

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
300-2**

Première édition
First edition
1995-12

Gestion de la sûreté de fonctionnement –

Partie 2:

Éléments et tâches du programme de sûreté
de fonctionnement

Dependability management –

Part 2:

Dependability programme elements and tasks



Numéro de référence
Reference number
CEI/IEC 300-2: 1995

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
300-2**

Première édition
First edition
1995-12

Gestion de la sûreté de fonctionnement –

Partie 2:

Eléments et tâches du programme de sûreté
de fonctionnement

Dependability management –

Part 2:

Dependability programme elements and tas

© CEI 1995 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 pro-
cédé, 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

W

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

AVA Documents
Document Sharing Hub

SOMMAIRE

	Pages
AVANT-PROPOS.....	6
INTRODUCTION.....	8
Articles	
1 Domaine d'application	12
2 Références normatives	12
3 Définitions	14
4 Vue générale d'un programme de sûreté de fonctionnement.....	14
4.1 Généralités	14
4.2 Cycle de vie d'un produit	20
4.2.1 Phase de concept et de définition	20
4.2.2 Phase de conception et de développement	20
4.2.3 Phase de fabrication	20
4.2.4 Phase d'installation	22
4.2.5 Phase d'exploitation et de maintenance	22
4.2.6 Phase de mise au rebut	24
5 Critères d'ajustement pour programmes de sûreté de fonctionnement.....	24
5.1 Généralités	24
5.2 Application propre à l'utilisateur	26
5.3 Situation contractuelle	26
5.4 Application aux phases du cycle de vie	26
5.5 Caractéristiques du produit	26
5.6 Considérations relatives au logiciel	28
6 Eléments et tâches d'un projet ou d'un programme spécifique d'un produit ou d'un projet	28
6.1 Planification et gestion	28
6.1.1 Plans de sûreté de fonctionnement	28
6.1.2 Gestion des décisions concernant le projet	30
6.1.3 Gestion de la traçabilité	30
6.1.4 Gestion de configuration	30
6.2 Revue de contrat et liaison	32
6.2.1 Revue de contrat	32
6.2.2 Représentants de la direction	32
6.3 Exigences de sûreté de fonctionnement	32
6.3.1 Spécification des exigences de sûreté de fonctionnement	32
6.3.2 Interprétation des exigences	34
6.3.3 Répartition des exigences	36
6.4 Ingénierie	36
6.4.1 Ingénierie de la fiabilité	36
6.4.2 Ingénierie de la maintenabilité	38
6.4.3 Ingénierie de la logistique de maintenance	38
6.4.4 Ingénierie de la testabilité	40
6.4.5 Ingénierie des facteurs humains	

CONTENTS

	Page
FOREWORD	7
INTRODUCTION	9
Clause	
1 Scope	13
2 Normative references	13
3 Definitions	15
4 Dependability programme overview	15
4.1 General	15
4.2 Life cycle of product	21
4.2.1 Concept and definition phase	21
4.2.2 Design and development phase	21
4.2.3 Manufacturing phase	21
4.2.4 Installation phase	23
4.2.5 Operation and maintenance phase	23
4.2.6 Disposal phase	25
5 Tailoring criteria for dependability programmes	25
5.1 General	25
5.2 User application	27
5.3 Contract situation	27
5.4 Life-cycle phase applications	27
5.5 Product-related characteristics	27
5.6 Software considerations	29
6 Project-specific or product-specific programme elements and tasks	29
6.1 Planning and management	29
6.1.1 Dependability plans	29
6.1.2 Project decision management	31
6.1.3 Traceability management	31
6.1.4 Configuration management	31
6.2 Contract review and liaison	33
6.2.1 Contract review	33
6.2.2 Management representative	33
6.3 Dependability requirements	33
6.3.1 Specification of dependability requirements	33
6.3.2 Requirements interpretation	35
6.3.3 Requirements allocation	37
6.4 Engineering	37
6.4.1 Reliability engineering	37
6.4.2 Maintainability engineering	39
6.4.3 Maintenance support engineering	39
6.4.4 Testability engineering	41
6.4.5 Human factors engineering	41

Articles	Pages
6.5 Produits fournis par des tiers	40
6.5.1 Produits fournis par des sous-traitants	40
6.5.2 Produits fournis par le client	42
6.6 Analyse, prévision et revues de conception	42
6.6.1 Analyse des modes de défaillance et de leurs effets	42
6.6.2 Analyse par arbre de panne	42
6.6.3 Analyses des contraintes et des charges	44
6.6.4 Analyse des facteurs humains	44
6.6.5 Prévisions	44
6.6.6 Analyses de compromis	46
6.6.7 Analyse des risques	46
6.6.8 Revues de conception formalisées	46
6.7 Vérification, validation et essai	48
6.7.1 Planification des validations, des vérifications et des essais	48
6.7.2 Essai de durée de vie	50
6.7.3 Essai de sûreté de fonctionnement	50
6.7.4 Essai de croissance de fiabilité	50
6.7.5 Essai en production	50
6.7.6 Essai d'acceptation	50
6.7.7 Déverminage de fiabilité sous contraintes	52
6.8 Programme de coût du cycle de vie	52
6.9 Planification de l'exploitation et de la logistique de maintenance	52
6.9.1 Planification de la logistique de maintenance	52
6.9.2 Installation	54
6.9.3 Service de soutien	54
6.9.4 Ingénierie de soutien	54
6.9.5 Approvisionnement des rechanges	54
6.10 Améliorations et modifications	56
6.10.1 Programmes d'amélioration	56
6.10.2 Gestion des modifications	56
6.11 Retour d'expérience	56
6.11.1 Acquisition des données	56
6.11.2 Analyse des données	58
Annexes	
A Organigramme simplifié d'un exemple de programme de sûreté de fonctionnement	62
B Exemples d'éléments et tâches du programme pendant les phases principales d'un projet	64
C Normes applicables à chaque élément et tâche	68
D Bibliographie	70

Clause	Articles
6.5 Externally provided products	41
6.5.1 Subcontracted products	41
6.5.2 Customer-provided products	43
6.6 Analysis, prediction and design review	43
6.6.1 Fault modes and effects analysis	43
6.6.2 Fault tree analysis	43
6.6.3 Stress and load analysis	45
6.6.4 Human factors analysis	45
6.6.5 Predictions	45
6.6.6 Trade-off analysis	47
6.6.7 Risk analysis	47
6.6.8 Formal design review	47
6.7 Verification, validation and test	49
6.7.1 Verification, validation and test planning	49
6.7.2 Life testing	51
6.7.3 Dependability testing	51
6.7.4 Reliability growth testing	51
6.7.5 Production testing	51
6.7.6 Acceptance testing	51
6.7.7 Reliability stress screening	53
6.8 Life-cycle cost programme	53
6.9 Operation and maintenance support planning	53
6.9.1 Maintenance support planning	53
6.9.2 Installation	55
6.9.3 Support services	55
6.9.4 Support engineering	55
6.9.5 Spares provisioning	55
6.10 Improvements and modifications	57
6.10.1 Improvement programmes	57
6.10.2 Modification control	57
6.11 Experiences feedback	57
6.11.1 Data acquisition	57
6.11.2 Data analysis	59
Annexes	
A Simplified flow diagram of an example of a dependability programme	63
B Examples of programme elements and tasks during the principal phases of a project	65
C Standards applicable to each element and task	69
D Bibliography	71

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 2: Eléments et tâches du programme de sûreté de fonctionnement

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant des questions techniques, représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales; ils sont publiés comme normes, rapports techniques ou guides et agréés comme tels 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.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La présente partie de la CEI 300 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	Rapport de vote
56/437/FDIS	56/488/RVD

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

La Norme Internationale CEI 300 est publiée en trois parties:

- CEI 300-1: Gestion du programme de sûreté de fonctionnement
- CEI 300-2: Eléments et tâches du programme de sûreté de fonctionnement
- CEI 300-3: (Série de guides d'application)

L'annexe A fait partie intégrante de la présente norme.

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 2: Dependability programme elements and tasks

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international cooperation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters, express as nearly as possible an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are 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.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 300 has been prepared by IEC technical committee 56: Dependability.

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

DIS	Report on voting
56/437/FDIS	56/488/RVD

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

This international Standard is one of the several Parts:

- IEC 300-1: Dependability programme management
- IEC 300-2: Dependability programme elements and tasks
- IEC 300-3: (Application guides series)

Annex A forms an integral part of this standard.

Annexes B, C and D are for information only.

INTRODUCTION

Trois facteurs sont d'une importance fondamentale pour ceux qui ont la responsabilité du développement d'un nouveau produit et pour ceux qui auront la responsabilité de l'utilisation ou de l'exploitation du produit, ce sont:

Les performances

Est-ce que les performances du produit (y compris la sûreté de fonctionnement) correspondront aux attentes et aux besoins de l'utilisateur final?

Le coût

Quel sera le coût, non seulement de développement et de fabrication du produit, mais aussi d'exploitation et de maintenance et éventuellement de mise au rebut, c'est-à-dire quel sera le coût global du produit?

Le planning

Est-ce que le produit sera disponible dans le délai exigé et apparaîtra-t-il sur le marché au moment approprié?

La satisfaction du client, la réputation du produit et de son fournisseur dépendent pour une grande part de la manière dont ces facteurs sont gérés et harmonisés pendant les différentes phases du cycle de vie.

Le terme sûreté de fonctionnement englobe la fiabilité, la maintenabilité, la disponibilité et le soutien logistique de maintenance. La fiabilité, la disponibilité et la maintenabilité sont elles-mêmes des caractéristiques de performance fondamentales et sont fréquemment spécifiées en tant qu'exigences clés d'un produit.

Le soutien logistique de maintenance est l'aptitude à fournir les moyens nécessaires pour maintenir le produit.

Les caractéristiques de sûreté de fonctionnement d'un produit ont une influence majeure sur l'aptitude d'ensemble du produit à satisfaire les exigences de l'utilisateur et pourraient bien être des aspects fondamentaux et dominants de la qualité. La sûreté de fonctionnement a aussi une influence majeure sur les coûts d'exploitation et de maintenance du produit en utilisation, ainsi que sur l'obtention d'un coût de cycle de vie acceptable.

Le coût initial ou d'achat d'un produit est souvent le facteur qui influence principalement le choix de l'utilisateur, mais il est important de reconnaître que le coût d'achat est seulement une partie du coût total de possession d'un produit. Les coûts d'exploitation et de maintenance peuvent être réduits de façon importante si le produit est conçu pour être fiable et maintenable, c'est-à-dire d'un fonctionnement plus sûr. L'amélioration et le développement du produit, dans ces conditions, accroît le coût d'achat, mais le coût supplémentaire le plus important est souvent compensé par des coûts d'exploitation et de maintenance réduits de façon importante. Il est important de réaliser des études de compromis pour optimiser le coût de l'amélioration de la fiabilité et de la maintenabilité par rapport à la baisse attendue du coût réalisée sur l'ensemble du cycle de vie du produit.

Il est important que le client comme le fournisseur reconnaissent que les caractéristiques de sûreté de fonctionnement peuvent avoir un impact majeur sur la performance et la qualité du produit, le coût et le planning, comme cela a été décrit plus haut.

INTRODUCTION

Three factors are of fundamental importance to those responsible for developing a new product and to those who will be responsible for using or operating the product; they are:

Performance

Will the performance (including dependability) of the product meet the expectations and needs of the end user?

Cost

What will be the cost, not only of developing and producing the product, but also of operating and maintaining and eventually disposing of it, i.e. what will be its life-cycle cost?

Timescale

Will the product be available when required and appear on the market at the appropriate time?

The customer's satisfaction with a product, and the reputation of the product and of its supplier, depends to a considerable degree on how well these factors are managed and harmonized during the various phases of the product life cycle.

The term dependability embraces reliability, maintainability, availability and maintenance support. Reliability, availability and maintainability are themselves fundamental product performance characteristics and are frequently specified as key product requirements.

Maintenance support is the ability to provide the resources required to maintain the item.

The dependability characteristics of a product have a major influence on the overall ability of the product to satisfy the requirements of the user and may well be fundamental and dominating aspects of quality. Dependability also has a major effect on the cost of operating and maintaining the product in use and on the achievement of acceptable life-cycle cost.

The initial or purchase cost of a product is often the major factor influencing the user's selection but it is important to recognize that the purchase cost is only a part of the total cost of ownership of a product. The costs of operation and maintenance can be greatly reduced if the product is designed to be reliable and maintainable. Improving and developing a product in this way usually adds to the purchase cost, but the greater additional cost is often compensated by greatly reduced operating and maintenance costs. It is important to perform studies to trade off the cost of improving reliability and maintainability against the expected reduction in cost achieved over the whole life of the product.

It is important that both supplier and customer should recognize that dependability characteristics may have a major impact on product performance, cost and time scale as described above.

Les exigences de la sûreté de fonctionnement sont souvent complexes et dans le but de les réaliser il est nécessaire de répartir les moyens appropriés, soigneusement planifiés et coordonnés au sein d'un programme de sûreté de fonctionnement. L'objectif de tels programmes est de s'assurer que toutes les exigences de fiabilité, maintenabilité, disponibilité et soutien logistique de maintenance sont remplies; un utilisateur aura besoin de réaliser un programme de sûreté de fonctionnement conçu pour s'assurer que les exigences du soutien logistique de maintenance sont satisfaites.

Il convient que les divers programmes de sûreté de fonctionnement (par exemple le programme de gestion de la fiabilité, le programme de gestion de la maintenabilité) soient complètement intégrés dans l'ensemble du programme associé au produit et dans le programme qualité du produit.

Une spécification des exigences de la sûreté de fonctionnement constitue souvent la base de la conception du produit et de son soutien logistique de maintenance et il convient en conséquence de le préparer avant que la phase de conception ne démarre.

Cette norme est un guide général pour établir les programmes de sûreté de fonctionnement et elle est applicable aux matériels et aux logiciels. Il convient que les éléments choisis pour élaborer le programme associé à un produit spécifique soient adaptés en fonction des exigences particulières, des circonstances et des conditions qui s'appliquent.

Il convient que le choix des éléments particuliers, l'importance à donner à chacun d'eux et le planning de l'ensemble du programme de sûreté de fonctionnement prennent en compte les conditions du marché, les exigences et attentes des utilisateurs, la situation contractuelle, et les exigences d'ensemble du produit et du soutien qui lui est associé. Les éléments d'un programme particulier doivent aussi être ajustés à la phase du cycle de vie dans laquelle ils sont situés.

WITKOOP

Dependability requirements are often complex and in order to achieve them it is necessary to allocate appropriate resources, carefully planned and coordinated, into a dependability programme. The object of such programmes is to ensure that all reliability, maintainability, availability and maintenance support requirements are met. A supplier will typically need to implement dependability programmes to ensure that product reliability and maintainability requirements are met; a user will need to implement a dependability programme designed to ensure that maintainability support requirements are satisfied.

The various dependability programmes (for example the reliability management programme and the maintainability management programme) should be fully integrated into the overall product programme and into the product quality programme.

The specified dependability requirements are often a major feature of the design of the product and of its maintenance support and the specification should therefore be prepared before the design work is started.

This standard provides general guidance on the establishment of dependability programmes and is applicable to hardware products and systems containing software. The elements selected to provide the programme for a specific product should be tailored according to the individual requirements, circumstances and conditions that apply.

The selection of individual elements, the emphasis to be given to each element and the scale of the overall dependability programme should take account of the conditions of the market, the requirements and expectations of users, the contractual situation and the overall requirements for the product and its support. Individual programme elements also need to be adjusted to the phase of the life cycle in which they are implemented.

Withholding

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 2: Eléments et tâches du programme de sûreté de fonctionnement

1 Domaine d'application

La présente partie de la CEI 300 décrit les éléments d'un programme de sûreté de fonctionnement et fournit un guide sur la sélection des tâches nécessaires afin d'aboutir à la sûreté de fonctionnement spécifiée des produits. Cette norme est harmonisée avec l'ISO 9004-1. Elle est applicable aux matériels et aux systèmes comprenant des logiciels.

Les descriptions des éléments d'un programme particulier sont fournies. Cependant, les procédures détaillées qui doivent être utilisées pour mettre en œuvre les tâches ne sont pas incluses; à leur place, on se réfère aux guides d'application de la CEI 300-3 et aux Normes internationales de la CEI sur la gestion de la sûreté de fonctionnement.

Le cadre de cette partie de la CEI 300 concerne en premier lieu le cas des relations entre deux parties: un «fournisseur» qui fournit des produits ou des services de maintenance à un «client». Des parties du produit peuvent être achetées par le fournisseur à une autre source. Lorsqu'il est nécessaire de clarifier une telle situation, les termes «fournisseur» (en contact direct avec le client) et «sous-traitant» (en contact direct avec le fournisseur) sont utilisés. Le véritable utilisateur (utilisateur final) du produit peut être «le client» ou un tiers.

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 Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes aux accords fondés sur la présente partie de la CEI 300 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes Internationales en vigueur à un moment donné.

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

CEI 300-1/ISO 9000-4: 1993, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement*

ISO 8402: 1994, *Management de la qualité et assurance de la qualité – Vocabulaire*

ISO 9001: 1994, *Systèmes qualité – Modèle pour l'assurance de la qualité en conception, développement, production, installation et soutien après la vente et prestations associées*

ISO 9004-1: 1994, *Gestion de la qualité et éléments de système qualité – Partie 1: Lignes directrices*

DEPENDABILITY MANAGEMENT –

Part 2: Dependability programme elements and tasks

1 Scope

This Part of IEC 300 describes the elements of a dependability programme and gives guidance on the selection of tasks necessary to achieve specified dependability of products. This standard cross-references and complements ISO 9004-1. It is applicable to hardware and systems containing software products.

Descriptions of individual programme elements are provided. Detailed procedures to be employed when implementing the tasks are not included but reference is made to related application guides contained in IEC 300-3 and to other IEC International Standards on dependability management.

The format of this part of IEC 300 primarily addresses the case of a two party relationship, between a "supplier" who provides products or maintenance services and a "customer". Parts of the product may be purchased from other sources by the supplier (by subcontracting). Where it is necessary to clarify such a situation, the terms "first level supplier" (with direct relation to the customer) and "second level supplier" ("subcontractor", with direct relation to the first level supplier) are used. The actual users (end users) of the product may be the customers themselves or a third body.

2 Normative references

The following normative documents contain provisions which, through reference in this text constitute provisions of this part of IEC 300. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this part of IEC 300 are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

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

IEC 300-1/ISO 9000-4: 1993, *Dependability management – Part 1: Dependability programme management*

ISO 8402: 1994, *Quality management and quality assurance – Vocabulary*

ISO 9001: 1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing*

ISO 9004-1; 1994, *Quality management and quality system elements – Part 1: Guidelines*

3 Définitions

Pour les besoins de la présente Norme internationale les termes et définitions de la CEI 50(191), de la CEI 300-1 s'appliquent ainsi que l'ISO 8402. De plus les termes et définitions suivants sont utilisés:

3.1 tâche du programme de sûreté de fonctionnement: Ensemble d'activités concernant les aspects sûreté de fonctionnement d'un produit.

3.2 élément du programme de sûreté de fonctionnement: Un ensemble de tâches du programme de sûreté de fonctionnement appartenant au domaine d'un sujet spécifique.

3.3 cycle de vie: Intervalle de temps compris entre le concept et la définition d'un produit et son retrait du service.

3.4 phase de concept et de définition: Phase du cycle de vie d'un produit au cours de laquelle le besoin du produit est établi et (généralement) ses exigences sont spécifiées.

3.5 phase de conception et de développement: Phase du cycle de vie d'un produit au cours de laquelle le matériel et/ou le logiciel est créé et documenté suivant les spécifications détaillées de fabrication et/ou codage et pendant laquelle sont réalisées les autres documentations du produit, comme les instructions d'utilisation et de maintenance.

3.6 phase de fabrication: Phase du cycle de vie d'un produit au cours de laquelle le produit est fabriqué, le logiciel dupliqué et le produit est assemblé.

3.7 phase d'installation: Phase du cycle de vie d'un produit au cours de laquelle le produit est installé.

3.8 phase d'exploitation et de maintenance: Phase du cycle de vie d'un produit au cours de laquelle le produit est utilisé, maintenu et soutenu.

3.9 phase de mise au rebut: Phase du cycle de vie d'un produit, postérieure à la phase d'exploitation et de maintenance au cours de laquelle le produit est retiré de son site d'exploitation, mis hors service, désassemblé, détruit ou stocké si nécessaire dans un environnement protégé.

4 Vue générale d'un programme de sûreté de fonctionnement

4.1 Généralités

Les objectifs d'un programme de sûreté de fonctionnement sont de s'assurer que l'effort adéquat et effectif est apporté pour faire en sorte que la sûreté de fonctionnement soit une mesure principale de la qualité pendant toutes les phases du cycle de vie d'une entité (depuis la définition en passant par la phase de conception et d'acceptation, jusqu'à la fin de la vie) et que les activités qui contribuent à la sûreté de fonctionnement sont intégrées correctement avec les activités contractuelles et les spécifications. Il convient qu'un programme de sûreté de fonctionnement produise en continu l'étude des exigences qualitatives et quantitatives à travers toutes les phases d'un projet; il convient que les évaluations de sûreté de fonctionnement soient mises à jour, que les exigences spécifiées soient vérifiées, que les activités soient intégrées avec les autres éléments du programme de développement, de production et d'exploitation. Voir l'annexe A.

3 Definitions

For the purpose of this International Standard the terms and definitions of IEC 50(191) and IEC 300-1 apply together with ISO 8402. In addition, the following terms and definitions are used:

3.1 dependability programme task: A set of activities addressing dependability aspects of a product.

3.2 dependability programme element: A set of dependability programme tasks, pertaining to a specific subject area.

3.3 life cycle: The time interval from a product's inception until its ultimate disposal and removal from use.

3.4 concept and definition phase: That product life-cycle phase during which the need for the product is established and (usually) its requirements specified.

3.5 design and development phase: That product life-cycle phase during which the product's hardware and/or software is created and documented as detailed manufacturing/coding specifications, and other product documentation such as use and maintenance instructions produced.

3.6 manufacturing phase: That product life-cycle phase during which the product is produced, software replicated and the product assembled.

3.7 installation phase: That product life-cycle phase during which the product is installed.

3.8 operation and maintenance phase: That product life-cycle phase during which the product is used for any purpose and is maintained and supported.

3.9 disposal phase: That possible product life-cycle phase, after the operation and maintenance phase, during which the product is removed from its use site and decommissioned, dismantled, destroyed or stored if necessary in a protected environment.

4 Dependability programme overview

4.1 General

The aims of a dependability programme are to ensure that adequate and effective effort is brought to bear on dependability as a principal quality attribute during all phases of the life-cycle of an item (from definition through design and acceptance into service, to the end of its working life) and that the activities which contribute to dependability are properly integrated with other contract and specification activities. A dependability programme should provide continuous study of both quantitative and qualitative requirements throughout all phases of a project. This also includes the updating of dependability assessments and the verification of specified requirements. The dependability programme elements should be integrated with other elements of the development, production and operation programme. See annex A.

Il convient que l'étendue et le contenu du programme de sûreté de fonctionnement soient dépendants des caractéristiques particulières du projet et de toute contrainte spécifique, ainsi que de l'importance de la sûreté de fonctionnement pour le produit en question.

Pour de nombreux projets, il n'y a pas de démarcation précise entre les phases de définition, de conception, de développement, de production et d'exploitation. Toutefois, pour la clarté, ces distinctions sont faites au cours de cet article. Les activités propres à chacune des phases sont données en annexe B qui liste les tâches du programme de sûreté de fonctionnement qui peuvent être choisies et réalisées pendant les phases de cycle de vie. Elles sont expliquées dans le texte de cet article, en rapport avec les responsabilités liées à la gestion d'ensemble du projet et au planning. Il convient que le programme de sûreté de fonctionnement soit préparé conjointement avec d'autres programmes en rapport avec le produit ou le projet. La référence aux normes de la CEI appropriées sont données en annexe C.

Les relations entre les phases du cycle de vie et les tâches du programme de sûreté de fonctionnement sont données en figure 1.

NOTE – La figure 1 ainsi que les annexes A, B et C présentent des aspects de programmes de sûreté de fonctionnement généraux, selon des perspectives différentes. Dans une certaine mesure, ces présentations sont simplifiées, ce qui entraîne le risque de quelques différences entre elles.

Un programme effectif de sûreté de fonctionnement peut être construit par le choix des éléments et tâches appropriés en accord avec le processus d'adaptation décrit dans l'article 5, pour correspondre aux besoins et aux circonstances spécifiques.

Les activités de sûreté de fonctionnement à mettre en oeuvre pour chaque phase du cycle de vie du produit doivent être sélectionnées suivant le contexte du cycle de vie total du produit. A quelque instant que ce soit, les décisions prises ont un impact sur la sûreté de fonctionnement du produit et le coût au moment de la décision et dans les phases ultérieures du cycle de vie.

Il convient de noter qu'une exigence légale ou réglementaire, soit dans la situation des moyens d'utilisation ou des moyens de fabrication, doit être prise en compte et que la conformité à la présente norme ne confère pas, par elle-même, une immunité en regard des obligations légales.

The extent and contents of the dependability programme should be governed by the particular needs of the project and any specific constraints, and on the importance of dependability of the actual product.

In many projects, there are no sharp demarcations between the definition, design and development, production and operation phases. However, for clarity, distinctions are drawn in this clause. The activities appropriate to the different phases are given in annex B which lists the dependability programme tasks that may be selected for implementation during the product life-cycle phases. They are explained in the text of this clause in relation to the overall project management responsibilities and time scale. The dependability programme should be prepared in conjunction with other project/product related programmes. References to appropriate IEC standards are given in annex C.

An example of the relationships between life-cycle phases and dependability programme elements and tasks is given in figure 1.

NOTE – Figure 1 and annexes A, B, and C present views of generalized dependability programmes from different perspectives. All are simplified to some extent and this gives rise to minor differences between them.

An effective dependability programme can be assembled by selecting the appropriate elements and tasks in accordance with the tailoring process, described in clause 5, to suit specific needs and circumstances.

The dependability activities to be implemented during each phase of the product life cycle should be selected in the context of the total life cycle of the product. Decisions made at any instant of time have an impact on product dependability and cost at that time and in subsequent phases of the product life.

It should be noted that a legal or regulatory requirement in either user or manufacturing facility location should be considered and that compliance with this standard does not of itself confer immunity from legal obligations.

Article	Tâche	Phase de cycle de vie					
		Concept et définition	Conception et développement	Fabrication	Installation	Exploitation et maintenance	Mise au rebut
6.1	PLANIFICATION ET GESTION						
6.1.1	Plans de sûreté de fonctionnement						
6.1.2	Gestion des décisions de projet						
6.1.3	Gestion de la traçabilité						
6.1.4	Gestion de la configuration						
6.2	REVUE DE CONTRAT ET LIAISON						
6.2.1	Revue de contrat						
6.2.2	Représentants de la direction						
6.3	EXIGENCES DE SÛRETÉ DE FONCTIONNEMENT						
6.3.1	Spécification des exigences de sûreté de fonctionnement						
6.3.2	Interprétation des exigences						
6.3.3	Répartition des exigences						
6.4	INGENIERIE						
6.4.1	Ingénierie de la fiabilité						
6.4.2	Ingénierie de la maintenabilité						
6.4.3	Ingénierie du soutien logistique de maintenance						
6.4.4	Ingénierie de la testabilité						
6.4.5	Ingénierie des facteurs humains						
6.5	PRODUITS FOURNIS EXTÉRIEUREMENT						
6.5.1	Produits sous-traités						
6.5.2	Produits fournis par le client						
6.6	ANALYSE, PRÉDICTION ET REVUE DE CONCEPTION						
6.6.1	Analyse des modes de défaillance et de leurs effets						
6.6.2	Analyse par arbre de panne						
6.6.3	Analyse des contraintes et des charges						
6.6.4	Analyse des facteurs humains						
6.6.5	Prévision						
6.6.6	Analyse de compromis						
6.6.7	Analyse des risques						
6.6.8	Revue de conception formalisée						
6.7	VÉRIFICATION, VALIDATION, ESSAI						
6.7.1	Planification de la vérification, de la validation et des essais						
6.7.2	Essai de durée de vie						
6.7.3	Essai de sûreté de fonctionnement						
6.7.4	Essai de croissance de fiabilité						
6.7.5	Essai en production						
6.7.6	Essai d'acceptation						
6.7.7	Essai de déverminage sous contrainte						
6.8	PROGRAMME DE COÛT DU CYCLE DE VIE						
6.9	PLANIFICATION DE L'EXPLOITATION ET DE LA MAINTENANCE						
6.9.1	Planification de la logistique de maintenance						
6.9.2	Installation						
6.9.3	Service de soutien						
6.9.4	Ingénierie de soutien						
6.9.5	Approvisionnement des rechanges						
6.10	AMÉLIORATION ET MODIFICATIONS						
6.10.1	Programmes d'amélioration						
6.10.2	Gestion des modifications						
6.11	RETOUR D'EXPÉRIENCE						
6.11.1	Acquisition des données						
6.11.2	Analyse des données						

Figure 1 – Relation entre les phases du cycle de vie et les tâches du programme de sûreté de fonctionnement

Clause	Element/task	Life-cycle phase					
		Concept and definition	Design and development	Manufacturing	Installation	Operation and maintenance	Disposal
6.1	PLANNING AND MANAGEMENT						
6.1.1	Dependability plans						
6.1.2	Project decision management						
6.1.3	Traceability management						
6.1.4	Configuration management						
6.2	CONTRACT REVIEW AND LIAISON						
6.2.1	Contract review						
6.2.2	Management representative						
6.3	DEPENDABILITY REQUIREMENTS						
6.3.1	Specification of dependability requirements						
6.3.2	Requirements interpretation						
6.3.3	Requirements allocation						
6.4	ENGINEERING						
6.4.1	Reliability engineering						
6.4.2	Maintainability engineering						
6.4.3	Maintenance support engineering						
6.4.4	Testability engineering						
6.4.5	Human Factors engineering						
6.5	EXTERNALLY PROVIDED PRODUCTS						
6.5.1	Subcontracted products						
6.5.2	Customer-provided products						
6.6	ANALYSIS, PREDICTION AND DESIGN REVIEW						
6.6.1	Fault modes and effects analysis						
6.6.2	Fault tree analysis						
6.6.3	Stress and load analyses						
6.6.4	Human factors analysis						
6.6.5	Predictions						
6.6.6	Trade-off analysis						
6.6.7	Risk analysis						
6.6.8	Formal design review						
6.7	VERIFICATION, VALIDATION AND TEST						
6.7.1	Verification, validation and test planning						
6.7.2	Life testing						
6.7.3	Dependability testing						
6.7.4	Reliability growth testing						
6.7.5	Production testing						
6.7.6	Acceptance testing						
6.7.7	Reliability stress screening						
6.8	LIFE-CYCLE COST PROGRAMME						
6.9	OPERATION AND MAINTENANCE SUPPORT PLANNING						
6.9.1	Maintenance support planning						
6.9.2	Installation						
6.9.3	Support services						
6.9.4	Support engineering						
6.9.5	Spares provisioning						
6.10	IMPROVEMENTS AND MODIFICATIONS						
6.10.1	Improvement programmes						
6.10.2	Modification control						
6.11	EXPERIENCES FEEDBACK						
6.11.1	Data acquisition						
6.11.2	Data analysis						

Figure 1 – Relation between life cycle phases and dependability programme tasks

4.2 Cycle de vie d'un produit

4.2.1 Phase de concept et de définition

La phase de concept et de définition est la phase du cycle de vie pendant laquelle les besoins du produit sont définis et ses exigences spécifiées. Pendant cette phase, les bases de la sûreté de fonctionnement du produit et de son coût de cycle de vie sont établies. C'est dans cette phase que les décisions prises ont le plus grand impact sur le produit et son coût de cycle de vie.

Il convient que les activités de sûreté de fonctionnement dans cette phase se concentrent sur l'obtention des exigences adaptées au produit et à son soutien futur ainsi qu'à l'établissement d'un plan de sûreté de fonctionnement utilisé comme base pour le contrôle de la sûreté de fonctionnement pendant les phases ultérieures.

4.2.2 Phase de conception et de développement

C'est la phase du cycle de vie pendant laquelle les aspects matériel et/ou logiciel du produit sont créés et documentés, suivant les spécifications détaillées de fabrication et/ou codage et pendant laquelle sont réalisées les autres documentations du produit, comme les instructions d'utilisation et de maintenance.

Les objectifs premiers des activités de sûreté de fonctionnement pendant cette phase sont de s'assurer que:

- les exigences de la spécification de sûreté de fonctionnement sont totalement prises en compte pendant le processus de conception;
- les activités d'analyse et de prévision sont mises en oeuvre et utilisées pour atteindre la sûreté de fonctionnement du produit;
- les procédures et les critères de validation, de vérification et d'essais sont définis et exécutés selon les exigences de sûreté de fonctionnement;
- les exigences de sûreté de fonctionnement allouées à toutes les parties de produit livrées par des sous-traitants ou par le client sont respectées;
- les activités d'ingénierie et le planning du soutien logistique de maintenance sont coordonnés avec la conception du produit pour assurer la conformité avec toutes les exigences de sûreté de fonctionnement.
- les exigences de la mise au rebut sont définies.

4.2.3 Phase de fabrication

C'est la phase du cycle de vie pendant laquelle le matériel est fabriqué, le logiciel dupliqué et le produit assemblé.

Il convient que les activités de sûreté de fonctionnement soient dirigés afin de s'assurer que les performances de sûreté de fonctionnement du produit réalisées pendant la phase de conception et développement ne sont pas dégradées par le procédé de fabrication. Il convient que le programme de sûreté de fonctionnement établisse des procédures à suivre pendant la production des systèmes et des équipements afin de s'assurer que la fiabilité est conforme à des niveaux spécifiés.

4.2 *Life cycle of product*

4.2.1 *Concept and definition phase*

The concept and definition phase is the life-cycle phase during which the need for the product is established and its requirements specified. During this phase the foundation is laid for the product's dependability and its life-cycle cost. Decisions made during this phase have greatest impact on the product and its life-cycle cost.

The dependability activities in this phase should concentrate on reaching the correct requirements for the product and its future support and for establishing the dependability plan used as a basis for the control of dependability during the subsequent phases.

4.2.2 *Design and development phase*

The design and development phase is the life-cycle phase during which the product's hardware and/or software is created and documented as detailed manufacturing/coding specifications, and other product documentation such as use and maintenance instructions are produced.

The prime objectives of dependability activities during this phase are to ensure that:

- the requirements of the dependability specification are taken into full consideration during the design process;
- analysis and prediction activities are implemented and used to achieve dependability of the product;
- validation, verification and test procedures and criteria are defined and executed based on dependability requirements;
- dependability requirements allocated to any part of the product provided by second level suppliers or customers are complied with;
- maintenance support planning and engineering activities are coordinated with the product design to ensure compliance with dependability requirements;
- disposal requirements are defined.

4.2.3 *Manufacturing phase*

The manufacturing phase is the life-cycle phase during which the product is produced, software replicated and the product assembled.

Dependability activities during this phase should be directed at ensuring that dependability performances of the product achieved during design and development are not degraded during the manufacturing process. The dependability programme should state procedures to be followed during the production of systems and equipment to ensure that dependability meets specified levels.

Pendant cette phase, les activités essentielles du programme de sûreté de fonctionnement sont:

- essai de fiabilité et de maintenabilité;
- essai de production;
- déverminage de fiabilité sous contrainte.

4.2.4 Phase d'installation

C'est la phase du cycle de vie pendant laquelle le produit est installé.

Il convient que les activités de sûreté de fonctionnement soient dirigées afin de s'assurer que les performances du produit ne sont pas dégradées pendant l'installation. Il convient de fournir les procédures et les instructions pour conduire l'inspection d'acceptation, l'essai des systèmes et des composants par vérification de la conformité à la spécification initiale et à la conception.

Pendant cette phase, les activités essentielles du programme de sûreté de fonctionnement sont:

- les essais de mise en service;
- les essais d'acceptation;
- les essais de croissance de fiabilité;
- la démonstration des performances de fiabilité et maintenabilité;
- la création et la mise à jour du recueil des données et leur analyse;
- la gestion des défaillances initiales.

4.2.5 Phase d'exploitation et de maintenance

C'est la phase du cycle de vie du produit pendant laquelle le produit est exploité, maintenu et soutenu. Pendant cette phase, les actions de maintenance corrective et préventive essentielles sont exécutées, si nécessaire, et la performance du produit est surveillée.

Afin de s'assurer que les niveaux requis de sûreté de fonctionnement sont valablement atteints pendant cette phase, il sera nécessaire d'établir:

- les procédures d'exploitation;
- les procédures de maintenance;
- les procédures d'alerte;
- le plan de formation;
- la liste des composants de rechanges.

La vie utile d'un produit se termine lorsque son exploitation devient trop onéreuse en raison de coûts de maintenance accrus ou d'autres facteurs, ou bien lorsque le produit devient techniquement périmé.