

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
706-5**

Première édition
First edition
1994-11

Guide de maintenabilité de matériel –

Partie 5:

Section 4: Essais pour diagnostic

Guide on maintainability of equipment –

Part 5:

Section 4: Diagnostic testing



Numéro de référence
Reference number
CEI/IEC 706-5: 1994

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 auprès du Bureau Central de la CEI.

Les renseignements relatifs à ces révisions, à l'établissement des éditions révisées et aux amendements peuvent être obtenus auprès des Comités nationaux de la CEI et dans les documents ci-dessous:

- **Bulletin de la CEI**
- **Annuaire de la CEI**
Publié annuellement
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement

Terminologie

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 50: *Vocabulaire Electrotechnique International* (VEI), qui se présente sous forme de chapitres séparés traitant chacun d'un sujet défini. Des détails complets sur le VEI peuvent être obtenus sur demande. Voir également le dictionnaire multilingue de la CEI.

Les termes et définitions figurant dans la présente publication ont été soit tirés du VEI, soit spécifiquement approuvés aux fins de cette publication.

Symboles graphiques et littéraux

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera:

- la CEI 27: *Symboles littéraux à utiliser en électro-technique;*
- la CEI 417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles;*
- la CEI 617: *Symboles graphiques pour schémas;*

et pour les appareils électromédicaux,

- la CEI 878: *Symboles graphiques pour équipements électriques en pratique médicale.*

Les symboles et signes contenus dans la présente publication ont été soit tirés de la CEI 27, de la CEI 417, de la CEI 617 et/ou de la CEI 878, soit spécifiquement approuvés aux fins de cette publication.

Publications de la CEI établies par le même comité d'études

L'attention du lecteur est attirée sur les listes figurant à la fin de cette publication, qui énumèrent les publications de la CEI préparées par le comité d'études qui a établi la présente publication.

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 from the IEC Central Office.

Information on the revision work, the issue of revised editions and amendments may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **IEC Yearbook**
Published yearly
- **Catalogue of IEC publications**
Published yearly with regular updates

Terminology

For general terminology, readers are referred to IEC 50: *International Electrotechnical Vocabulary* (IEV), which is issued in the form of separate chapters each dealing with a specific field. Full details of the IEV will be supplied on request. See also the IEC Multilingual Dictionary.

The terms and definitions contained in the present publication have either been taken from the IEV or have been specifically approved for the purpose of this publication.

Graphical and letter symbols

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications:

- IEC 27: *Letter symbols to be used in electrical technology;*
- IEC 417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets;*
- IEC 617: *Graphical symbols for diagrams;*

and for medical electrical equipment,

- IEC 878: *Graphical symbols for electromedical equipment in medical practice.*

The symbols and signs contained in the present publication have either been taken from IEC 27, IEC 417, IEC 617 and/or IEC 878, or have been specifically approved for the purpose of this publication.

IEC publications prepared by the same technical committee

The attention of readers is drawn to the end pages of this publication which list the IEC publications issued by the technical committee which has prepared the present publication.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
706-5**

Première édition
First edition
1994-11

Guide de maintenabilité de matériel –

Partie 5:

Section 4: Essais pour diagnostic

Guide on maintainability of equipment –

Part 5:

Section 4: Diagnostic testing

© CEI 1994 Droits de reproduction réservés — Copyright — all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

Bureau Central de la Commission Electrotechnique Internationale 3, rue de Varembe Genève, Suisse



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

U

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

SOMMAIRE

	Pages
AVANT-PROPOS	4
INTRODUCTION	8
Articles	
1 Domaine d'application	10
2 Références normatives	10
3 Définitions et abréviations	12
3.1 Définitions	12
3.2 Abréviations	14
4 Exigences et contraintes techniques.....	14
4.1 Coût du cycle de vie	14
4.2 Concepts d'exploitation et de maintenance	16
4.3 Concept de diagnostic	16
5 Exigences d'un programme de testabilité.....	34
5.1 Conception de la testabilité.....	34
5.2 Vérification de la testabilité.....	36
5.3 Documentation de testabilité.....	36
6 Etablissement de contrats pour la testabilité.....	38
6.1 Définition d'exigences.....	38
6.2 Spécification de testabilité.....	40
6.3 Conséquences.....	40
Annexes	
A Concepts mathématiques dans les essais pour diagnostic.....	42
B Bibliographie.....	52

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	9
Clause	
1 Scope	11
2 Normative references	11
3 Definitions and acronyms	13
3.1 Definitions	13
3.2 Acronyms	15
4 Technical requirements and constraints	15
4.1 Life cycle cost	15
4.2 Operational and maintenance concepts	17
4.3 Diagnostic concept	17
5 Testability programme requirements	35
5.1 Testability engineering	35
5.2 Testability verification	37
5.3 Testability documentation	37
6 Contracting for testability	39
6.1 Statement of requirements	39
6.2 Testability specification	41
6.3 Consequences	41
Annexes	
A Mathematical concepts in diagnostic testing	43
B Bibliography	53

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GUIDE DE MAINTENABILITÉ DE MATÉRIEL –

Partie 5: Section 4: Essais pour diagnostic

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 les conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparées 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 706-5 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

DIS	Rapports de vote
56(BC)157	56(BC)171
56(BC)160	56(BC)173

Les rapports de vote indiqués dans le tableau ci-dessus donnent toute information sur le vote ayant abouti à l'approbation de cette norme.

La CEI 706 comprend les parties suivantes, présentées sous le titre général: *Guide de maintenabilité de matériel*.

La partie 1, publiée en 1982, comprend les sections suivantes:

Section un – Introduction à la maintenabilité

Section deux – Exigences de maintenabilité dans les spécifications et les contrats

Section trois – Programme de maintenabilité

La partie 2, publiée en 1990, comprend la section suivante:

Section cinq – Etudes de maintenabilité au niveau de la conception

La partie 3, publiée en 1987, comprend la section suivante:

Section six – Vérification de la maintenabilité

Section sept – Recueil, analyse et présentation des données relatives à la maintenabilité

La partie 4, publiée en 1992, comprend la section suivante:

Section 8 – Planification de la maintenance et de la logistique de maintenance

INTERNATIONAL ELECTROTECHNICAL COMMISSION

GUIDE ON MAINTAINABILITY OF EQUIPMENT –

Part 5: Section 4: Diagnostic testing

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a world-wide 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 706-5 has been prepared by IEC technical committee 56: Dependability.

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

DIS	Reports on voting
56(CO)157	56(CO)171
56(CO)160	56(CO)173

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

IEC 706 consists of the following parts, under the general title: *Guide on maintainability of equipment*.

Part 1, issued in 1982, contains the following sections:

- Section one – Introduction to maintainability
- Section two – Maintainability requirements in specifications and contracts
- Section three – Maintainability programme

Part 2, issued in 1990, contains the following section:

- Section five – Maintainability studies during the design phase

Part 3, issued in 1987, contains the following sections:

- Section six – Maintainability verification
- Section seven – Collection, analysis and presentation of data related to maintainability

Part 4, issued in 1992, contains the following section:

- Section 8 – Maintenance and maintenance support planning

La partie 5, publiée en 1994, comprend la section suivante:

Section 4 – Essais pour diagnostic

La partie 6, publiée en 1994, comprend la section suivante:

Section 9 – Méthodes statistiques pour l'évaluation de la maintenabilité

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

IECNORM.COM: Click to view the full PDF of IEC 60706-5:1994
Withdrawn

Part 5, issued in 1994, contains the following section:

Section 4 – Diagnostic testing

Part 6, issued in 1994, contains the following section:

Section 9 – Statistical methods in maintainability evaluation

Annexes A and B are for information only.

Withdr2wn
IECNORM.COM: Click to view the full PDF of IEC 60706-5:1994

INTRODUCTION

Les essais pour diagnostic sont un élément important pour l'exploitation et la maintenance d'un système ou d'un équipement, et ont un effet significatif sur sa maintenabilité. De tels essais peuvent être effectués manuellement ou bien à l'aide d'équipements de test qui peuvent être dotés de divers niveaux d'automatisation. La conception optimale d'un processus d'essais pour diagnostic nécessite une étroite coopération entre les organisations de conception, d'exploitation et de maintenance. Ce guide a pour but de mettre en lumière les diverses exigences et d'assurer leur coordination dans le temps.

IECNORM.COM: Click to view the full PDF of IEC 60706-5:1994

Withdrawn

INTRODUCTION

Diagnostic testing is an important feature in the operation and maintenance of a system or equipment and has a significant effect on its maintainability. Such testing may be carried out manually or with test equipment which may contain various levels of automation. Optimum design of a diagnostic testing process requires close cooperation between the design, operation and maintenance organizations. This guide is intended to highlight the various requirements and to assist in their timely coordination.

Withdr2Wm
IECNORM.COM: Click to view the full PDF of IEC 60706-5:1994

GUIDE DE MAINTENABILITÉ DE MATÉRIEL –

Partie 5: Section 4: Essais pour diagnostic

1 Domaine d'application

La présente Norme internationale est la section 4 du Guide de maintenabilité de matériel. Ce guide a pour but de:

- fournir des indications pour la prise en considération, très tôt, des aspects de testabilité en conception et développement;

NOTE – La conception d'un dispositif doit faciliter et aider les essais pour diagnostic, et ceci peut être réalisé le plus efficacement en prenant en considération les aspects de testabilité aussi tôt que possible dans le processus de conception, généralement conjointement avec l'analyse des modes de défaillance et de leurs effets (AMDE). Si ces aspects de testabilité sont repoussés à plus tard, dans des phases ultérieures du projet, lorsque la conception a été finalisée, seul un nombre très limité de caractéristiques de testabilité peut être ajouté. Ces dernières seront moins efficaces et conduiront de façon disproportionnée à des coûts élevés.

- aider dans la détermination de procédures de test efficaces en tant que partie intégrante de l'exploitation et de la maintenance.

NOTE - Le concept d'exploitation et de maintenance dépendra, dans une certaine mesure, de la philosophie de conception et, par conséquent, afin de s'assurer qu'une pleine utilisation des possibilités d'essais de diagnostic peut être effectuée, il convient que les exigences d'essai soient incluses dans la politique d'exploitation et de maintenance, et qu'elles soient développées comme partie intégrante du processus de conception.

La présente section de la CEI 706 est applicable à toutes les catégories d'équipements dans leur conception et leurs principes, bien que nombre des techniques décrites soient indubitablement plus applicables aux domaines de l'électricité et de l'électronique, car c'est dans ces domaines qu'il existe la plus grande opportunité de les appliquer. Pour les équipements mécaniques, les techniques traditionnelles de diagnostic peuvent toujours être utilisées mais, là également, les progrès réalisés sur les dispositifs électroniques de mesure et de contrôle signifient que des moyens d'essais pour diagnostic notablement améliorés peuvent maintenant être appliqués aux composants et systèmes mécaniques complexes. Ceci fait qu'il est particulièrement important que la méthode d'approche structurée proposée pour fournir des moyens d'essais pour diagnostic soit utilisée pour une large gamme de tâches.

Dans cette section, il est fait référence au pilotage des conditions. C'est un aspect qui est en relation étroite avec les concepts couverts par ce guide sur les essais pour diagnostic, et qui ne peut pas et ne doit pas en être dissocié. Cependant, il n'est pas prévu qu'une couverture complète des aspects de pilotage de conditions soit assurée dans ce guide.

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 706-5. 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 706-5 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*

GUIDE ON MAINTAINABILITY OF EQUIPMENT –

Part 5: Section 4: Diagnostic testing

1 Scope

This International Standard is being issued as Section 4 of the guide on maintainability of equipment. Its purpose is to:

- provide guidance for the early consideration of testability aspects in design and development;

NOTE – The design of an item should facilitate and support diagnostic testing, and this can be achieved most efficiently by considering testability aspects as early as possible in the design process, usually in conjunction with a fault mode and effects analysis (FMEA). If left till later project phases, when the design has been finalized, only very limited testability features may be added. These will be less effective and will involve disproportionately high costs.

- assist in determining effective test procedures as an integral part of operation and maintenance.

NOTE – The operational and maintenance concept will depend to a certain extent on the design philosophy, and therefore to ensure that full use can be made of the diagnostic testing possibilities, test requirements should be included in the operational and maintenance policy and be developed as an integral part of the design process.

This section of IEC 706 is applicable to all categories of equipment in their concept and principles, although many of the techniques described are clearly more applicable to the electrical and electronic fields, as it is in those areas where there is the greatest opportunity for them to be applied. For mechanical equipment, the traditional diagnostic techniques can still be used, but here too the advances being made in electronic measuring and monitoring devices mean that much improved diagnostic testing facilities can now be applied to mechanical components and complex systems. This makes it particularly important that the structured approach given for the provision of diagnostic testing facilities is used for a wide range of tasks.

Reference is made in this section to condition monitoring. This is a facility which closely relates to the concepts covered in this guide on diagnostic testing, and cannot, and should not, be dissociated from it. However, it is not the intention that full coverage of condition monitoring should be part of this standard.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this section of IEC 706-5. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this section of IEC 706-5 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*

CEI 706-3: 1987, *Guide de maintenabilité de matériel – Troisième partie: Sections six et sept – Vérification et recueil, analyse et présentation des données*

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

ISO 3534-1: 1993, *Statistique – Vocabulaire et symboles – Partie 1: Probabilité et termes statistiques généraux*

3 Définitions et abréviations

3.1 Définitions

Pour les besoins de la présente section de la CEI 706-5, les termes et les définitions de la CEI 50(191) et de l'ISO 3534-1 s'appliquent. En supplément, les termes et définitions suivants s'appliquent.

3.1.1 test intégré (TI): Capacité intrinsèque du système ou équipement opérationnel fournissant une possibilité de test pour détecter et localiser les pannes ou les diminutions de performances.

3.1.2 équipement de test intégré (ETI): Dispositif quelconque monté en permanence dans le but de réaliser la fonction TI.

3.1.3 diagnostic: Méthode ou acte de recherche de la nature d'une panne à partir de symptômes.

3.1.4 exactitude de diagnostic: Proportion de pannes, dans un dispositif, pouvant être correctement diagnostiquées dans des conditions données.

3.1.5 essais pour diagnostic: Procédure d'essais réalisés dans le but d'établir un diagnostic.

3.1.6 fausse alarme: Panne indiquée par l'équipement de test intégré ou tout autre circuit de contrôle, alors qu'il n'existe pas de panne fonctionnelle.

3.1.7 taux de fausse alarme: Nombre de fausses alarmes par unité de temps.

3.1.8 temps de détection de panne: Durée écoulée entre l'instant de la défaillance et la détection de la panne.

3.1.9 résolution de panne: Degré jusqu'auquel un programme ou une procédure de test peut localiser une panne à l'intérieur d'un système ou d'un équipement.

3.1.10 testabilité: Caractéristique qualitative de conception qui détermine le degré jusqu'auquel un dispositif peut être testé dans des conditions données.

3.1.11 exigences de testabilité: Ensemble d'objectifs, buts, seuils et contraintes globaux de conception de testabilité.

3.1.12 vérification de testabilité: Procédure appliquée dans le but de déterminer si les exigences de testabilité d'un dispositif ont été satisfaites ou non.

3.1.13 efficacité de test: Ensemble des mesures qui incluent la prise en considération de la conception du matériel, de la conception du TI, de la conception de l'équipement d'essais et de la conception de l'ensemble du programme d'essais (EPE). Les mesures d'efficacité de test comprennent, sans y être limitées, la couverture de pannes, la résolution de pannes, le temps moyen de détection de panne, le temps moyen de localisation de panne et l'exactitude de diagnostic.

IEC 706-3: 1987, *Guide on maintainability of equipment – Part 3: Sections Six and Seven – Verification and collection, analysis and presentation of data*

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

ISO 3534-1: 1993, *Statistics – Vocabulary and symbols – Part 1: Probability and general statistical terms*

3 Definitions and acronyms

3.1 Definitions

For the purposes of this section of IEC 706-5, the terms and definitions of IEC 50(191) and ISO 3534-1 apply. In addition, the following terms and definitions are used.

3.1.1 **built-in test (BIT):** An intrinsic capability of the mission system or equipment which provides a test capability to recognize and localize faults or deterioration of performance.

3.1.2 **built-in test equipment (BITE):** Any permanently mounted device intended to perform the built-in test function.

3.1.3 **diagnosis:** The art or act of deciding from symptoms the nature of a fault.

3.1.4 **diagnostic correctness:** The proportion of faults of an item which can be correctly diagnosed under given conditions.

3.1.5 **diagnostic testing:** Test procedure carried out in order to make a diagnosis.

3.1.6 **false alarm:** A fault indicated by built-in test equipment or other monitoring circuitry where no functional fault exists.

3.1.7 **false alarm rate:** Number of false alarms per unit of time.

3.1.8 **fault recognition time:** The period of time between the instant of failure and fault recognition.

3.1.9 **fault resolution:** The degree to which a test programme or procedure can localize a fault within a system or equipment.

3.1.10 **testability:** A qualitative design characteristic which determines the degree to which an item can be tested under stated conditions.

3.1.11 **testability requirements:** Set of overall testability design objectives, goals, thresholds, and constraints.

3.1.12 **testability verification:** A procedure applied for the purpose of determining whether the testability requirements for an item have been achieved or not.

3.1.13 **test effectiveness:** Set of measures which include consideration of hardware design, built-in test design, test equipment design, and test programme set design. Test effectiveness measures include, but are not limited to, fault coverage, fault resolution, mean fault recognition time, mean fault localization time, and diagnostic correctness.

3.2 Abréviations

EEA	équipement d'essais automatiques
TI	test intégré
ETI	équipement de test intégré
CFEAO	conception, fabrication et essais assistés par ordinateur
AMDE	analyse des modes de défaillance et de leurs effets
CCV	coût du cycle de vie
UI	unité d'interchangeabilité
UEE	unité en essais

4 Exigences et contraintes techniques

4.1 Coût du cycle de vie

Le coût du cycle de vie (CCV) est un aspect de plus en plus important pour l'évaluation de la qualité de toute conception. En supplément au coût d'acquisition immédiat, de nombreux clients demandent à contrôler les coûts associés à l'exploitation au quotidien, à la maintenance et à la logistique de maintenance. Ces coûts sont influencés au premier chef par la fiabilité, la maintenabilité du produit et les caractéristiques du support de maintenance. Dans ce contexte, l'application des techniques des essais pour diagnostic peut être un facteur significatif qui contribue à la réduction de certains éléments de coût du cycle de vie. Il convient que les contraintes résultant des efforts d'optimisation soient prises en compte lorsque les exigences des essais pour diagnostic sont établies.

4.1.1 Compromis initiaux

Dans les études de développement, pendant la phase de conception et de définition, il convient que la testabilité d'un produit soit comparée aux risques encourus. Dans ce contexte, il faut considérer les points suivants.

De nombreuses conceptions, bien que nouvelles, sont basées, dans une certaine mesure, sur certains équipements toujours en utilisation. De tels équipements font apparaître un certain «état de l'art» technologique reflété par la sophistication de la conception, les diagnostics techniques planifiés envisagés au moment de leur conception et des modifications effectuées pendant la vie de ces équipements, mais la nouvelle conception contiendra quelques concepts de fonctionnement différents associés aux avancées dans la technologie. La fiabilité de certains des ensembles, parties et composants, peut être telle que l'application du contrôle en fonctionnement ou des essais pour diagnostic n'est pas nécessaire, dès lors que les mêmes conditions d'utilisation s'appliquent. Au fur et à mesure que les incertitudes à cet égard augmentent, ou bien lorsque l'importance de la partie considérée nécessite garantie, l'exigence de connaissance de l'état du dispositif augmentera aussi de la même manière. D'un autre côté, il peut être possible ou conseillé d'investir dans des essais pour diagnostic spécifiques afin de minimiser les zones d'incertitude. La décision dépendra de la nature de l'incertitude, de sa probabilité d'être levée, de même que des coûts de développements et du coût du dispositif relativement au coût de l'équipement nécessaire pour diagnostiquer et contrôler le fonctionnement du dispositif en exploitation, en incluant les coûts de l'indisponibilité et du personnel de maintenance.

Il convient de prendre en considération l'«état de l'art» en essais pour diagnostic, les diverses méthodes utilisées, comprenant leurs avantages et leurs inconvénients, les coûts ainsi que les capacités d'adaptation à des exigences futures possibles, pour l'évaluation des autres solutions possibles.

3.2 Acronyms

ATE	automatic test equipment
BIT	built-in test
BITE	built-in test equipment
CADMAT	computer-aided design, manufacture and testing
FMEA	failure modes and effects analysis
LCC	life cycle cost
LRU	line replaceable unit
UUT	unit under test

4 Technical requirements and constraints

4.1 Life cycle cost

Life cycle cost (LCC) is an increasingly important aspect in evaluating the quality of any design. In addition to the immediate acquisition cost, many customers demand control of the costs associated with day-to-day operation, maintenance, and logistic support. These costs are primarily influenced by the product's reliability, maintainability and maintenance support characteristics. In this context, the application of diagnostic testing techniques can be a significant contributory factor in the reduction of certain cost elements in the LCC. Constraints resulting from LCC optimization efforts should therefore be taken into account whenever diagnostic testing requirements are established.

4.1.1 Initial trade-offs

In engineering studies during the concept and definition phase, the testability of the product should be traded against any risks involved. Typical considerations in this context are as follows.

Many designs, however new, are based to a certain extent on equipment currently in use. This equipment demonstrates a given technological "state of the art" reflected in the sophistication of the design, the planned technical diagnostics envisaged at the time it was designed, and modifications made during the life of the equipment, but the new design will involve some different operating concept associated with advances in technology. The reliability of some of the assemblies, parts and components may be such that the application of condition monitoring or diagnostic testing is not required, provided that the same conditions of usage apply. As uncertainties in this respect increase, or the importance of the subject part warrants, the requirement for knowledge of the state of the item will also increase accordingly. Alternatively, it may be possible or advisable to invest in specific design testing to minimize the areas of uncertainty. The decision will depend on the nature of uncertainty, the probability of its being solved and the development and unit costs relative to the cost of the equipment required to diagnose and monitor the condition of the item in operation, including cost of down times and maintenance personnel.

The "state of the art" in diagnostic testing, the various methods employed, including their advantages, disadvantages, costs and adaptability to possible future requirements should be considered in evaluating the alternatives.

4.1.2 Disponibilité et essais pour diagnostic

Dans la phase de conception et de développement, il convient que les principes et caractéristiques de testabilité soient intégrés dans la conception en accord avec les résultats des études initiales. Il convient de porter une attention particulière aux techniques d'essais pour diagnostic qui peuvent améliorer la maintenabilité et minimiser les temps d'indisponibilité, et donc augmenter la disponibilité ainsi que les profits, tout en diminuant les coûts globaux.

Dans le cas de dispositifs ayant des caractéristiques inhérentes d'usure, ces améliorations concernent en premier lieu le coût de la maintenance préventive, qui peut être diminué de façon significative grâce à des procédures d'essais pour diagnostic; ceci, tout particulièrement lorsque l'optimisation des intervalles entre maintenance, des ressources nécessaires et de la maintenance préventive peut être réalisée. S'il n'y a pas de processus d'usure, comme c'est le cas pour la plupart des systèmes électroniques à semi-conducteurs, le coût de maintenance préventive est négligeable, et l'impact des coûts les plus élevés est dû aux coûts d'investissement, qui sont eux-mêmes largement dépendants de la disponibilité obtenue. Dès lors que la majeure partie du temps d'indisponibilité est constituée par les temps de détection et de localisation de panne, les efforts consacrés aux diagnostics concernant ces éléments sont plus efficaces.

4.2 Concepts d'exploitation et de maintenance

Les activités d'essais pour diagnostic sont étroitement interconnectées avec les processus d'exploitation et de maintenance du produit. Il convient donc que les concepts d'exploitation et de maintenance soient définis aussitôt que possible dans le cycle de vie du système, de préférence au stade des spécifications. Il convient que le concept d'exploitation soit le premier pris en considération afin que le système satisfasse correctement à ses exigences. Il convient que le concept de maintenance soit élaboré afin de permettre de satisfaire aux besoins opérationnels avec l'utilisation la plus efficace possible des ressources pour un coût minimal. Un certain degré de compromis devra invariablement être pris en compte afin de réaliser l'équilibre optimal parmi des exigences qui peuvent parfois être contradictoires.

4.2.1 Concept d'exploitation

Les éléments qu'il convient de prendre en considération pour définir le concept d'exploitation sont indiqués dans le tableau 1. Chacun d'eux nécessite d'être spécifié en détail, de sorte que l'environnement de maintenance ainsi que les contraintes d'exploitation puissent être correctement pris en compte.

4.2.2 Concept de maintenance

Les nombreux éléments qu'il convient de prendre en considération dans la définition du concept de maintenance sont indiqués dans le tableau 2. Ce sont ces éléments qui déterminent l'exigence et l'extension des essais pour diagnostic à inclure à la conception. Un certain degré de compromis peut à nouveau être nécessaire entre le concept de maintenance et la technique de diagnostic de façon à satisfaire les nombreuses inter-dépendances mutuelles mises en jeu.

4.3 Concept de diagnostic

Avant la phase de conception et de développement, il convient qu'un concept approprié du diagnostic soit déterminé, prenant en compte les contraintes d'optimisation du coût du cycle de vie, les concepts d'exploitation et de maintenance, en accord avec les facteurs suivants:

- objectifs, tâches et applications des essais pour diagnostic;
- méthodes utilisées pour les essais de diagnostic;
- exigences pour les essais de diagnostic.

4.1.2 *Availability and diagnostic testing*

In the design and development phase, testability features and characteristics should be incorporated into the design in accordance with the results of related initial trade-off studies. Specific consideration should be given to diagnostic testing techniques having the potential of improving the product's maintainability and minimizing down time, thus increasing availability and profit and decreasing overall costs.

In the case of items with inherent wear-out characteristics, improvements affect primarily the cost of preventive maintenance, which can be significantly decreased by diagnostic test procedures, particularly where optimization of maintenance intervals and of the necessary amount of preventive maintenance work and resources can be achieved. If no wear-out is involved as is the case for most solid-state electronic systems, the cost of preventive maintenance is negligible, and the highest cost impact is caused by the capital costs, which are in turn largely dependent on the achieved availability. Since the major portion of down time is the fault recognition and localization times, emphasis on diagnostics is most effectively placed on these elements.

4.2 *Operational and maintenance concepts*

Diagnostic testing activities are closely interconnected with the processes of the product's operation and maintenance. Therefore, the operational and maintenance concepts are important factors to be considered when diagnostic testing requirements are established. They should both be defined as early as possible in the system life cycle, preferably in the concept and definition phase. The operational concept should be the first consideration in order that the system properly fulfils its requirement. The maintenance concept should be designed to allow the operational need to be met with the most efficient use of resources at minimum cost.

A degree of trade-off will invariably have to be considered to achieve the optimum balance of what can often be conflicting requirements.

4.2.1 *Operational concept*

The elements which should be considered in defining the operational concept are given in table 1. Each of these needs to be specified in detail in order that the maintenance environment and the operational constraints can be properly considered.

4.2.2 *Maintenance concept*

The many elements which should be considered in defining the maintenance concept are given in table 2. It is these elements which determine the requirement for and extent of the testability features to be included in the design. Some degree of trade-off may again be required between the maintenance concept and the diagnostic technique in order to accommodate the numerous mutual interdependencies involved.

4.3 *Diagnostic concept*

Prior to the design and development phase, a suitable diagnostic concept should be determined, taking into account constraints due to life cycle cost optimization, operational and maintenance concepts, in accordance with the following factors:

- objectives, tasks and applications of diagnostic testing;
- methods used for diagnostic testing;
- requirements for diagnostic testing.

4.3.1 Objectifs, tâches et applications des essais pour diagnostic

L'objectif des essais pour diagnostic est de fournir la méthode la plus efficace vis-à-vis des coûts, la plus rapide et la moins ambiguë concernant l'identification de panne à un niveau déterminé par la politique de maintenance de l'équipement en essai. De bons essais pour diagnostic vont:

- augmenter la disponibilité de l'équipement;
- diminuer les coûts de maintenance;
- réduire le risque de dommages indirects;
- améliorer la sécurité du système;
- optimiser l'utilisation opérationnelle.

Pour atteindre leur objectif, il convient que les essais pour diagnostic:

- fournissent des types de vérifications de confiance afin de confirmer l'aptitude au service de l'équipement concernant le rôle qui lui est dévolu;
- reconnaissent les défaillances cataclysmiques et les dégradations;
- localisent les pannes en rapport avec la fonction défaillante ou l'UI défaillante;
- avertissent des défaillances d'usure potentielle grâce à une évaluation des états d'usure;
- fournissent des données pour la maintenance et l'exploitation de l'équipement.

Les principales applications des dispositifs d'essais pour diagnostic sont:

- les vérifications fonctionnelles et de sécurité avant la mise en fonctionnement du système;
- le contrôle des performances en fonctionnement;
- l'identification des défaillances du système en environnement opérationnel, au niveau de l'ensemble défaillant ou de l'UI;
- la localisation détaillée des pannes dans les ateliers de réparation.

4.3.2 Méthodes utilisées pour les essais de diagnostic

Les procédures possibles pouvant être appliquées pour les essais de diagnostic vont des mesures purement manuelles et de l'évaluation des caractéristiques mécaniques au diagnostic entièrement automatisé de processus et installations complètes, y compris le test de composants élémentaires et de systèmes complexes. La large panoplie de méthodes de diagnostic appliquées est illustrée en figure 1 et se classe en trois catégories principales:

- le **diagnostic externe** utilise des équipements de test distincts de l'UEE qui ne sont branchés que lorsque c'est nécessaire. L'équipement de test utilisé peut être d'une nature très générale, adapté aux buts requis à partir d'appareils standards, ou bien être spécialement conçu pour l'équipement à essayer. Des EEA pilotés par ordinateur peuvent également être utilisés;
- le **diagnostic interne** utilise en permanence l'équipement de test intégré (ETI) qui peut être mis en fonctionnement de façon continue ou intermittente pendant le fonctionnement du système. En outre, des essais spéciaux, pour un état de fonctionnement réduit du système, ou bien hors fonctionnement, peuvent aussi être réalisés;
- le **diagnostic intégré** est une forme particulière de diagnostic interne pour laquelle l'ensemble fonctionnel commandant le processus réalise en même temps le diagnostic, avec les fonctions opérationnelles et de diagnostic qui sont réalisées, soit en même temps, soit alternativement grâce au logiciel de TI. Ce système offre la possibilité de reconfiguration, ce qui permet la prise en charge automatique de panne suite à la détection de défaillances, afin de préserver l'aptitude au fonctionnement. Ceci constitue un avantage particulier à la méthode de diagnostic interne.

4.3.1 Objectives, tasks and applications of diagnostic testing

The objective of diagnostic testing is to provide the most cost-effective, rapid and unambiguous method of fault identification to a level determined by the maintenance policy for the equipment under test. Good diagnostic testing will:

- increase equipment availability;
- decrease maintenance costs;
- reduce the risk of consequential damage;
- improve the safety of the system;
- optimize the operational use.

To achieve the objective, the diagnostic system should:

- provide confidence type checks to confirm the serviceability of the equipment for its intended role;
- recognize catastrophic and degradation failures;
- localize faults with respect to the failed function or LRU;
- warn of impending wear-out failures, by evaluation of wear-out states;
- provide data for operation and maintenance of the equipment.

The principal applications of diagnostic testing facilities are:

- safety and functional checks prior to the operation of the system;
- performance monitoring during operation;
- equipment failure identification in the operating environment to failed assembly or LRU level;
- detailed fault localization in the designated repair facility.

4.3.2 Methods used for diagnostic testing

The possible procedures which can be applied for diagnostic testing range from the purely manual measurements and evaluation of mechanical characteristics to the fully automated diagnosis of entire processes and installations, with the testing of single components and complex systems. The broad diagnostic methods applied are illustrated in figure 1 and fall into three main categories:

- **external diagnosis** utilizes test equipment discrete from the UUT which is only connected when required. The test equipment used may be of a general-purpose nature, adapted for the purpose from standard equipment or specially designed for the equipment to be tested. Computer controlled ATE may also be involved;
- **internal diagnosis** utilizes permanently built-in test equipment (BITE) which may be continuously or intermittently operated during the operation of the system. In addition, special tests, in the reduced, or non-operating state of the system, may also be carried out;
- **built-in diagnosis** is a special form of internal diagnosis in which the functional assembly controlling the process at the same time performs the diagnosis, with operational and diagnostic functions being carried out concurrently or alternately by the BIT software. This system provides the facility for reconfiguration, which is automatic fault handling following failure recognition in order to preserve operability. This is a particular advantage of the internal diagnosis method.

4.3.3 Exigences pour les essais de diagnostic

4.3.3.1 Modes de défaillances

L'AMDE est la méthode fournissant le meilleur point de départ pour la spécification, la conception et l'évaluation des essais pour diagnostic. Elle permet le classement des modes de défaillance possibles en fonction de leur facilité à être détectés, diagnostiqués et testés, fournissant ainsi les informations permettant à l'ETI de détecter sélectivement les modes de défaillance identifiés, de même que la sélection des points de test appropriés et des procédures de diagnostic (voir également la CEI 812).

L'AMDE présente également une base homogène pour les évaluations de sécurité et de risques, ainsi que la conception de la tolérance aux pannes et à la testabilité. Dans le cas d'un système complexe, il est important que l'analyse comprenne le système dans son ensemble afin d'offrir une couverture des défaillances interactives, et d'éviter une duplication de l'effort qui peut résulter de l'analyse indépendante des sous-systèmes seuls.

4.3.3.2 Données primaires

Les éléments de base des essais pour diagnostic sont établis par la mesure des données primaires (binaires ou analogiques) qui peuvent décrire l'état de l'UEE avec suffisamment de détails, et il convient qu'ils soient de préférence ceux qui sont également requis dans des buts opérationnels. Afin de minimiser les coûts, il convient que des paramètres supplémentaires ne soient rajoutés qu'en cas de nécessité absolue, particulièrement dans le cas de paramètres non électriques, dont les valeurs mesurées seraient difficiles et coûteuses à transformer en signaux électriques représentatifs.

Il convient que les données primaires disponibles reflètent l'état et le comportement en régime transitoire de l'UEE de façon non ambiguë et avec suffisamment de sensibilité, si des déclarations de diagnostic utiles doivent être établies. En conséquence, il convient d'établir ou de déterminer par des moyens théoriques ou pratiques des valeurs limites, des tolérances, ou bien des tables de vérité ou de décision et également des interrelations physiques plus complexes.

Dans certains cas, il faut non seulement des données issues de mesures, mais il faut aussi des données primaires actives, telles que des signaux électriques discrets ou digitaux, appliqués de l'extérieur à l'UEE, de façon à faire apparaître un certain état fonctionnel qui permette d'établir un diagnostic. Ceci est défini comme étant la stimulation.

4.3.3 *Requirements for diagnostic testing*

4.3.3.1 Failure modes

The failure modes and effects analysis (FMEA) is the method which best provides the starting-point for the specification, design and evaluation of diagnostic testing. It allows for the classification of possible failure modes according to their ease of detection, diagnosis and testability, so providing information for the selection of BITE to detect the failure modes identified, and for the appropriate test points and diagnostic procedures (see also IEC 812).

The FMEA also presents a unifying base-line for safety and hazard evaluation, design for fault tolerance and testability. In the case of a larger system, it is important that the analysis includes the complete system in order to provide for the coverage of interactive failures, and to prevent duplication of effort that can result from the independent analysis of subsystems only.

4.3.3.2 Primary data

The basis of diagnostic testing is established by the measurement of the primary data (binary or analogue) which can describe the state of the UUT in sufficient detail and preferably should be those which are also needed for operational purposes. To minimize cost, further parameters should only be added if absolutely necessary, especially in the case of non-electrical parameters, where it may be difficult and expensive to transform measured values into representative electrical signals.

The available primary data should reflect the state and the transitional behaviour of the UUT unambiguously, and with sufficient sensitivity, if useful diagnostic statements are to be derived. Therefore limiting values, tolerances, truth or decision tables and also more complex physical interrelations should be established or determined by theoretical or practical means.

In certain cases, not only data from measurements are needed, but also active primary data, such as discrete or digital electrical signals externally applied to the UUT in order to enforce a certain functional state which enables diagnostic statements. This is defined as stimulation.

Tableau 1 – Eléments du concept d'exploitation

Elément	Possibilités		
Situation	Mobile		
	Fixe	Transportable	Lieu variable
			Lieu fixe
		Non transportable	
Mode de fonctionnement	Fonctionnement continu	Contrôle permanent	
		Contrôles à certains moments dans le temps	
		Arrêts autorisés et conditions d'arrêt	
	Fonctionnement intermittent incluant les conditions d'intermittence		
Conditions de contraintes en exploitation	Fonctionnement sous contraintes réduites		
	Fonctionnement sous contraintes nominales		
	Fonctionnement sous contraintes élevées		
Conséquences	Sécurité		
	Coût	Utilisation réduite	
		Dommages indirects	
		Coûts de maintenance	
	Mesures correctives d'urgence		
Conditions d'environnement	Contraintes mécaniques		
	Contraintes thermiques		
	Contraintes électriques		
	Contraintes chimiques		
	Autres		
Personnel	Non formé		
	Formé dans un domaine différent		
	Formé	Qualification élevée	
		Qualification moyenne	
Qualification faible			
Manipulation	Manuelle		
	Partiellement automatisée		
	Complètement automatisée		

Table 1 – Elements of the operational concept

Element	Possibilities		
Location	Mobile		
	Stationary	Transportable	Varying location
			Fixed location
		Not transportable	
Operational mode	Continuous operation	Continuous monitoring	
		Monitoring at discrete points of time	
		Allowable breaks and break conditions	
	Intermittent operation, incl. conditions of intermittence		
Operational stress condition	Operation at partial stress		
	Operation at nominal stress		
	Operation at overstress		
Consequences	Safety		
	Cost	Reduced utilization	
		Consequential damage	
		Maintenance costs	
	Corrective, emergency measures		
Environmental conditions	Mechanical stress		
	Thermal stress		
	Electrical stress		
	Chemical stress		
	Others		
Personnel	Untrained		
	Trained in different area		
	Trained	High qualification	
		Medium qualification	
		Low qualification	
Handling	Manual		
	Partially automated		
	Fully automated		

Tableau 2 – Eléments du concept de maintenance

Elément	Détails nécessaires		
Politique de maintenance	Préventive	Maintenance	
		Contrôle	
		Réparation programmée	
	Corrective	Niveau système	Détection de panne
			Localisation de panne
			Réparation (remplacement)
			Étalonnage
			Vérification fonctionnelle
		Niveau composant	Localisation de panne
Réparation			
Étalonnage			
Temps de maintenance	Contrôle permanent		
	Maintenance programmée	Intervalles	Période de temps
		Types	Action
			Niveau
			Maintenance hors fonctionnement
			Maintenance en fonctionnement
			Maintenance non programmée
Lieu de maintenance	Fixe	Nombre d'ateliers	
		Répartition géographique des ateliers	
		Potentiel technique des ateliers	
	Mobile	Équipement de station	
		Potentiel technique de la station	
Procédure de maintenance	Procédure		
	Ressources	Matériel	
		Logiciel	
	Documentation (descriptive, illustrative) pour		Matériel
			Logiciel
Logistique	Stocks	Nombre de magasins	
		Répartition géographique des magasins	
		Taille des stocks	
		Conditions de stockage	
	Gestion des stocks	Approvisionnement	
		Fourniture	
		Transport	
Environnement de maintenance	Conditions thermiques		
	Autres conditions		
Personnel de maintenance	Formation de base	Type de formation	
		Niveau de qualification	
	Formation spéciale	Niveau système	
		Niveau composant	
	Remise à niveau de formation	Intervalles	
Contenu			

Table 2 – Elements of the maintenance concept

Element	Required details			
Maintenance policy	Preventive	Maintenance		
		Inspection		
		Scheduled repair		
	Corrective	System level	Fault recognition	
			Fault localization	
			Repair (replacement)	
			Calibration	
			Functional check	
		Component level	Fault localization	
			Repair	
Calibration				
Functional test				
Maintenance time	Continuous monitoring			
	Scheduled maintenance	Intervals	Time period	
			Action	
		Type	Level	
			Hard time maintenance	
			On condition maintenance	
Unscheduled maintenance				
Maintenance location	Stationary	Number of shops		
		Local distribution of shops		
		Technical potential of shop		
	Mobile	Equipment of station		
		Technical potential of station		
Maintenance procedure	Procedure			
	Resources	Hardware		
		Software		
	Documentation (descriptive, illustrative) for		Hardware	
Logistics	Stock	Number of stores		
		Local distribution of stores		
		Stock size		
		Storage conditions		
	Stock management	Procurement		
		Supply		
		Transportation		
		Maintenance environment	Thermal conditions	
Other conditions				
Maintenance personnel	Basic training	Branch of training		
		Qualification level		
	Special training	System level		
		Component level		
	Refresher training	Intervals		
Curricula				

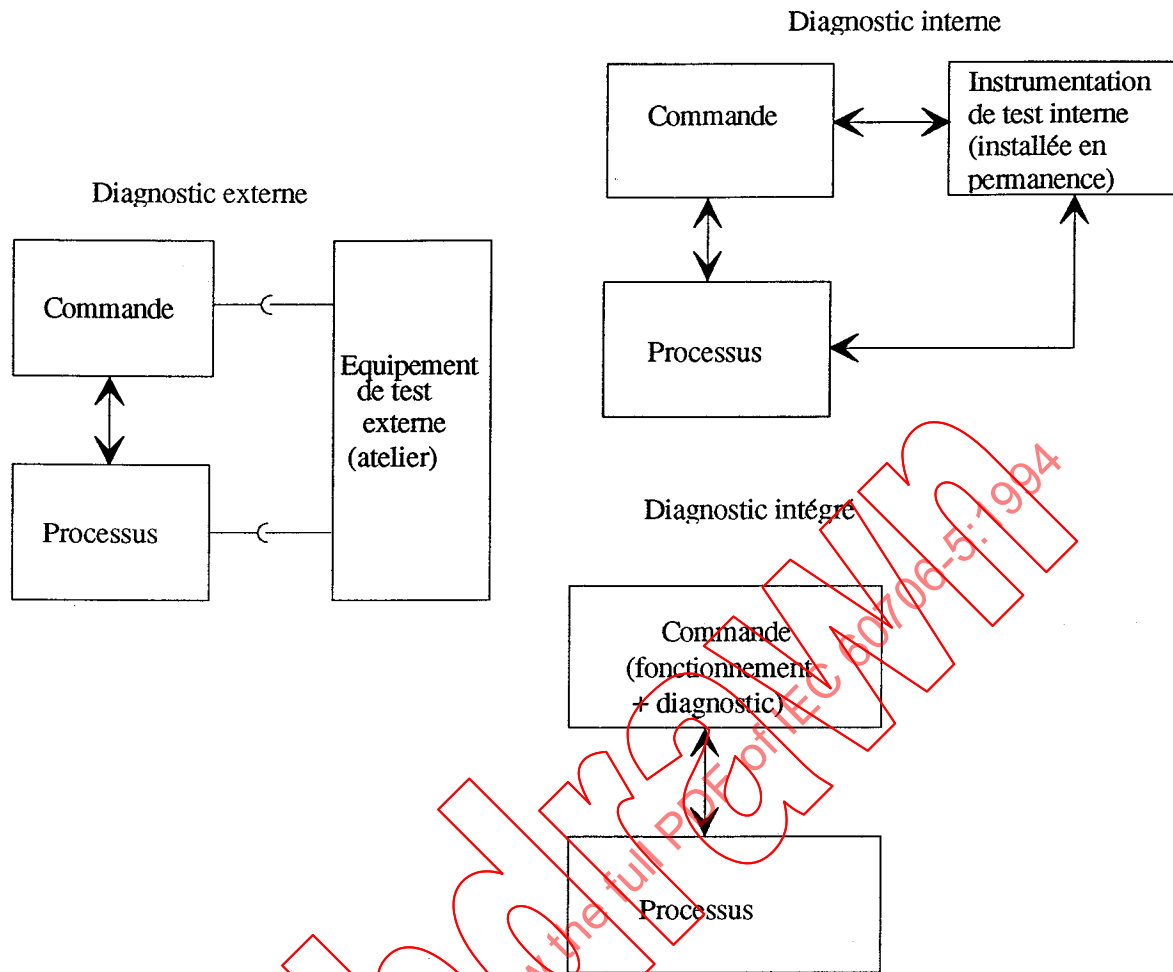


Figure 1 – Méthodes d'essais pour diagnostic

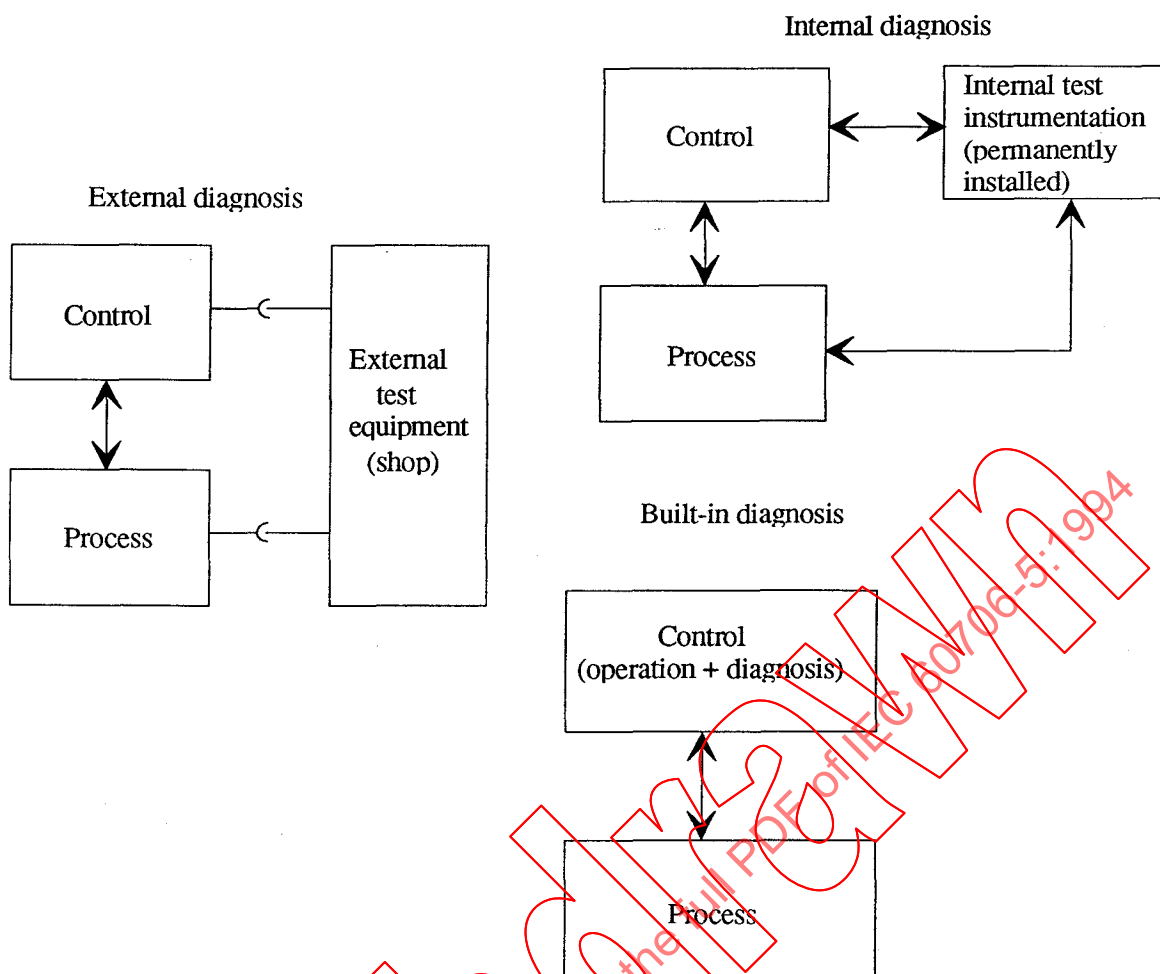


Figure 1 – Methods of diagnostic testing

4.3.3.3 Données secondaires

Les données secondaires sont celles déduites des données primaires, généralement grâce à la combinaison de plusieurs données élémentaires. Ces données secondaires déterminent l'efficacité du test et incluent les éléments qui suivent, sans y être limitées:

a) la couverture de pannes

Dans le cas de pannes concernant la sécurité, il convient que le taux de couverture de pannes soit aussi proche que possible de 100 %. Dans tous les autres cas, la couverture de pannes peut être optimisée en fonction de considérations techniques et de coût.

NOTE – Il n'est pas nécessaire que la détection de panne se fasse au même niveau hiérarchique que celui où la fonction défaillante est localisée. Si des actions destinées à conserver la sécurité des systèmes peuvent être initialisées à un niveau supérieur, l'allocation de détection de panne à ce niveau est autorisée.

b) temps de détection de panne

Dans le cas de pannes concernant la sécurité, il convient que le temps de détection de panne soit minimisé et que les exigences relatives aux limites de temps supérieures résultant de conditions externes soient tenues. Dans tous les autres cas, les temps de détection de pannes peuvent être optimisés en fonction de considérations techniques et de coût.

c) résolution de panne

Cet élément est caractérisé quantitativement par le degré:

- de sélectivité de la localisation de panne en fonction des niveaux d'intervention;
- de la précision d'évaluation de l'état d'usure.

La résolution de panne dépend des niveaux d'intervention donnés, des procédures et des conditions de maintenance.

d) temps de localisation de panne

Cet élément s'exprime grâce au temps écoulé entre l'occurrence de défaillance ou l'initialisation de la procédure de test et l'aboutissement du résultat de diagnostic.

e) exactitude de diagnostic

Dans le cas de pannes concernant la sécurité, il convient que l'exactitude de diagnostic soit aussi proche de 100 % que possible. Dans tous les autres cas, l'exactitude de diagnostic peut être optimisée en fonction de considérations techniques et de coût.

Il convient que les cas de diagnostic erroné soient considérés en fonction de leurs types et de leurs effets, et pris en compte durant la planification, le développement et l'évaluation d'un produit. En fonction du degré de carence, les niveaux de dégradation suivants peuvent être définis:

- 1) panne concernant la sécurité, non détectée: il convient d'éliminer ce cas;
- 2) fausse alarme: ce cas, particulièrement si sa fréquence dépasse une limite acceptable, peut également entraîner de sérieuses conséquences. Par conséquent, une caractéristique spéciale, le taux de fausse alarme, a été définie pour être observée séparément (voir annexe A);
- 3) panne non détectée (à l'exception de 1);
- 4) panne attribuée à tort;
- 5) panne évaluée à tort.

L'expression mathématique des paramètres définis ci-dessus est donnée dans l'annexe A.

4.3.3.3 Secondary data

Secondary data are derived from primary data, generally by the combination of several individual data elements. They constitute the test effectiveness and include, but are not limited to, the following parameters:

a) fault coverage

In the case of safety relevant faults, the fault coverage should be as close to 100 % as possible. In all other cases, the fault coverage may be optimized in accordance with technical and cost considerations.

NOTE – It is not necessary for recognition of the fault to occur in the same hierarchical level as that in which the faulty function is located: if actions to maintain product safety can be initiated from a higher level, the allocation of fault recognition to that level is admissible.

b) fault recognition time

In the case of safety relevant faults, the fault recognition time should be minimized and the requirements for upper time limits due to external conditions adhered to. In all other cases, the fault recognition times may be optimized in accordance with technical and cost considerations.

c) fault resolution

This element is measured quantitatively by the degree of:

- selectivity of fault localization on individual indenture levels;
- accuracy of evaluation of wear-out features.

The fault resolution is related to given indenture levels and is dependent on maintenance procedures and conditions.

d) fault localization time

This element is expressed by the time between failure occurrence or test routine initiation and completion of the diagnostic result.

e) diagnostic correctness

In the case of safety relevant faults, the diagnostic correctness should be as close to 100 % as possible. In all other cases, the diagnostic correctness may be optimized in accordance with technical and cost considerations.

Cases of wrong diagnosis should be considered according to their type and effect and taken into account in the planning, development and evaluation of a product. Depending on the degree of deficiency, the following degradation levels can be defined:

- 1) not recognized safety relevant fault: this case should be avoided;
- 2) false alarm: this case, especially if its frequency is beyond an acceptable limit, can also result in serious consequences. Therefore a special measure, the false alarm rate, has been defined for its separate observation (see annex A);
- 3) not recognized fault (except 1);
- 4) erroneously allocated fault;
- 5) erroneously evaluated fault.

Mathematical expressions for the above parameters are given in annex A.

4.3.3.4 Interfaces standardisées

Pour la réalisation et l'utilisation de diagnostics techniques, un échange important de données primaires et secondaires est nécessaire. Il convient que la conception des interfaces de données, leurs tâches, ainsi que les procédures d'échange de données appliquées, soient définies en détail. Les tâches et procédures de conception pour des interfaces principales sont:

a) interfaces de communication homme-machine

1) tâches

- visualisation de résultats de diagnostic (données secondaires);
- retrait des fichiers de données secondaires;
- initialisation de procédures d'essais particulières;
- vérification des données primaires courantes;
- modification de certains paramètres du processus;
- initialisation de programmes de rétablissement à des fins de reconfiguration, en cas de défaillance.

2) procédures de conception

Il n'est pas possible d'établir des procédures de conception généralisées pour la très large diversité de fonctions et de diagnostics qui seront rencontrés. Cependant, il est essentiel que les aspects opérationnels et de maintenance de la conception soient entièrement pris en considération à ce stade.

La normalisation dans des domaines d'application individuelle est hautement souhaitable, et peut souvent être facilitée en faisant référence aux normes du produit considéré.

b) interface de gestion du dispositif

1) tâches

Raccordement à des ressources pour:

- vérification des résultats du diagnostic (données secondaires);
- vérification des données primaires courantes et stockées;
- manipulation du processus et modification des paramètres du processus;
- développement et essai des modifications de logiciel.

2) procédures de conception

Il convient que toutes les liaisons de données soient conformes aux normes internationales applicables, en fonction de la configuration et de l'utilisation choisies. Comme exemples: ISO/TR 7477, EIA/TIA 232-E, EIA-422-A, EIA-485, IEEE 488.1, IEEE 488.2, ITU-TV.11, ITU-TV.22, ITU-TV.24, ITU-TV.28, ITU-TV.29, ITU-TX.25 et CEI 625-1.

c) interface ordinateur

1) tâches

Une interface est nécessaire pour les échanges série ou parallèle-série des données primaires et secondaires entre deux ou plusieurs composants microélectroniques d'une UEE.

2) procédures de conception

Les procédures de conception dépendent étroitement des conditions individuelles, mais il convient qu'elles soient, en tout cas, en conformité avec les normes internationales. Si possible (nombre de participants, sécurité, distances), il convient d'adopter de préférence EIA-422, ITU-TV.11 ou EIA 485. En outre, référence est faite à la CEI 625.

4.3.3.4 Standardized interfaces

For the realization and use of technical diagnostics, extensive exchange of primary and secondary data is required. The design of the data interfaces, their tasks and the data exchange procedures applied should be defined in detail. The tasks and design procedures for the principal interfaces are:

a) man-machine communication interface

1) tasks

- display of diagnostic results (secondary data);
- removal of secondary data files;
- initiating special test routines;
- checking of current primary data;
- modification of certain process parameters;
- initiation of recovery programmes for reconfiguration purposes in case of failures.

2) design procedures

It is not possible to lay down generalized design procedures for the wide variation of functions and diagnosis which will be met. However, it is essential that the operational and maintenance aspects of the design are fully considered at this point.

Standardization in individual application fields is highly desirable and can often be aided with reference to the respective product standards.

b) item management interface

1) tasks

Connection of external resources for:

- checking of diagnostic results (secondary data);
- checking of current and stored primary data;
- process handling and modification of process parameters;
- development and testing of software modifications.

2) design procedures

All data links should conform to the applicable international standards according to the chosen configuration and usage. Examples are ISO/TR 7477, EIA/TIA 232-E, EIA-422-A, EIA-485, IEEE 488.1, IEEE 488.2, ITU-TV.11, ITU-TV.22, ITU-TV.24, ITU-TV.28, ITU-TV.29, ITU-TX.25 and IEC 625-1.

c) computer interface

1) tasks

An interface is needed for serial or parallel-serial exchange of primary and secondary data between two or more microelectronic components of a UUT.

2) design procedures

Design procedures are strongly dependent on individual conditions, but should in any case be in accordance with international standards. If possible (number of participants, safety, distances), EIA-422, ITU-TV.11 or EIA-485 should be preferred. In addition, reference is made to IEC 625.

4.3.4 *Evaluation de méthodes alternatives pour les essais de diagnostic*

Il convient que les alternatives possibles de conception de diagnostic (déterminé sur la base de 4.3.1 à 4.3.3) soient comparées et évaluées pour choisir la solution optimum. Il convient que les critères économiques suivants soient pris en compte:

- coûts d'investissement:
 - nombre de systèmes nécessaires, basé sur l'utilisation et la disponibilité;
 - coûts de développements;
 - coûts de logiciels non répétitifs;
 - coûts des installations de maintenance;
- les coûts unitaires d'équipement dépendant de:
 - la complexité;
 - la quantité à produire;
 - le degré de redondance;
 - le degré de la capacité en TI;
 - le standard de qualité;
- coûts relatifs à la maintenance:
 - coûts de maintenance programmée et non programmée;
 - gain résultant d'un système de diagnostic évitant des détériorations conséquentes;
 - degré d'automatisation comparé aux niveaux de formation;
 - durée de vie prévue pour l'équipement;
- moyens d'augmenter les bénéfices en exploitation:
 - caractéristiques de manipulation améliorées;
 - disponibilité améliorée, par exemple grâce à des diagnostics et à des réparations rapides des pannes, ou bien par utilisation de la redondance;
 - utilisation accrue;
- autres facteurs:
 - potentiel de modification;
 - incidence technique et économique de matériel ou de logiciel supplémentaire sur la sécurité et la fiabilité de l'équipement;
 - capacité à détecter des défaillances transitoires et intermittentes;
 - capacité du système de diagnostic pour un mode réversible.

NOTE – L'état de l'art actuel est le suivant:

- niveau système: les essais pour diagnostic sont, en premier lieu, réalisés par diagnostic interne, moyen qui peut aussi être utilisé pour la commande fonctionnelle et les vérifications initiales. Le diagnostic intégré est utilisé chaque fois que possible, et peut inclure la localisation de panne en descendant jusqu'au niveau UI. Toute exigence de diagnostic externe au niveau système aura tendance à augmenter le temps d'indisponibilité et donc à diminuer la disponibilité. Dans la plupart des cas, les équipements pour le diagnostic externe comprenant des tests pilotés par logiciel doivent être développés spécialement. Des terminaux de données non spécifiques peuvent être utiles et suffisants dans le cas de systèmes simples (par exemple les ordinateurs portables)
- niveau composant: Le diagnostic interne est uniquement applicable à certains composants matériels. Par conséquent, les possibilités de diagnostic interne jusqu'au niveau composant sont limitées. Le diagnostic externe peut être réalisé avec des équipements standards. Les tests internes aux circuits sont applicables à la localisation des pannes, et les tests fonctionnels peuvent être utilisés pour l'étalonnage.

4.3.4 Evaluation of alternative methods for diagnostic testing

The possible alternative diagnostic designs (determined on the basis of 4.3.1 to 4.3.3) should be compared and evaluated in order to select the optimum solution. The following economic criteria should be taken into account:

- capital cost:
 - numbers of systems required based on usage and availability;
 - development cost;
 - non-recurring software cost;
 - maintenance installation cost;
- equipment unit cost influenced by:
 - complexity;
 - quantity to be produced;
 - degree of redundancy;
 - degree of BIT capability;
 - quality standard;
- maintenance related cost:
 - scheduled and unscheduled maintenance cost;
 - savings by diagnostic system preventing consequential damage;
 - degree of automation considered against training levels;
 - planned equipment life;
- means to increase operating profit:
 - improved handling characteristics;
 - increased availability, for example by quick diagnosis and repair of faults or by use of redundancy;
 - increased utilization;
- other factors:
 - modification potential;
 - technical and cost impact of additional hardware or software on safety and reliability of equipment;
 - capability to recognize transient and intermittent failures;
 - reversionary mode capability of diagnostic system.

NOTE – The present state of the art is as follows:

– system level: diagnostic testing is primarily carried out by internal diagnosis, which can also be used for functional monitoring and initial checks. Built-in diagnosis is used wherever possible and can include fault localization down to LRU level. Any requirement for external diagnosis at system level will tend to increase the down time and thus decrease availability. In most cases, equipment for external diagnosis including software driven tests must be specifically developed. Off-the-shelf data terminals may be useful and sufficient for simple systems (e.g. laptop PCs).

– component level: internal diagnosis is only applicable to certain hardware components. Therefore, the possibilities of internal diagnosis down to component level are limited. External diagnosis can be carried out with off-the-shelf equipment. In-circuit tests are applicable for fault localization, and functional tests can be used for calibration.

5 Exigences d'un programme de testabilité

Si les exigences techniques relatives aux essais pour diagnostic sont spécifiées pour un produit, il convient qu'un programme de testabilité soit établi de façon à assurer que ces exigences seront respectées et que les aspects de testabilité seront correctement traités dans toutes les phases du processus d'acquisition. Le programme peut faire partie de l'ensemble du programme de disponibilité, mais il convient qu'il comprenne les éléments suivants:

- conception de testabilité;
- vérification de testabilité;
- documentation de testabilité.

5.1 Conception de la testabilité

Le but de cette partie du programme est de définir les moyens de satisfaire aux exigences des essais pour diagnostic établies pour le produit. Dans ce contexte, il convient que les critères suivants de conception de testabilité soient pris en compte:

- partition fonctionnelle en groupes et unités fonctionnels avec des interfaces clairement disposées et bien définies. Chaque fois que possible, il convient que les partitions physiques et électriques soient compatibles avec cette structure afin de faciliter un ajustement optimal des diagnostics, de la maintenance et de la logistique;
- préférence pour l'utilisation de fonctions, composants et éléments de conception, pour lesquels l'état et le comportement transitoire peuvent être mesurés et évalués grâce à des données primaires appropriées;
- prise en considération des procédures de mesure qui sont applicables durant la maintenance et compatibles avec l'équipement externe existant ou prévu. Il convient que l'accessibilité physique et électrique des équipements de mesure soit également prise en compte;
- pour tous les composants matériels internes et externes du système de diagnostic, il convient que la capacité TI soit fournie. Il convient que l'exactitude de la performance ETI ainsi que l'étalonnage soient assurés;
- initialisation: il convient que le système ou l'équipement soit conçu de telle sorte qu'il ait un état initial bien défini afin de commencer le processus de localisation de panne. En cas de défaillance, il convient que l'initialisation se produise automatiquement et de manière répétée;
- l'application de procédure de test et de stimulations externes ne doit avoir aucun effet dommageable, ni sur les composants eux-mêmes ni sur l'équipement considéré ou le système global;
- il convient que tous les systèmes de bus soient accessibles pour les mesures;
- il convient que le logiciel fonctionnel et, si possible, le logiciel d'application de diagnostic, soient conçus et documentés de sorte qu'ils puissent être facilement vérifiés par le personnel de maintenance;
- mode réversible: aucun système de diagnostic n'est jamais parfait, c'est-à-dire qu'il peut tomber en panne, malgré une haute fiabilité. En conséquence, dans le cas d'une défaillance du système de diagnostic, il convient d'avoir la capacité d'arrêter le processus sans détriment pour l'exploitation du système. Il convient d'être assuré que dans ce cas, la méthode de test conventionnelle, orientée fonctionnellement, peut être appliquée afin de localiser les pannes au niveau des composants interchangeables. Il convient qu'il soit possible d'utiliser l'interface de service pour vérifier les données primaires courantes.

5 Testability programme requirements

If technical requirements with regard to diagnostic testing are specified for a product, a testability programme should be established in order to ensure that these requirements are met and that testability aspects are adequately considered in all phases of the procurement process. The programme may be part of the overall dependability programme, but should contain dedicated elements concerning

- testability engineering;
- testability verification;
- testability documentation.

5.1 Testability engineering

The purpose of this programme element is to provide the means of achieving the diagnostic testing requirements established for the product. In this context, the following testability design criteria should be considered:

- functional partitioning in functional groups and units with clearly arranged and well-defined interfaces. Whenever possible, the physical and electrical partitioning should be compatible with this structure in order to facilitate optimum adjustment of diagnostics, maintenance and logistics;
- preference for the use of functions, components and design elements, the status and the transitional behaviour of which can be measured and evaluated by appropriate primary data;
- consideration of those measuring procedures which are applicable during maintenance and compatible with existing or planned external equipment. The physical and electrical accessibility of the measuring equipment should also be taken into account;
- for all internal and external hardware components of the diagnosis system, BIT capability should be provided. Correctness of the BITE performance and calibration should be ensured;
- initialization: the system or equipment should be designed such that it has a well-defined initial state to commence the fault localization process. In case of a failure, the initialization should take place automatically and repeatedly;
- application of test procedures and external stimuli shall have no harmful effects on the component itself or related equipment or the overall system;
- all bus-systems should be accessible for measurements;
- the functional and, where applicable, diagnostic application software should be designed and documented such that it can be readily verified by the maintenance personnel;
- reversionary mode: each diagnostic system is expected to be less than perfect, i.e. it can fail in spite of high reliability. Therefore, in the event of a failure of the diagnostic system, it should have the capability to abort the process without detriment to the operation of the system. It should be ensured that in this case the conventional, functionally oriented test method can be applied to localize faults on the level of replaceable components. It should be possible to use the service interface for checking current primary data.

5.2 Vérification de la testabilité

Le but de cette partie du programme est de prouver, initialement par des moyens théoriques, plus tard par des moyens pratiques, que les exigences des essais pour diagnostic ont été satisfaites. Ceci peut être effectué par des méthodes et procédures semblables à celles appliquées pour la vérification des paramètres de maintenabilité (voir la section six de ce guide). Les concepts de vérification qu'il convient de prendre en considération, comprennent:

- une vérification théorique;
- une vérification pratique.

5.2.1 Vérification théorique

Les éléments de la vérification théorique sont:

- revue de la documentation: il convient que les documents fournis en réponse aux exigences définies en 5.3 soient examinés eu égard à l'exhaustivité, la précision, la facilité d'utilisation;
- analyse: cette activité comprend les recherches analytiques sur le dispositif et l'évaluation de ses caractéristiques de testabilité, par exemple, taux de couverture de pannes, résolution des pannes et exactitude de diagnostic. L'évaluation peut être réalisée en utilisant les définitions de l'annexe A.

5.2.2 Vérification pratique

La testabilité peut être vérifiée par des moyens pratiques tels que:

- contrôle visuel et essais de partition. Ils seront effectués afin de revoir la conception de la testabilité et pour s'assurer que les interfaces sont conformes aux exigences;
- essai de qualification: l'essai de qualification est destiné à démontrer le fonctionnement correct des procédures et des tâches de diagnostic dans toute la gamme des conditions d'exploitation et d'essais d'environnement. Il convient que la démonstration de testabilité soit réalisée sur un produit sans panne, et après l'introduction de pannes représentatives. Il convient que l'évaluation d'état d'usure soit démontrée pour divers degrés d'usure. L'approbation du client sera requise, les pannes liées à la sécurité étant affectées d'une priorité;
- essais de série: il convient que les essais de série soient exécutés pour prouver que les performances des interfaces et leur exactitude sont correctes, ainsi que celles des essais "tout ou rien";
- évaluation des données d'exploitation: il convient que la qualité des mesures qui ne peuvent pas être démontrées avec une précision suffisante grâce aux inspections visuelles, à la qualification ou aux essais de série soient vérifiées grâce au recueil et à l'évaluation de données d'exploitation supplémentaires. Les principales mesures concernées sont:
 - la précision du diagnostic;
 - la couverture de détection de panne;
 - le taux de fausse alarme.

5.3 Documentation de testabilité

Le but de cette partie du programme est de s'assurer qu'une documentation complète du concept de diagnostic sera fournie sous une forme normalisée, de sorte que toute information pertinente soit rendue disponible pour les opérateurs et le personnel de maintenance du système. Il convient que la conception de la documentation tienne compte des conditions opérationnelles concernant à la fois l'utilisation et la maintenance, le concept de maintenance, les niveaux de compétence et le degré de la formation qui doit être dispensée.

5.2 Testability verification

The purpose of this programme element is to prove, initially by theoretical and later by practical means, that the diagnostic testing requirements have been fulfilled. This can be done by methods and procedures similar to those applied for the verification of maintainability parameters (see Section Six of this guide, contained in IEC 706-3). Verification concepts which should be considered include

- theoretical verification;
- practical verification.

5.2.1 Theoretical verification

Elements of the theoretical verification are:

- documentation review: documents supplied in response to the requirements in 5.3 should be reviewed with respect to completeness, accuracy and ease of use;
- analysis: this activity includes the analytical investigation of the item and the assessment of its testability features, for example fault coverage, fault resolution and diagnostic correctness. The assessment can be carried out in accordance with annex A.

5.2.2 Practical verification

The testability can be verified by practical means, such as

- visual inspection and partitioning tests: these are carried out in order to review the design for testability and to ensure that the interfaces are in accordance with requirements;
- qualification testing: the qualification test is to demonstrate the correct operation of the diagnostic tasks and procedures over the full range of operating and environmental conditions. The testability demonstration should be carried out for the fault-free case and after the introduction of representative faults. The evaluation of wear-out states should be demonstrated for different wear-out degrees. Customer approval will be required, with safety relevant faults having priority;
- series tests: these tests should be carried out in order to prove the correct performance of interfaces and of confidence and "go-no go" tests;
- evaluation of field data: quality measures which cannot be demonstrated with sufficient accuracy by visual inspections, qualification or series tests, should be verified by the collection and evaluation of additional field data. The principal measures concerned are:
 - diagnostic correctness;
 - fault coverage;
 - false alarm rate.

5.3 Testability documentation

The purpose of this programme element is to ensure that full documentation of the diagnostic concept will be supplied in a standardized form, so that all the relevant information is made available to the operators and maintainers of the system. The design of the documentation should take into account the operational conditions for both usage and maintenance, the maintenance concept, levels of skill, and degree of training to be given.

5.3.1 Exigences générales

Indépendamment des exigences de diagnostic, la documentation concernant les sujets suivants sera nécessaire pour faire fonctionner un système complexe. Parmi ces sujets, il convient que les éléments fournis pour le diagnostic soient convenablement décrits afin d'intégrer les fonctions d'exploitation, de maintenance et de diagnostic à l'intérieur d'une gamme de conditions spécifiées:

- description générale du produit;
- instructions d'exploitation et de maintenance;
- diagrammes d'ensemble électriques;
- diagrammes des alimentations;
- dessins topologiques ou catalogue composants;
- autres dessins;
- documentation logiciel;
- listes des composants;
- instructions de tests;
- certificat de sécurité.

5.3.2 Exigences particulières

Il convient que les documents supplémentaires suivants soient normalement fournis:

- descriptions des procédures de diagnostic, comprenant les types et l'importance des données secondaires ainsi que les processus d'interfaces. Si les procédures de diagnostic sont incorporées dans des programmes d'ordinateur pour des diagnostics externes ou internes, le fournisseur peut procurer suffisamment de documentation concernant ces programmes au lieu d'une description sous forme textuelle, si le client est d'accord. En se basant sur cette documentation, il convient que le client soit capable de réaliser une optimisation de programme, ou bien d'écrire et de mettre en oeuvre par lui-même des programmes de diagnostic supplémentaires;
- description des procédures de test en mode réversible.

6 Etablissement de contrats pour la testabilité

Des dispositions appropriées et contractuelles sont un préalable essentiel à la conversion des exigences d'essais pour diagnostic en réalisations pratiques mesurables. Pour rendre possible une conception optimale, un développement et une fourniture de procédures pour des essais de diagnostic, il convient que le client fournisse une spécification précise de ses exigences de testabilité. Pour cela, il convient que le client procure au fournisseur les documents suivants:

- définition d'exigences;
- spécification de testabilité.

6.1 Définition d'exigences

La définition des exigences est constituée de descriptions détaillées des besoins du client et a pour but de constituer la base du programme de conception et de développement. La mise à jour est possible si des informations supplémentaires deviennent disponibles en cours de développement; cependant, il convient que les modifications soient mutuellement avalisées, du fait qu'elles induiront souvent des délais supplémentaires et des pénalités en coût. Il convient que les exigences comprennent:

- les objectifs des essais pour diagnostic (voir 4.3.1);
- le concept d'exploitation (voir 4.2.1);
- le concept de maintenance (voir 4.2.2);
- une description qualitative de l'environnement économique (voir 4.1);
- les méthodes et solutions préférentielles (voir 4.3.2, 4.3.4);
- la sélection, le recueil et l'évaluation des données primaires (voir 4.3.3.2).

5.3.1 General requirements

Irrespective of the diagnostic requirements, documentation on the following topics will be necessary to operate a complex system. Within these topics, the diagnostic provisions should be properly described to integrate the operational, maintenance and diagnostic functions under the range of specified conditions:

- general description of the product;
- operational and maintenance instructions;
- electrical overview diagrams;
- power supply diagrams;
- positioning drawings or parts catalogue;
- other drawings;
- software documentation;
- parts lists;
- test instructions;
- safety certificate.

5.3.2 Special requirements

The following additional documents should normally be supplied:

- description of the diagnostic procedures, including types and importance of secondary data and the interface processes. If the diagnostic procedures are incorporated in computer programs for external or internal diagnosis, the supplier may provide sufficient documentation of these programs instead of a narrative description, if the customer agrees. Based on this documentation, the customer should be able to perform a program optimization, or to write and implement additional diagnostic programs on his own;
- description of the test procedures in the reversionary mode.

6 Contracting for testability

Appropriate contractual provisions are a key prerequisite for efficient conversion of diagnostic testing requirements into measurable practical achievements. In order to enable optimum design, development and supply of diagnostic test procedures, the customer should provide an exact specification of his testability requirements. For this purpose, he should provide the supplier with the following documents:

- statement of requirements;
- testability specification.

6.1 Statement of requirements

The statement of requirement contains detailed descriptions of the customer's needs and is intended to form the basis of the design and development programme. Updating is possible, if additional information becomes available in the course of development; however, modifications should be mutually agreed upon, as they will often incur additional time and cost penalties. The requirements should include:

- objectives of diagnostic testing (see 4.3.1);
- operational concept (see 4.2.1);
- maintenance concept (see 4.2.2);
- qualitative description of the economical environment (see 4.1);
- preferred methods and solutions (see 4.3.2, 4.3.4);
- selection, collection and evaluation of primary data (see 4.3.3.2).

6.2 Spécification de testabilité

La spécification de testabilité détermine les exigences relatives au produit, et éventuellement pour la phase de développement. Il convient que ces dernières comprennent ce qui suit:

- les tâches et les applications des essais pour diagnostic (voir 4.3.1);
- le type et la qualité des données secondaires (voir 4.3.3.3), particulièrement:
 - une liste des pannes concernant la sécurité pour lesquelles un degré de détection de pannes aussi proche que possible de 100 % est requis;
 - une limite inférieure du taux de couverture de pannes pour toutes les autres pannes;
 - une valeur maximale du temps de détection de pannes;
 - le degré de localisation de panne, par exemple sous forme d'une liste de pannes;
 - des valeurs objectifs (maximum) des temps de localisation de panne;
 - un objectif et une valeur minimale pour l'exactitude de diagnostic;
 - la valeur maximale du taux de fausse alarme;
- la conception concernant la testabilité (voir 5.1)
 - exigences générales;
 - exigences détaillées au moyen de listes de vérification;
 - critères de conception concernant la testabilité;
- les temps et les procédures pour (voir 5.2)
 - la vérification de la testabilité;
 - la vérification de la sécurité.

6.3 Conséquences

Il convient que les conséquences du non-respect des exigences spécifiées selon 6.2 soient définies.

6.2 Testability specification

The testability specification determines the requirements for the product and possibly for the development phase. These should include the following:

- tasks and applications of diagnostic testing (see 4.3.1);
- type and quality of secondary data (see 4.3.3.3), especially
 - list of safety relevant faults, for which a fault coverage of as close to 100 % as possible is required;
 - lower limit of fault coverage for all other faults;
 - maximum value of the fault recognition time;
 - fault resolution, for example in the form of a fault list;
 - target (maximum) values of the fault localization time;
 - target and minimum value of the diagnostic correctness;
 - maximum value of the false alarm rate;
- design for testability (see 5.1);
 - general requirements;
 - detailed requirements by check lists;
 - design criteria for testability;
- times and procedures for (see 5.2)
 - testability verification;
 - safety verification.

6.3 Consequences

The consequences of not meeting the specified requirements according to 6.2 should be defined.

Annexe A (informative)

Concepts mathématiques dans les essais pour diagnostic

A.1 Définitions, abréviations et symboles

Toutes les définitions et abréviations de l'article 3 s'appliquent dans cette annexe. De plus, les termes, définitions, abréviations et symboles définis ci-dessous sont utilisés.

A.1.1 Définitions

A.1.1.1 défaut d'alarme: Impossibilité de déclencher l'alarme due à une panne de l'élément superviseur du système.

A.1.1.2 non-détection de panne: Non-déclenchement de l'alarme alors qu'il existe une panne dans la partie fonctionnelle du système et qu'il n'y a pas de panne dans le superviseur.

A.1.2 Abréviations

F	fonctionnel
S	supervision
DA	défaut d'alarme
JD	justesse de diagnostic
FA	fausse alarme
CP	couverture de panne
LP	localisation de panne
RP	reconnaissance de panne
NDP	non-détection de panne

A.1.3 Symboles

$\lambda(t)$	taux de défaillance instantané des composants
$\Lambda(t)$	diagramme du taux de défaillance instantané de la fiabilité-série d'un équipement/système
p_{DA}	probabilité de défaut d'alarme
p_{JD}	probabilité de justesse de diagnostic
p_{FA}	probabilité de fausse alarme
p_{CP}	probabilité de couverture de panne
p_{LP}	probabilité de localisation de panne
p_{RP}	probabilité de reconnaissance de panne
p_{NDP}	probabilité de non-détection de panne
$p_{i,jk}$	probabilité conditionnelle de mode de défaillance jk du composant i , conduisant à l'événement k .

A.2 Hypothèses

Chaque système technique est considéré comme constitué par deux éléments:

- un élément fonctionnel (symbole F) qui réalise les fonctions opérationnelles;
- un élément superviseur (symbole S) qui réalise toutes les fonctions de supervision, contrôle et affichage.

La maintenabilité, comme caractéristique d'un système complet, est relative aux deux éléments fonctionnel et superviseur à la fois. Dans la description mathématique des essais pour diagnostic, les hypothèses suivantes sont avancées:

- seule la maintenance corrective est prise en compte (c'est-à-dire, les actions de réparation entraînées par des défaillances);

Annex A (informative)

Mathematical concepts in diagnostic testing

A.1 Definitions, abbreviations and symbols

All definitions and acronyms in clause 3 also apply to this annex. In addition, the terms, definitions, acronyms and symbols determined in the following subclauses are used:

A.1.1 Definitions

A.1.1.1 **alarm defect:** Inability to raise alarm due to a fault in the supervision part of a system.

A.1.1.2 **fault undetection:** Failure to raise alarm when the functional part of a system is faulty and there is no fault in the supervision part.

A.1.2 Abbreviations

F	functional
S	supervision
AD	alarm defect
DC	diagnostic correctness
FA	false alarm
FC	fault coverage
FL	fault localization
FR	fault recognition
FU	fault undetection

A.1.3 Symbols

$\lambda(t)$	component instantaneous failure rate
$\Lambda(t)$	equipment/system serial reliability diagram instantaneous failure rate
p_{AD}	alarm defect probability
p_{DC}	diagnostic correctness probability
p_{FA}	false alarm probability
p_{FC}	fault coverage probability
p_{FL}	fault localization probability
p_{FR}	fault recognition probability
p_{FU}	fault undetection probability
$P_{i,jk}$	conditional probability of fault mode jk on component i , leading to event k

A.2 Assumptions

It is assumed that every technical system can be considered as consisting of two parts:

- a functional part (symbol F) which carries out all operational functions;
- a supervision part (symbol S) which carries out all supervising, monitoring and display functions.

Maintainability, as a total system characteristic, is related to both the functional and the supervision part. In the mathematical description of diagnostic testing, the following assumptions are made:

- only corrective maintenance (i.e. repair actions caused by failures) is taken into account;

- la panne à diagnostiquer résulte de l'impossibilité d'un dispositif à accomplir la fonction exigée; les pannes dues à une dérive des paramètres en dehors des limites spécifiées pour le dispositif ne peuvent pas être prises en compte (et il ne convient pas de le faire);
- les pannes intermittentes ne sont pas prises en compte;
- les cas de pannes multiples présentes en même temps à un moment donné ne peuvent pas être prises en compte (et il ne convient pas de le faire).

A.3 Modèle mathématique

Dans le cas général d'un événement élémentaire k pris dans une série exhaustive d'événements mutuellement exclusifs, la probabilité d'occurrence de l'événement k , $p_k(t)$, sera:

$$p_k(t) = \frac{\sum_i \lambda_i(t) \sum_{jk} p_{i,jk}}{\Lambda(t)}$$

(i = indice du composant élémentaire), avec les relations suivantes:

$$\sum_i \lambda_i(t) = \Lambda(t)$$

$$\sum_{i,jk} p_{i,jk} = 1$$

p_k est indépendant du temps dans le cas d'un taux de défaillance constant. Au lieu d'utiliser une évaluation numérique de la formule donnée ci-dessus, il est plus aisé d'utiliser une procédure d'estimation. Ceci peut être obtenu par la technique de simulation de Monte-Carlo, qui permet:

- d'obtenir un point estimé;
- d'obtenir un intervalle de confiance estimé;
- de procéder à des essais de vérification/démonstration.

A.4 Traitement de la panne

A.4.1 Partition des pannes

En raison de la subdivision du système en deux éléments fonctionnel et superviseur, le processus de partition des pannes peut être structuré en accord avec le tableau A.1, définissant quatre mesures qui peuvent être quantifiées par des probabilités (indépendantes du temps dans le cas d'un taux de défaillance constant).

Tableau A.1 – Structure du processus de partition des pannes de systèmes techniques
(+ = pas de panne, – = panne)

Elément F	Elément S	Événement	Probabilité	Nombre d'observations (voir exemple)
+	+	Pas d'alarme		
+	–	Alarme: FA	p_{FA}	60
+	–	Pas d'alarme: DA	p_{DA}	40
–	+	Alarme: RP	p_{RP}	800
–	+	Pas d'alarme: NDP	p_{NDP}	100
–	–	Indifférent (panne multiple)		