

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61713

Première édition
First edition
2000-06

**Sûreté de fonctionnement des logiciels
pendant leurs processus de cycle de vie –
Guide d'application**

**Software dependability through
the software life-cycle processes –
Application guide**

© IEC 2000 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.

International Electrotechnical Commission
Telefax: +41 22 919 0300

e-mail: inmail@iec.ch

3, rue de Varembe Geneva, Switzerland
IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

V

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

SOMMAIRE

	Pages
AVANT-PROPOS.....	4
INTRODUCTION.....	6
Articles	
1 Domaine d'application	8
2 Références normatives	8
3 Définitions	10
4 Processus du cycle de vie d'un logiciel.....	18
5 Activités de sûreté de fonctionnement dans les processus de base.....	20
5.1 Processus d'acquisition	20
5.2 Processus de fourniture	28
5.3 Processus de développement	32
5.4 Processus d'exploitation.....	44
5.5 Processus de maintenance	50
6 Activités de sûreté de fonctionnement dans les processus de soutien du logiciel	56
7 Activités de sûreté de fonctionnement dans les processus organisationnels du cycle de vie du logiciel.....	56
Annexe A (informative) Association des processus du cycle de vie des logiciels avec les éléments et tâches du programme de sûreté de fonctionnement	62
Annexe B (informative) Interaction entre les utilisateurs et les processus de base du cycle de vie du logiciel.....	64
Bibliographie	66

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	7
Clause	
1 Scope	9
2 Normative references.....	9
3 Definitions.....	11
4 Software life-cycle processes.....	19
5 Dependability activities in the primary software processes	21
5.1 Acquisition process.....	21
5.2 Supply process	29
5.3 Development process	33
5.4 Operation process	45
5.5 Maintenance process	51
6 Dependability activities in the supporting software processes	57
7 Dependability activities in the organizational software life-cycle processes	57
Annex A (informative) Association of software life-cycle processes with dependability programme elements and tasks.....	63
Annex B (informative) Interaction of users with primary software life-cycle processes	65
Bibliography	67

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SÛRETÉ DE FONCTIONNEMENT DES LOGICIELS PENDANT LEURS PROCESSUS DE CYCLE DE VIE – GUIDE D'APPLICATION

AVANT-PROPOS

- 1) La CEI (Commission Électrotechnique 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, spécifications techniques, 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 61713 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
56/685/FDIS	56/690/RVD

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2003. A cette date, la publication sera

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SOFTWARE DEPENDABILITY THROUGH
THE SOFTWARE LIFE-CYCLE PROCESSES –
APPLICATION GUIDE**

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 specifications, 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 61713 has been prepared by IEC technical committee 56: Dependability

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

FDIS	Report on voting
56/685/FDIS	56/690/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A and B are for information only.

The committee has decided that the contents of this publication will remain unchanged until 2003. At this date, the publication will be

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

INTRODUCTION

Le terme «sûreté de fonctionnement» est un terme générique utilisé pour décrire la disponibilité et les facteurs qui l'influencent: fiabilité, maintenabilité et logistique de maintenance. La CEI 60300-2 fournit un guide concernant les éléments et tâches à inclure dans un programme de sûreté de fonctionnement complet. Un guide plus détaillé concernant les aspects logiciels d'un programme de sûreté de fonctionnement est donné par la CEI 60300-3-6. La présente Norme internationale est destinée à compléter la CEI 60300-3-6 en fournissant un guide pour la sûreté de fonctionnement des logiciels dans le cadre du processus du cycle de vie des logiciels, qui est à la base de nombreuses normes sur les logiciels. Le présent guide identifie les activités liées aux processus du cycle de vie des logiciels qui aideront à obtenir des logiciels sûrs (c'est-à-dire des logiciels qui fonctionnent de manière fiable conformément aux exigences). Une description complète des processus du cycle de vie des logiciels et du cadre qu'ils fournissent pour représenter le cycle de vie du logiciel de l'acquisition à la maintenance est donnée par l'ISO/CEI 12207.

Les activités logicielles sont liées aux différents processus du cycle de vie des logiciels. Un processus du cycle de vie d'un logiciel est un ensemble d'activités planifiées comprenant des exigences exécutées pour atteindre l'objectif indiqué d'un projet logiciel. Le présent guide facilitera l'identification et la mise en œuvre des activités du cycle de vie qui influent sur la sûreté de fonctionnement des logiciels.

INTRODUCTION

Dependability is the collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. IEC 60300-2 provides guidance on the elements and tasks to be included in a comprehensive dependability programme. More detailed guidance on the software aspects of a dependability programme is contained in IEC 60300-3-6. This International Standard is intended to support IEC 60300-3-6 by providing guidance on the achievement of software dependability in the context of software life-cycle processes which form the basis for many software standards. This guide identifies software life-cycle process activities that will help achieve dependable software (i.e. software that reliably performs according to requirements). A full description of the software life-cycle processes and the framework they provide to represent the software life cycle from software acquisition through to software maintenance is provided in ISO/IEC 12207.

The software activities are related to the various software life-cycle processes. A software life cycle process is a set of planned activities, including requirement specifications, performed to achieve the stated objective of a software project. This guide will facilitate the identification and implementation of those life-cycle activities that have a bearing on software dependability.

SÛRETÉ DE FONCTIONNEMENT DES LOGICIELS PENDANT LEURS PROCESSUS DE CYCLE DE VIE – GUIDE D'APPLICATION

1 Domaine d'application

La présente Norme internationale constitue un guide pour les aspects des activités liées au cycle de vie des logiciels qui influent pour obtenir des logiciels fiables. Les activités liées au cycle de vie des logiciels sont définies dans le contexte des processus du cycle de vie des logiciels. Le présent guide est destiné à être utilisé en complément de la CEI 60300-3-6.

Les activités identifiées liées au cycle de vie des logiciels peuvent faire partie d'un programme de sûreté de fonctionnement pour un système ou être en relation avec un produit contenant un logiciel. Les activités identifiées aideront à obtenir un logiciel fiable et dont on peut assurer la maintenance, et contribueront à assurer une logistique de maintenance appropriée. Ces activités peuvent être applicables pendant l'ensemble du cycle de vie du logiciel ou être limitées à un sous-ensemble des processus du cycle de vie du logiciel selon les utilisateurs du logiciel. La relation entre les utilisateurs du logiciel et les processus du cycle de vie du logiciel est donnée à l'annexe B. On a effectué un regroupement en fonction des processus du cycle de vie de logiciels particuliers. Ce regroupement représente l'ensemble du cycle de vie du logiciel comme défini dans l'ISO/CEI 12207.

L'accent est mis surtout sur les exigences de sûreté de fonctionnement et les activités applicables dans le processus de base du cycle de vie du logiciel.

Le présent guide peut être utilisé par les acquéreurs, les fournisseurs, les développeurs, les chargés de l'exploitation ou les personnes chargées de la maintenance des logiciels. En plus des spécialistes des logiciels et de la sûreté de fonctionnement, le présent guide s'adresse aux chefs de projet, aux professionnels de la qualité et aux autres personnes intervenant dans les projets qui développent ou utilisent des systèmes ou produits contenant des logiciels.

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. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60050(191), *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

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

CEI 60300-3-6:1997, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 6: Aspects logiciels de la sûreté de fonctionnement*

CEI 61160, *Revue de conception formalisée*

ISO/CEI 12207, *Technologies de l'information – Processus du cycle de vie des logiciels* (publiée en anglais seulement)

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

SOFTWARE DEPENDABILITY THROUGH THE SOFTWARE LIFE-CYCLE PROCESSES – APPLICATION GUIDE

1 Scope

This International Standard provides guidance on those aspects of software life-cycle activities that have a bearing on the achievement of dependable software. The software life-cycle activities are defined in the context of software life-cycle processes. This guide is intended to be used to support IEC 60300-3-6.

The software life-cycle activities identified can be part of a dependability programme for a system or in relation to a product containing software. The activities identified will help achieve software that is reliable and maintainable and help ensure that appropriate maintenance support will be provided. The activities can be applicable throughout the entire software life cycle or be limited to a subset of the software life-cycle processes depending upon the users of the software. The relationship between the users of the software and the software life-cycle processes is shown in annex B. They are grouped according to the various individual software life-cycle processes that represent the overall software life-cycle as defined in ISO/IEC 12207.

Emphasis is placed on the dependability requirements and activities applicable in the primary software life-cycle processes.

This guide can be used by acquirers, suppliers, developers, operators or maintainers of software. In addition to software and dependability specialists, this guide is intended for use by project managers, quality practitioners and other project participants who develop or use systems or products containing software.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60050(191), *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

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

IEC 60300-3-6:1997, *Dependability management – Part 3: Application guide – Section 6: Software aspects of dependability*

IEC 61160, *Formal design review*

ISO/IEC 12207, *Information technology – Software life cycle processes*

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