NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60300-3-6

Première édition
First edition
1997-11

Gestion de la sûreté de fonctionnement –

Partie 3:
Guide d'application –
Section 6: Aspects logiciels de la sûreté de fonctionnement

Dependability management –

Part 3:
Application guide –
Section 6: Software aspects of dependability

Numéro de référence
Reference number
CEI/IEC 60300-3-6: 1997

Numéros des publications

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

Publications consolidées

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

Validité de la présente publication

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

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

Les renseignements relatifs à 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**
  Accès en ligne*
- **Catalogue des publications de la CEI**
  Publié annuellement et mis à jour régulièrement
  (Accès en ligne)*

Terminologie, symboles graphiques et littéraux

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

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

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.

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

Numbering

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

Consolidated publications

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

Validity of this publication

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

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

Information on the 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**
  On-line access*
- **Catalogue of IEC publications**
  Published yearly with regular updates
  (On-line access)*

Terminology, graphical and letter symbols

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

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

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.

* See web site address on title page.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60300-3-6

Première édition
First edition
1997-11

Gestion de la sûreté de fonctionnement –

Partie 3:
Guide d'application –
Section 6: Aspects logiciels de la sûreté de fonctionnement

Dependability management –

Part 3:
Application guide –
Section 6: Software aspects of dependability

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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE U

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

SOMMAIRE

Pages

AVANT-PROPOS 4

INTRODUCTION 6

Articles

1 Domaine d'application 10

2 Références normatives 10

3 Définitions 10

4 Aspects logiciels 10

5 Phases et processus du cycle de vie d'un logiciel 12

6 Application des programmes de sûreté de fonctionnement aux produits comprenant un logiciel 14

7 Adaptation des programmes de sûreté de fonctionnement 38

Annexes

A Relation typique entre les phases du cycle de vie du produit et les phases du cycle de vie du logiciel 42

B Sélection des éléments du programme de sûreté de fonctionnement 44

C Processus du cycle de vie du logiciel 46

D Association des processus du cycle de vie du logiciel avec les phases du cycle de vie du produit 54

E Correspondances entre la CEI 60300-2 et l'ISO 9000-3 56

F Bibliographie 58

CONTENTS

Page

FOREWORD 5
INTRODUCTION 7

Clause

1 Scope 11
2 Normative references 11
3 Definitions 11
4 Software aspects 11
5 Software life cycle phases and processes 13
6 Application of dependability programmes to products containing software 15
7 Tailoring of dependability programmes 39

Annexes

A Typical relationship of product life cycle phases and software life cycle phases 43
B Selection of dependability programme elements 45
C Software life cycle processes 47
D Association of the software life cycle processes with the product life cycle phases 55
E Cross-references between IEC 60300-2 and ISO 9000-3 57
F Bibliography 59

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3: Guide d'application – Section 6: Aspects logiciels de la 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 les 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 Norme internationale CEI 60300-3-6 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:

FDIS	Rapport de vote
56/583/FDIS	56/600/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.

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3: Application guide –
Section 6: Software aspects of dependability

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation 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. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-6 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/583/FDIS	56/600/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.

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

INTRODUCTION

La sûreté de fonctionnement est un terme générique utilisé pour traduire la disponibilité d'un système ou d'un produit. Cette disponibilité dépend de la fiabilité, de la maintenabilité et de la logistique de maintenance du produit. Dans de nombreux systèmes et produits, la fiabilité, la maintenabilité et la disponibilité font partie des caractéristiques les plus importantes aux yeux des utilisateurs qui recherchent un fonctionnement rentable. La fiabilité et la maintenabilité sont des caractéristiques inhérentes à la conception d'un produit, alors que la logistique de maintenance est un critère indépendant qui influe sur la qualité du service et qui reflète la capacité d'une organisation de maintenance à fournir les ressources nécessaires pour atteindre les objectifs de disponibilité.

Pour qu'un programme de sûreté de fonctionnement soit efficace, sa mise en oeuvre doit être adaptée au produit. Il est recommandé d'inclure ce programme dans celui de gestion globale du projet afin d'obtenir une bonne coordination avec le développement, la fabrication, la vérification et l'utilisation du produit. Il est aussi conseillé que les éléments et les tâches du programme de sûreté de fonctionnement soient cohérents avec les autres programmes de support tels que la gestion de la qualité, la gestion de la configuration, la collecte des données etc.

La gestion de la sûreté de fonctionnement inclut la planification du projet, la spécification, l'analyse de la conception, la vérification et la validation, la réalisation, l'évaluation du produit ou du service ainsi que le retour d'expérience. Les systèmes et produits modernes comportent souvent un logiciel comme entité fonctionnelle, utilisé pour atteindre les objectifs de performances opérationnelles. Le logiciel, inclus dans le système ou dans le produit, est assujetti au processus de gestion de la sûreté de fonctionnement. Le présent guide d'application concerne les aspects logiciels liés à cette gestion. Il donne des directives spécifiques permettant de sélectionner les actions appropriées et de les appliquer aux programmes de sûreté de fonctionnement associés aux produits contenant le logiciel ou aux systèmes configurés par le logiciel et comprenant des éléments matériels.

La disponibilité d'un produit peut être affectée par des défaillances du matériel, des défauts de logiciel ou des erreurs humaines. Un mauvais fonctionnement provoquant des temps d'indisponibilité peut être imputable à des anomalies de conception interne ou à des interférences avec l'extérieur, y compris des erreurs de procédure. Des défaillances du produit peuvent, elles aussi, provenir d'erreurs de conception internes liées à des problèmes de matériel ou de logiciel. Les matériels défectueux ou les pièces usées peuvent être identifiés et localisés, réparés ou remplacés, afin de conserver le niveau de fiabilité du produit. A la différence de la plupart des matériels, un logiciel, une fois créé sous la forme de codes et d'instructions, ne s'use pas et ne se détériore pas. C'est la raison pour laquelle certains processus applicables aux logiciels peuvent être différents de ceux utilisés pour la mise en oeuvre du matériel. Le but de ce guide d'application est de lier le cycle de vie du logiciel à celui du produit, dans le cadre de la gestion de la sûreté de fonctionnement.

La gestion de la sûreté de fonctionnement est définie dans la CEI 60300-1. Les éléments et les tâches du programme correspondant sont spécifiés dans la CEI 60300-2. Le présent guide d'application est complémentaire à la CEI 60300-2 en ce qui concerne la mise en oeuvre du programme de sûreté de fonctionnement des systèmes ou produits dotés d'un logiciel. L'accent est mis sur l'application séquentielle des activités relatives au logiciel associées à la mise en oeuvre de la CEI 60300-2, ainsi que cela est présenté à l'annexe A. L'annexe B présente la sélection des éléments du programme de sûreté de fonctionnement associés aux phases du cycle de vie du logiciel.

Des efforts ont été réalisés pour harmoniser le présent guide d'application avec l'ISO/CEI 12207 sur les processus du cycle de vie du logiciel. Une vue générale du processus du cycle de vie du logiciel est fournie à l'annexe C. Des correspondances sont identifiées à l'annexe D pour faciliter l'association du processus de cycle de vie du logiciel avec les éléments de sûreté de fonctionnement appropriés et les phases du cycle de vie du produit.

INTRODUCTION

Dependability is the collective term describing the availability performance of a system or product. The availability performance is influenced by the reliability, maintainability and maintenance support performance factors. In many systems and products, reliability, maintainability, and availability rank amongst the dominant performance characteristics of importance to the users seeking cost-effective operation. Reliability and maintainability are performance characteristics inherent to the product design. Maintenance support is external to the product itself, and will affect the quality of service. Maintenance support performance reflects the ability of the maintenance organization to provide the necessary resources to sustain a level of maintenance support effort to achieve availability performance objectives.

A dependability programme must be tailored to the product for effective application. The dependability programme should form part of the overall project management programme for proper coordination with product development, manufacture, verification and deployment. Dependability programme elements and tasks should be consistent with the other support programmes such as quality management, configuration management, data collection etc.

The dependability management process includes project planning, specification, design analysis, verification and validation, implementation, evaluation, and data feedback of the product or service. Modern systems and products often contain software as a functional entity to achieve operational performance objectives. The software contained in the system or embedded in the product is subject to the dependability management process. This application guide addresses the software aspects of dependability. It provides specific guidance on the selection and application of relevant activities in dependability programmes associated with products containing software, or systems configured by software with hardware elements.

The availability performance of a product can be affected by hardware failures, software faults, or human errors. Product malfunction causing downtimes can be traceable to its internal design anomalies, or due to external interference including procedural errors. Product failures can arise from internal design faults relating to hardware or software problems. Failed hardware and worn-out parts can be identified and isolated, repaired or replaced to maintain the same level of product reliability. Unlike most physical hardware, software, once created in the form of codes or instructions, will not wear-out or deteriorate. Hence, some of the software processes may be different from those applicable for the hardware implementation. The intent of this application guide is to relate the software life cycle processes with the product life cycle phases within the dependability management framework.

Dependability management is defined in IEC 60300-1. Dependability programme elements and tasks are specified in IEC 60300-2. This application guide complements IEC 60300-2 in terms of dependability programme implementation of systems or products containing software. Emphasis is placed on the time-phase application of relevant software activities associated with the implementation of IEC 60300-2 as shown in annex A. Annex B presents the selection of dependability programme elements associated with the software life cycle phases.

Efforts have been made to harmonize this application guide with ISO/IEC 12207 on software life cycle processes. An overview of the software life cycle processes is provided in annex C. Cross-references are identified in annex D to facilitate association of software life cycle processes with relevant dependability elements and product life cycle phases.

La relation entre la sûreté de fonctionnement (série de normes CEI 60300) et la qualité (série de normes ISO 9000) est traitée dans la CEI 60300-1/ISO 9000-4 et ne sera pas abordée dans le présent guide d'application. Toutefois, il convient de noter, en termes de facteurs de qualité influençant les caractéristiques de sûreté de fonctionnement des éléments de logiciel, les recommandations de l'ISO 9000-3 concernant l'application de l'ISO 9001 aux logiciels. Les correspondances entre la CEI 60300-2 et l'ISO 9000-3 sont présentées à l'annexe E.

Une bibliographie est fournie, à l'annexe F, pour donner des références supplémentaires concernant les aspects logiciels de la sûreté de fonctionnement.

The relationship of dependability (IEC 60300 series of standards) and quality (ISO 9000 series of standards) is addressed in IEC 60300-1/ISO 9000-4 and will not be elaborated in this application guide. However, the guidelines contained in ISO 9000-3 for application of ISO 9001 to software should be noted in terms of quality factors influencing the dependability characteristics of software elements. Cross-references between IEC 60300-2 and ISO 9000-3 are shown in annex E.

A bibliography is provided in annex F for additional references to software aspects of dependability.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3: Guide d'application – Section 6: Aspects logiciels de la sûreté de fonctionnement

1 Domaine d'application

Le présent guide d'application est complémentaire à la CEI 60300-2. Il donne des lignes directrices pour la sélection des éléments et des tâches du programme de sûreté de fonctionnement, et leur application aux systèmes et produits comportant un logiciel.

Le présent guide d'application est conçu pour les chefs de projets, les gestionnaires, les concepteurs de produits, les développeurs de logiciels, les spécialistes en sûreté de fonctionnement, les spécialistes de la qualité, les personnels de soutien et les personnels chargés de l'entretien des systèmes, qui contribuent à la sûreté de fonctionnement des produits ou des systèmes.

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 section de la CEI 60300-3. 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 section de la CEI 60300-3 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 60050(191): 1990, *Vocabulaire électrotechnique international (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-1/ISO 9000-4: 1993, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement*

CEI 60300-2: 1995, *Gestion de la sûreté de fonctionnement – Partie 2: Eléments et tâches du programme de sûreté de fonctionnement*

CEI 61160: 1992, *Revue de conception formalisée*
Amendement 1 (1994)

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

3 Définitions

Pour les besoins de la présente section de la CEI 60300-3, les termes et définitions de la CEI 60050(191) et de l'ISO 8402 s'appliquent.

4 Aspects logiciels

Les aspects logiciels de la sûreté de fonctionnement traitent des considérations spécifiques relatives aux logiciels pour l'établissement et la mise en oeuvre d'un programme de sûreté de fonctionnement, pour un système ou un produit comprenant du logiciel. Le point important est d'obtenir la sûreté de fonctionnement du produit et d'atteindre les objectifs de fiabilité, de maintenabilité et de logistique de maintenance.

DEPENDABILITY MANAGEMENT –

Part 3: Application guide –
Section 6: Software aspects of dependability

1 Scope

This application guide complements IEC 60300-2 and provides guidance for selection and application of dependability elements and tasks with respect to systems or products containing software.

This application guide is intended for use by project managers, contract administrators, product designers, software developers, dependability specialists, quality specialists, support personnel and system maintainers who contribute to the dependability of products or systems.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this section of IEC 60300-3. 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 60300-3 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 60050(191): 1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60300-1/ISO 9000-4: 1993, *Dependability management – Part 1: Dependability programme management*

IEC 60300-2: 1995, *Dependability management – Part 2: Dependability programme elements and tasks*

IEC 61160: 1992, *Formal design review*
Amendment 1 (1994)

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

3 Definitions

For the purpose of this section of IEC 60300-3, the terms and definitions of IEC 60050(191) and ISO 8402 apply.

4 Software aspects

The software aspects of dependability deal with the specific software issues in the establishment and implementation of a dependability programme for a system or product containing software. Emphasis is placed on achieving dependability in the product design and performance objectives in reliability, maintainability and maintenance support.

Lorsque l'on veut doter un système ou un produit d'un programme de sûreté de fonctionnement, il est important d'adopter le point de vue du système. Un produit est une entité pouvant inclure des composants matériels et/ou logiciels. Un système est une entité composite pouvant comprendre le produit, le matériel de soutien, le personnel ainsi que les moyens de support et les services associés. Son environnement détermine ses conditions de fonctionnement et les interactions de ses composants. Sa disponibilité est mesurée ou estimée afin de vérifier que les objectifs de sûreté de fonctionnement en termes de fiabilité, maintenabilité et logistique de maintenance sont atteints.

La sûreté de fonctionnement est une mesure globale des caractéristiques d'un système dans son application ou son utilisation réelles, avec ou sans la mise en oeuvre des fonctions logicielles spécifiques qui peuvent faire partie d'un système intégré.

Il convient de noter qu'un logiciel ne peut pas fonctionner de manière isolée, mais qu'il fait partie d'un système et que son rôle est de remplir une application spécifique. C'est un moyen permettant d'atteindre les objectifs de performance d'un système. Un logiciel est caractérisé, en particulier, par sa fonction, son environnement, sa taille, son langage et sa complexité ainsi que par son installation et son processus d'évolution. Les aspects logiciels de la sûreté de fonctionnement ont rapport avec les composants logiciels du système dans le contexte de la performance de la sûreté de fonctionnement du système. Ils ne dépendent pas de la qualité du logiciel en tant que tel. Cette qualité est décrite dans l'ISO/CEI 9126 [1]*.

Les aspects logiciels de la sûreté de fonctionnement dépendent de l'intégrité du composant logiciel pendant le fonctionnement du système. Cette intégrité est inhérente à la conception et associée au confinement du risque. Le risque est une exposition indésirable ou une crainte associée à l'exploitation du système. Le risque est caractérisé par sa probabilité d'occurrence et ses impacts ou conséquences lorsque l'événement survient. La capacité d'un système et de son logiciel à confiner un risque dépend de l'architecture du système, de la tolérance aux pannes et de la rigueur avec laquelle les méthodes appropriées sont appliquées au logiciel. Le niveau d'intégrité sert à caractériser le risque assigné associé au fonctionnement du système à confiner. Lorsqu'un logiciel influe sur les performances d'un système, la relation entre sûreté de fonctionnement et intégrité est étroitement en rapport avec la criticité de l'application logicielle associée aux niveaux d'intégrité assignés.

5 Phases et processus du cycle de vie d'un logiciel

Le cycle de vie d'un logiciel est étroitement lié à celui de son système parent. Une relation typique entre les phases du cycle de vie d'un logiciel et celles d'un produit classique, conforme à la CEI 60300-1/ISO 9000-4, est indiquée à l'annexe A. Un exemple de sélection d'éléments du programme de sûreté de fonctionnement associés aux phases du cycle de vie du logiciel est présenté à l'annexe B.

Le processus du cycle de vie d'un logiciel consiste en un ensemble d'activités ou de tâches planifiées, effectuées pour atteindre le but ou l'objectif déclaré d'un projet. Ce processus implique des activités liées au logiciel, depuis sa conception jusqu'à la fin de son utilisation. Des informations détaillées sont données dans l'ISO/CEI 12207 [2]. L'annexe C donne des notes informatives sur les processus du cycle de vie des logiciels.

L'annexe D montre l'association des processus du cycle de vie des logiciels dans un programme caractéristique de sûreté de fonctionnement. La CEI 60300-2 donne la description des différents éléments d'un programme de sûreté de fonctionnement, en fonction des phases du cycle de vie d'un produit. Le processus du cycle de vie d'un logiciel n'est pas toujours directement lié au cycle de vie du produit. Les relations séquentielles du processus avec les phases ne sont qu'approximatives, car il peut se produire de grandes fluctuations entre les différents projets. C'est ainsi que, par exemple, la version d'un logiciel peut devoir être réalisée avant le début de la fabrication du matériel. Cependant, les différents éléments et tâches de

---

* Les chiffres entre crochets renvoient à la bibliographie donnée à l'annexe F.