou des techniques empiriques, nécessitant un accès à un système existant.

Les résultats fournis par les différentes techniques d'évaluation peuvent être quantitatifs ou qualitatifs, ou combiner ces deux aspects.

Dans cette norme on suggère plusieurs techniques d'appréciation. Il est possible d'appliquer d'autres méthodes mais dans tous les cas il convient que le rapport d'évaluation fasse référence à des documents décrivant les techniques utilisées.

Une liste des éléments à prendre en compte pour l'évaluation se trouve dans la CEI 863. Les techniques analytiques, décrites ci-après, s'appuient sur des modèles. De tels modèles peuvent rarement représenter de manière exacte un système réel et, même s'ils le peuvent, on n'est jamais certain à 100 % qu'ils le fassent. Il convient donc de préciser également le niveau de confiance des résultats d'une appréciation s'appuyant sur des techniques analytiques.

La sûreté de fonctionnement d'un système est également influencée par les erreurs introduites dans le système lors des phases de conception, de spécification et de réalisation. Cette considération s'applique aussi bien au matériel qu'au logiciel du système. Ces erreurs ne peuvent être découvertes qu'en vérifiant minutieusement l'exécution correcte de chaque fonction.

De plus le fait d'injecter des pannes ou des erreurs hypothétiques constitue une technique efficace pour augmenter le niveau de confiance de la sûreté de fonctionnement finale d'un système, telle qu'elle est obtenue à l'issue des phases de conception, de spécification et de réalisation. Ces techniques d'injection de pannes (utilisant du matériel et/ou un logiciel conçu spécialement) sont utilisées pour découvrir quelles sont les conséquences globales sur la ou les tâches du système de telles pannes ou erreurs hypothétiques.

Il faut toutefois reconnaître que cette augmentation de confiance est limitée dans la pratique, car le nombre d'essais qui peuvent être conçus et effectués sera étroitement lié au nombre d'erreurs ou de pannes potentielles auxquelles on peut penser et que l'on peut injecter.

### 8.2 *Techniques d'appréciation qualitative*

L'appréciation qualitative est basée sur une analyse prédictive ou sur des essais.

Dans les deux cas il est nécessaire de débuter l'appréciation par une analyse de l'architecture fonctionnelle et matérielle du système et de la manière dont les tâches sont exécutées par le système.

L'architecture du système peut être décrite par des schémas blocs fonctionnels et matériels, des schémas de flux de signaux, des graphes d'états, des tableaux, etc.

## 8 Evaluation techniques

### 8.1 *General*

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

The techniques selected may be analytical using only the system documentation, or they may be empirical, requiring access to a built system.

The results provided by alternative evaluation techniques may be quantitative or qualitative, or a combination of these.

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.

A list of items to be considered for the assessment can be found in IEC 863. 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 (using hardware and/or specially designed software) are used to discover what is the overall consequence upon the system task(s) of such hypothetical faults or errors.

It must 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.

### 8.2 *Qualitative evaluation techniques*

Qualitative evaluation is based on a predictive analysis or on tests.

In both cases, it is necessary to start the evaluation with an analysis of the functional and physical structure of the system and how the tasks are performed by the system.

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

On prend en compte les modes de défaillance pour tous les éléments du système (matériels et logiciels). Leurs effets sur la sûreté de fonctionnement de la ou des tâches attribuées au système ainsi que l'influence des exigences pour la maintenabilité sont déterminés.

L'analyse qualitative peut être réalisée en utilisant une des méthodes ou une combinaison des méthodes suivantes.

8.2.1 *Analyse inductive*

Les modes de défaillance au niveau du composant ou de l'élément sont identifiés et pour chacun de ces modes on analyse au niveau immédiatement supérieur les effets correspondants sur la sûreté de fonctionnement de la ou des tâches du système. Les effets résultants de ces défaillances deviennent les modes de défaillance du niveau immédiatement supérieur.

Cette approche «ascendante» constitue une méthode fastidieuse qui finalement apporte, à tous les niveaux du système, une identification des effets de tous les modes de défaillance supposés.

Une méthode convenable d'analyse inductive est décrite dans la CEI 812.

8.2.2 *Analyse déductive*

Partant d'une hypothèse de défaillance au plus haut niveau du système, c'est-à-dire la défaillance d'une tâche, l'analyse déductive examine les niveaux inférieurs successifs.

Le niveau immédiatement inférieur est analysé pour identifier les modes de défaillance et les défaillances associées qui conduisent à la défaillance du niveau supérieur, c'est-à-dire du niveau de la tâche.

L'analyse est répétée en remontant les chemins fonctionnels et physiques du système jusqu'à ce que cette analyse fournisse suffisamment d'informations en termes de sûreté de fonctionnement (maintenabilité comprise) pour mener l'évaluation.

L'analyse déductive ne fournit pas d'informations concernant les modes de défaillance qui n'ont pas été pris en compte en tant qu'événements. Elle est par contre très efficace pour les systèmes complexes, pour lesquels il vaut mieux décrire ce qui est pris en compte en tant que défaillance ou comportement correct du système plutôt que de considérer tous les modes de défaillance possibles des éléments constitutifs du système.

Une méthode convenable d'analyse déductive est décrite dans la CEI 1025.

8.3 *Techniques d'appréciation quantitative*

Une appréciation quantitative peut se baser sur une analyse et des calculs prédictifs ou sur des essais.

Dans les deux cas, il est nécessaire de débuter l'appréciation par une analyse de l'architecture fonctionnelle et matérielle du système ainsi que de la manière dont les tâches sont exécutées par le système.

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

Qualitative analysis can be performed using one or a combination of the following methods.

8.2.1 *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 analyzed. 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 812.

8.2.2 *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 lower level is analyzed 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 1025.

8.3 *Quantitative evaluation techniques*

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

In both cases, it is necessary to start the evaluation with an analysis of the functional and physical structure of the system and how the tasks are performed by the system.

L'architecture du système peut être décrite par des schémas blocs fonctionnels et matériels, des schémas de flux de signaux, des graphes d'états, des tableaux, etc.

Les modes de défaillance pour tous les éléments du système (matériels et logiciels) sont pris en compte. On détermine leurs effets sur la sûreté de fonctionnement de la ou des tâches attribuées au système ainsi que l'influence des exigences pour la maintenabilité.

L'analyse quantitative peut être réalisée en utilisant une des méthodes ou une combinaison des méthodes suivantes.

8.3.1 *Appréciation prédictive*

Une appréciation prédictive s'appuie sur une analyse qualitative qui est complétée par une quantification de la fiabilité (taux de défaillance) des éléments du système pris individuellement. Pour quantifier le taux de défaillance d'un système dans l'accomplissement de sa ou ses tâches, une méthode d'analyse prédictive est utilisée. Celle qui est décrite dans la CEI 1078 est une méthode convenable.

Un schéma bloc de fiabilité peut pratiquement être construit directement à partir de l'architecture fonctionnelle et matérielle du système. La méthode est principalement orientée vers une analyse de réussite (deux états) et ne traite pas efficacement des stratégies complexes de réparation et de maintenance ni des situations à états multiples.

Pour effectuer les calculs des taux de défaillance, il existe de nombreux outils mathématiques tels que l'algèbre booléenne, les tables de vérité et/ou les méthodes des chemins et coupes. Pour prédire de manière quantitative les taux de défaillance d'un système dans l'exécution de sa ou ses tâches dans une situation à états multiples, on peut utiliser une méthode telle que celle décrite dans la CEI 1165.

Toutefois la méthode d'analyse markovienne devient très complexe si l'on doit prendre en compte un grand nombre d'états du système. Dans de tels cas il est plus efficace d'appliquer l'analyse markovienne pour calculer les données de fiabilité sur des modèles d'analyse intermédiaires déterminés à partir de l'une des autres méthodes, telle que «l'analyse par arbre de panne».

Il est possible d'obtenir des données d'entrée quantifiées pour les modules et les éléments utilisés dans les méthodes d'analyse décrites ci-dessus à partir du retour d'expérience ou par la méthode de calcul «prédiction de fiabilité par décompte des parties» en utilisant des données génériques pour les composants des modules et éléments. La méthode de prédiction de fiabilité par décompte des parties est décrite dans la CEI 1132.

Pour prendre en compte les niveaux de contraintes dues aux conditions d'influence, il convient d'utiliser la méthode décrite dans le projet de comité CEI 56 (Secrétariat)383: *Utilisation des données de taux de panne requises pour l'évaluation de la fiabilité du matériel électronique – Conditions de référence – Modèles sous contrainte en vue de leur conversion* (à l'étude), listé en annexe D.

La méthode par décompte des parties est basée sur l'hypothèse que les composants sont fonctionnellement connectés en série (estimation du pire cas). On établit la liste des composants faisant partie de chaque module et élément du système, en précisant pour chacun son type, son taux de défaillance adéquat, les facteurs influençant le taux de défaillance (qualité, environnement, etc.) et le nombre d'exemplaires utilisés.

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

Quantitative evaluations can be performed using one or a combination of the following methods.

8.3.1 *Predictive evaluation*

A predictive evaluation is based on a qualitative analysis complemented with quantification of the basic reliability (failure rates) of the system elements. To quantify the failure rate of the system to perform its task(s), a predictive analysis method is required. An appropriate method is that described in IEC 1078.

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 that described in IEC 1165 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 1132.

To account for stress levels due to influencing conditions the method described in IEC committee draft 56(Secretariat)383: *Use of failure rate data intended for reliability prediction of components in electronic equipment – Reference conditions – Stress models for their conversion* (under consideration), listed in annex D, 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 system modules 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.

Par ailleurs, on peut trouver des valeurs génériques de taux de défaillance dans le Recueil de Normes militaires Américaines MIL-HDBK-217 éditions A à F: *Prévision de la fiabilité des équipements électroniques*, listé en annexe D.

Pour des systèmes complexes tels que les systèmes de mesure et commande des processus industriels, il est en pratique impossible d'effectuer, avec précision, une évaluation prédictive des propriétés de sûreté de fonctionnement.

Cependant il est possible d'effectuer des prédictions précises mais partielles pour la fiabilité de certaines parties du système qui sont exploitées en nombre suffisant, ce qui permet de rassembler des données de retour d'expérience ayant une signification statistique.

Le degré de maintenabilité, de sûreté et d'intégrité du système dépend principalement de dispositifs conçus dans le système même et donc le degré de leur existence ne peut être calculé de manière probabiliste. La fiabilité des éléments utilisés pour assurer la sûreté et l'intégrité doit être prise en considération. Les méthodes utilisées pour évaluer la fiabilité de ces éléments peuvent être les mêmes que celles utilisées pour les éléments et les modules supportant les fonctions principales du système.

8.3.2 *Essais permettant d'apprécier la sûreté de fonctionnement*

8.3.2.1 *Introduction*

S'appuyer uniquement sur des essais au niveau du système pour mesurer la fiabilité et la disponibilité d'un système complexe n'est ni réalisable ni rentable. En général les systèmes complexes sont uniques (le nombre d'exemplaires est égal à un). De plus, la couverture de tels essais serait nécessairement fortement contrainte par le temps alloué pour les essais. Cependant de tels essais fournissent des informations précieuses pour des systèmes qui fonctionnement déjà.

Les données concrètes obtenues de cette manière sont utiles car elles fournissent:

– un guide pour l'amélioration des conceptions futures, de l'architecture du système, la reconception ou le remplacement de matériel et de logiciel enclin aux défaillances;

– une comparaison des caractéristiques attendues ou spécifiées avec des données réelles;

– une base de données de retour d'expérience qui peut être utilisée pour des prédictions futures en matière de sûreté de fonctionnement.

Des guides sur les procédures à suivre lorsque l'on définit des essais se trouvent dans la CEI 1070 et la CEI 300-3-2.

La raison principale pour effectuer des essais sur des systèmes est d'apprécier le comportement d'un système en présence d'une panne (matérielle ou logicielle) ou en cas d'entrée non autorisée ou incorrecte (intégrité et sûreté).

Pour observer le comportement d'un système, il faut définir une tâche ou un ensemble de tâches représentatives et pour chaque tâche il faut définir les états du système qui sont considérés comme une défaillance (par exemple l'état de la ou des sorties). Des guides sur le traitement de ces essais se trouvent dans la CEI 706-4.

Alternatively generic failure data may be found in the US Military Standardization Handbook MIL-HDBK-217 issues A through F: *Reliability prediction of electronic equipment*, listed in annex D.

For complex systems, such as industrial-process measurement and control systems, it is impossible in practice to make an accurate predictive assessment of the dependability properties.

Accurate partial predictions on reliability can, however, be made for those parts of the system of which there is a sufficient number in operation to be able to gather field data of statistical significance.

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.

8.3.2 *Tests to evaluate dependability*

8.3.2.1 *Introduction*

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 to be followed when defining tests can be found in IEC 1070 and IEC 300-3-2.

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 (e.g. state of the output(s)). Guidance on the treatment of these tests can be found in IEC 706-4.

8.3.2.2 *Essais utilisant les techniques d'injection de pannes*

Avant d'engager les essais par injection de pannes, il faut examiner les spécifications du système afin de déterminer:

- les mesures d'intégrité prises pour éviter la propagation des pannes dans le système;
- les mesures de sûreté prises pour éviter l'intrusion d'entrées incorrectes ou non autorisées;
- les dispositifs de diagnostic existants.

Afin d'atteindre une bonne efficacité, la conception des essais du système doit s'appuyer sur une analyse qualitative et autant que possible utiliser les dispositifs de diagnostic procurés par et fournis pour le système. Il faut prendre garde à ce que, lorsque ces dispositifs de diagnostic sont nécessaires à la sûreté de fonctionnement du système, ceux-ci soient essayés indépendamment.

Pour vérifier l'intégrité, on peut injecter des pannes dans le ou les modules, le ou les éléments, et/ou le ou les composants et observer si oui ou non:

- les sorties du système sont défaillantes; et/ou
- la panne est signalée.

Pour vérifier la sûreté, des pannes ou des informations non autorisées peuvent être injectées aux frontières du système, c'est-à-dire des entrées incorrectes, des erreurs humaines correspondant aux activités de conduite ou de maintenance.

Il faut veiller à introduire simultanément quelques essais portant sur l'intégrité et la sécurité. Le seul effet d'une panne à l'intérieur d'un système peut être d'empêcher la détection d'une panne sur une entrée. L'annexe C détaille de nombreuses pannes qui peuvent être injectées lors de l'exécution de ces essais.

8.3.2.3 *Essais utilisant des perturbations de l'environnement*

Certaines perturbations des conditions d'influence vont déclencher les mécanismes de sécurité.

Pour essayer les mécanismes de sécurité, il convient donc de choisir certaines conditions d'influence que l'on fait évoluer autour de leur valeur normale.

Pour la sélection des conditions d'influence, on se référera à 7.2.2.

## 9 Exécution et rédaction du rapport d'évaluation

L'exécution et la rédaction du rapport d'évaluation doivent être conformes à 5.5 et 5.6 de la CEI 1069-1.

Il convient que le rapport d'évaluation aborde également les points suivants:

a) les prévisions pour l'évaluation associées aux écarts qui sont apparus;

b) les données extraites du cahier des charges et du cahier des spécifications du système, telles que les tâches attribuées au système, les exigences de sûreté de fonctionnement, les conditions d'environnement, de fonctionnement et de maintenance, etc.;

8.3.2.2 *Tests by fault-injection techniques*

Prior to testing by fault injection, the system specification shall 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 shall be based on a qualitative analysis and, as far as possible, shall use the diagnostic features provided by and for the system. Care shall 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) and observations made of whether or not:

- 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 shall be taken to include some simultaneous tests of both integrity and security. The only effect of a fault within a system may be the prevention of the detection of an input fault. Annex C lists a number of faults which may be introduced when executing these tests.

8.3.2.3 *Tests by environmental perturbations*

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

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

For the selection of the influencing conditions refer to 7.2.2.

## 9 Execution and reporting of the assessment

The execution and reporting of the assessment shall be in accordance with 5.5 and 5.6 of IEC 1069-1.

The assessment report should also address the following points:

a) the assessment plan together with the necessary deviations;

b) the collation of data from the system requirements document and system specification document such as system tasks, dependability requirements, environmental, operational, and maintenance, conditions, etc.;

c) l'analyse du système;

– la structure matérielle et fonctionnelle du système, les contraintes appliquées aux modules, éléments et composants du système, les raisons du choix du ou des modèles pour l'évaluation des différents aspects de la sûreté de fonctionnement;

d) l'adaptation du modèle;

– l'adaptation des modèles, si cela est nécessaire pour une prévision, en tenant compte de la précision demandée;

e) l'origine des données, par exemple les sources de données utilisées pour les modèles mathématiques;

f) les calculs rapportés avec précision des résultats;

g) le ou les essais effectués:

– la description de l'essai et les raisons ayant conduit à son choix;

– les modes de défaillance simulés;

– le comportement attendu suite à l'analyse qualitative;

– l'estimation de la fréquence de défaillance suite à l'analyse quantitative;

– le type de pannes injectées dans le système pour vérifier l'intégrité et la sûreté, pour simuler la défaillance d'un module, d'un élément ou d'un composant, telles que pannes introduites par les éléments d'entrée/sortie, pannes dues à des erreurs humaines (par exemple en tant que résultats d'une activité de maintenance), pannes introduites en tant que résultats d'une mauvaise utilisation (par exemple utilisation de codes invalides);

– la nature et le niveau des conditions d'influence appliquées aux limites du système;

– la couverture des pannes;

– le temps d'identification de la panne;

– le confinement de la panne (recouvrement de la panne);

– le temps de localisation de la panne;

– la vérification de l'exactitude des diagnostics en ligne, par exemple si des fausses alarmes, des pannes se rapportant au fonctionnement du processus, etc. sont ou non reconnues comme telles, et/ou si ces pannes sont identifiées de manière erronée;

h) une liste des activités d'évaluation recommandées pour approfondir les analyses et/ou les essais.

c) analysis of the system;

– physical and functional structure of the system, stresses applied to the system-modules, elements and components, rationale behind the chosen model(s) for the different aspects of dependability assessment;

d) model adaptation;

– adaptation of the models, if necessary for predictive purposes, taking into account the accuracy required;

e) data acquisition, e.g. sources used for the mathematical models;

f) calculations should be reported with the accuracy of the results;

g) executed test(s):

– description of the test and rationale behind the choice of the tests;

– failure modes simulated;

– expected behaviour from qualitative analysis;

– expected frequency of failure occurrence as derived from the quantitative analysis;

– the type of faults injected into the system to test the integrity and security, to simulate the failure of a module, element or component, such as faults introduced via the input/output elements, faults due to human errors (e.g. as a result of a maintenance activity), faults introduced as a result of misuse (e.g. use of illegal codes);

– the nature and level of the influencing conditions applied at the system boundaries;

– fault coverage;

– fault recognition time;

– isolation of fault (fault resolution);

– fault localization time;

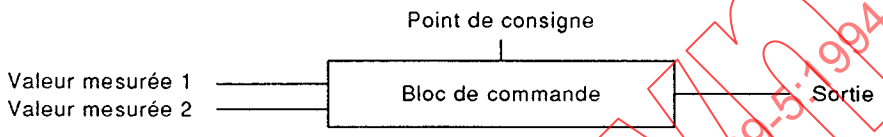
– checking the correctness of the on-line diagnostics, e.g. whether or not false alarms, system faults relevant to operation of process, etc. are recognized as such, and/or such faults are erroneously identified;

h) a list of assessment activities recommended for further analysis and/or tests.

# Annexe A
(informative)

## Exemple de prescriptions et de mise en forme de documentation pour une tâche commande maître-esclave dans un cahier des charges de système

### A.1 Schéma de principe de la tâche




### A.2 Etats à la limite du système

Etats possibles des entrées:

- valeur mesurée 1: > haut, normal, < bas
- valeur mesurée 2: > haut, normal, < bas
- point de consigne: > haut, normal, < bas

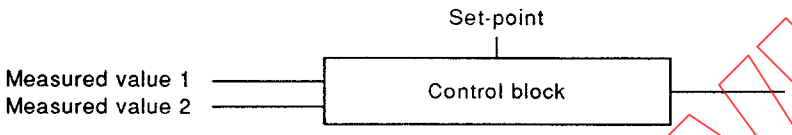
Etats possibles de la ou des sorties:

- sortie: pleine ouverture, gelé, flottant, pleine fermeture.

# Annex A
(informative)

# Example of required information and documentation format for a master-slave control task in a system requirements document

## A.1 Schematic of task




## A.2 Boundary states

Possible states of inputs:

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

Possible states of output(s):

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

**Tableau A.1 – Sûreté de fonctionnement**

| Tâche | | Mode | Evénement de défaillance | | |
|---|---|---|---|---|---|
| | | | Fréquence attendue | Action à prendre | Temps de remise en état |
| Maître-esclave | Entrée | Mesure 1 | | | |
| | | > haut | 1 par an | Rapport/gel sortie | * |
| | | normal | NA | — | — |
| | | < bas | 1 par an | Rapport/gel sortie | * |
| | | Mesure 2 | | | |
| | | > haut | 1 par an | Rapport/gel dernière valeur | * |
| | | normal | NA | — | — |
| | | < bas | 1 par an | Rapport/sortie à haut | * |
| | | Point de consigne | | | |
| | | > haut | 1 par an | Rapport/gel dernière valeur | 2 h |
| | | normal | NA | — | — |
| | | < bas | 1 par an | Rapport/sortie à haut | 2 h |
| | Sortie | Sortie | | | |
| | | > haut | 1 par an | Rapport/gel dernière valeur | 2 h |
| | | normal | NA | — | — |
| | | < bas | 1 par an | Rapport/gel dernière valeur | 2 h |

NOTES

1 Suivant la limite du système évalué, les éléments de mesure peuvent ou non faire partie du système. Dans le cas de cet exemple, les mesures sont extérieures à la limite et donc le terme fréquence «attendue» de l'événement est simplement noté, de même le «temps de remise en état» n'est pas une considération propre au système. Le point de consigne est commandé à partir du clavier et fait donc partie du système.

2 NA = non applicable.

3 * = Cette grandeur n'est pas une considération propre au système.

## Table A.1 – Dependability

| Task | | Mode | Failure event | | |
|---|---|---|---|---|---|
| | | | Expected frequency | Action to be taken | Time to restore |
| Master-slave | Input | Measurement 1 | | | |
| | | > high | 1 per year | Report/freeze output | * |
| | | normal | NA | — | — |
| | | < low | 1 per year | Report/freeze output | * |
| | | Measurement 2 | | | |
| | | > high | 1 per year | Report/freeze last value | * |
| | | normal | NA | — | — |
| | | < low | 1 per year | Report/output to high | * |
| | | Set-point | | | |
| | | > high | 1 per year | Report/freeze last value | 2 h |
| | | normal | NA | — | — |
| | | < low | 1 per year | Report/output to high | 2 h |
| | Output | Output | | | |
| | | > high | 1 per year | Report/freeze last value | 2 h |
| | | normal | NA | — | — |
| | | < low | 1 per year | Report/freeze last value | 2 h |

NOTES

1 Depending on the boundary of the system under assessment, the inputs from measurements may or may be not under control of the system. In the case of the example, the measurements are outside the boundary and hence the term "expected" frequency of event is noted, equally the "time to restore" is not a system consideration. The set-point is controlled via a keyboard and hence under system control.

2 NA = non applicable.

3 * = This quantity is not a system property.