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

Numéro de référence
Reference number
CEI/IEC 61713:2000

Numéros des publications

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

Publications consolidées

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

Validité de la présente publication

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

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

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

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

Terminologie, symboles graphiques et littéraux

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

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

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

Numbering

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

Consolidated publications

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

Validity of this publication

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

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

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

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

Terminology, graphical and letter symbols

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

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

* See web site address on title page.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
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

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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE V

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

SOMMAIRE

Pages

CONTENTS

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*

3 Définitions

Pour les besoins de la présente Norme internationale, les termes et les définitions donnés dans la CEI 60050(191), l'ISO/CEI 12207 et l'ISO 8402 s'appliquent, ainsi que les suivants.

3.1
sûreté de fonctionnement
ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance [VEI 191-02-03]

NOTE La sûreté de fonctionnement du logiciel sera décrite en termes de fiabilité, maintenabilité et logistique de maintenance du logiciel.

3.2
fonction de sûreté de fonctionnement
terme utilisé pour décrire un aspect individuel de la prescription de sûreté de fonctionnement du logiciel. La fonction de sûreté de fonctionnement peut décrire la fiabilité, la maintenabilité ou la logistique de maintenance liées aux exigences de sûreté de fonctionnement

3.3
version de maintenance
version de produit qui est effectuée plutôt dans le cadre d'une maintenance corrective que pour fournir une fonctionnalité améliorée

3.4
fiabilité du logiciel
probabilité selon laquelle aucune panne d'un élément logiciel d'un système n'interviendra dans un intervalle de temps donné pendant le fonctionnement du système dans des conditions données

3.5
maintenabilité du logiciel
facilité avec laquelle une panne détectée dans un élément logiciel d'un système peut être corrigée

3.6
logistique de maintenance du logiciel
aptitude d'une organisation de maintenance à fournir sur demande, dans des conditions données, les moyens nécessaires à la maintenance d'un élément logiciel d'un système, conformément à une politique de maintenance donnée

NOTE Les conditions données portent sur l'élément logiciel du système lui-même, ainsi que sur les conditions dans lesquelles cet élément est utilisé et dans lesquelles on assure sa maintenance.

[VEI 191-02-08, modifié]

Pour faciliter la compréhension de la présente norme, les définitions suivantes des termes utilisés dans l'ISO/CEI 12207 sont répétées.

3.7
acquéreur
organisme qui acquiert ou se procure un système, un logiciel ou une prestation logicielle auprès d'un fournisseur

NOTE L'acquéreur peut être acheteur, client, propriétaire, utilisateur, consommateur.

3.8
acquisition
processus consistant à acquérir un système, un logiciel ou une prestation logicielle

3 Definitions

For the purpose of this International Standard, the terms and definitions of IEC 60050(191), ISO/IEC 12207 and ISO 8402 apply together with the following.

3.1
dependability
collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. [IEV 191-02-03]

NOTE Software dependability will be described in terms of software reliability, software maintainability and software maintenance support.

3.2
dependability function
term used to describe an individual aspect of the software dependability requirement specification. The dependability function can describe reliability, maintainability or maintenance support-related dependability requirements

3.3
maintenance release
product release which is carried out for corrective maintenance rather than to provide enhanced functionality

3.4
software reliability
probability that no fault in any software element of a system will be activated in a given time interval in the operation of the system under given conditions

3.5
software maintainability
ease with which a detected fault in a software element of a system can be corrected

3.6
software maintenance support
ability of an organization, under given conditions, to provide upon demand the resources required to maintain a software element of a system, under a given maintenance policy

NOTE The given conditions are related to the software element itself and to the conditions under which it is used and maintained.

[IEV 191-02-08, modified]

To assist understanding of this standard, the following definitions of terms used in ISO/IEC 12207 are repeated here.

3.7
acquirer
organization that acquires or procures a system, software product or software service from a supplier

NOTE The acquirer could be one of the following: buyer, customer, owner, user, purchaser.

3.8
acquisition
process of obtaining a system, software product or software service

3.9
accord
définition des termes et conditions qui établissent une relation de travail

3.10
audit
activité menée par une personne autorisée en vue de fournir une évaluation indépendante de logiciels et de processus afin d'en déterminer la conformité aux exigences

3.11
référentiel de configuration
version formellement approuvée d'un élément de configuration, quel que soit le support, formellement attribuée et attachée à un instant spécifique du cycle de vie de l'élément de configuration

3.12
élément de configuration
entité au sein d'une configuration satisfaisant une fonction pour un utilisateur et pouvant être identifiée d'une manière unique à un instant spécifique du cycle de vie

3.13
contrat
accord engageant deux parties, particulièrement conforme à la législation en vigueur, ou résultant d'une convention interne concernant l'ensemble d'une organisation, pour la fourniture d'une prestation logicielle ou la fourniture, le développement, la production, l'exploitation ou la maintenance d'un logiciel

3.14
développeur
organisme qui réalise les activités de développement (incluant l'analyse des besoins, la conception, les essais d'acceptation) au cours du cycle de vie du logiciel

3.15
évaluation
détermination systématique de la façon dont une entité respecte ses critères spécifiés

3.16
micrologiciel
combinaison de dispositif câblé et d'instructions machine ou de données informatisées qui résident en tant que logiciel non réenregistrable sur le dispositif câble. Ce type de logiciel ne peut pas être modifié aisément par programme

3.17
modèle de cycle de vie
scénario contenant les processus, les activités, et les tâches mis en œuvre pour le développement, l'exploitation et la maintenance d'un logiciel, englobant la totalité de la vie du système depuis l'expression de besoins jusqu'à la fin de son exploitation

3.18
chargé de la maintenance
organisme qui assure les activités de maintenance

3.19
suivi d'avancement
examen par un acquéreur ou par une tierce partie de l'état des activités d'un fournisseur et de ses résultats

3.9
agreement
definition of terms and conditions under which a working relationship will be conducted

3.10
audit
conducted by an authorized person for the purpose of providing an independent assessment of software products and processes in order to assess compliance with requirements

3.11
baseline
formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle

3.12
configuration item
entity within a configuration that satisfies an end-use function and that can be uniquely identified at a given reference point

3.13
contract
binding agreement between two parties, especially enforceable by law, or a similar internal agreement wholly within an organization, for the supply of software service or for the supply, development, production, operation, or maintenance of a software product

3.14
developer
organization that performs development activities (including requirements analysis, design, testing through acceptance) during the software life-cycle process

3.15
evaluation
systematic determination of the extent to which an entity meets its specified criteria

3.16
firmware
combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control

3.17
life-cycle model
framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use

3.18
maintainer
organization that performs maintenance activities

3.19
monitoring
examination of the status of the activities of a supplier and of their results by the acquirer or a third party

3.20
élément non livrable
matériel ou logiciel dont la livraison n'est pas exigée par le contrat mais qui peut être utilisé dans le développement du logiciel

3.21
progiciel
produit déjà développé et disponible, utilisable soit «tel quel», soit après modification

3.22
chargé de l'exploitation
organisme qui exploite le système

3.23
processus
ensemble d'activités ordonnées dans le temps et liées qui transforment des éléments entrants en éléments sortants

NOTE Le terme «activités» recouvre l'utilisation de moyens.

3.24
qualification
processus démontrant qu'une entité est capable de répondre aux exigences spécifiées

3.25
exigence de qualification
ensemble de critères ou de conditions qui doivent être satisfaits pour que le logiciel soit qualifié comme répondant aux spécifications qui lui sont applicables et prêt à l'utilisation dans son environnement cible

3.26
essais de qualification
essais effectués par le développeur et dont l'acquéreur est témoin (le cas échéant), pour démontrer que le logiciel répond à ses spécifications et qu'il est prêt à l'utilisation dans son environnement cible

3.27
assurance de la qualité
ensemble des activités préétablies et systématiques mises en œuvre dans le cadre du système qualité et démontrées en tant que de besoin, pour donner la confiance appropriée en ce qu'une entité satisfera aux exigences pour la qualité

NOTE 1 L'assurance de la qualité vise à la fois des objectifs internes et externes:

a) assurance de la qualité interne: au sein d'un organisme, l'assurance de la qualité sert à donner confiance à la direction;

b) assurance de la qualité externe: dans des situations contractuelles, l'assurance de la qualité sert à donner confiance aux clients ou à d'autres.

NOTE 2 Certaines actions de maîtrise de la qualité et d'assurance de la qualité sont liées entre elles.

NOTE 3 Si les exigences pour la qualité ne reflètent pas entièrement les besoins de l'utilisateur, l'assurance de la qualité peut ne pas donner la confiance souhaitée.

3.28
version disponible
version particulière d'un élément de configuration rendue disponible dans un but spécifique (par exemple version d'essai)

3.20
non-deliverable item
hardware or software product that is not required to be delivered under the contract but may be employed in the development of a software product

3.21
off-the-shelf product
product that is already developed and available, usable either "as is" or with modification

3.22
operator
organization that operates the system

3.23
process
set of timely ordered and interrelated activities, which transform inputs into outputs

NOTE The term "activities" covers use of resources.

3.24
qualification
process of demonstrating whether an entity is capable of fulfilling specified requirements

3.25
qualification requirement
set of criteria or conditions that have to be met in order to qualify a software product as complying with its specifications and being ready for use in its target environment

3.26
qualification testing
testing, conducted by the developer and witnessed by the acquirer (as appropriate), to demonstrate that a software product meets its specifications and is ready for use in its target environment

3.27
quality assurance
all the planned and systematic activities implemented within the quality system, and demonstrated as needed, to provide adequate confidence that an entity will fulfil requirements for quality

NOTE 1 There are both internal and external purposes for quality assurance:

a) internal quality assurance: within an organization, quality assurance provides confidence to management;

b) external quality assurance: in contractual situations, quality assurance provides confidence to the customer or others.

NOTE 2 Some quality control and quality assurance actions are interrelated.

NOTE 3 Unless requirements for quality fully reflect the needs of the user, quality assurance may not provide adequate confidence.

3.28
release
particular version of a configuration item that is made available for a specific purpose (for example, test release)

3.29
appel d'offres
document utilisé par l'acquéreur pour annoncer à des soumissionnaires potentiels son intention d'acquérir un système, un logiciel ou une prestation logicielle spécifiques

3.30
retrait
abandon du support actif de l'organisme chargé de l'exploitation et de la maintenance, remplacement partiel ou total remplacement par un nouveau système, ou installation d'un système plus performant

3.31
confidentialité
protection des informations et des données afin qu'elles ne puissent pas être lues ou modifiées par des personnes ou des systèmes non autorisés alors que l'accès n'est pas refusé aux personnes ou systèmes habilités

3.32
logiciel
ensemble des programmes, des procédures et de la documentation et des données éventuellement associées

3.33
prestation logicielle
exécution d'activités, de travaux ou de tâches liés à un logiciel tels que le développement, la maintenance et l'exploitation

3.34
unité de logiciel
partie de code qui peut être compilée séparément

3.35
énoncé des travaux
document utilisé par l'acquéreur pour décrire ou spécifier les tâches à exécuter dans le cadre du contrat

3.36
fournisseur
organisme qui s'engage sous contrat avec l'acquéreur à fournir un système, un logiciel ou une prestation logicielle selon les modalités du contrat

NOTE 1 Le terme «fournisseur» est synonyme de contractant, producteur ou vendeur.

NOTE 2 L'acquéreur peut désigner une partie de son organisme en tant que fournisseur.

3.37
système
ensemble intégré qui comprend un ou plusieurs des éléments suivants: processus, matériel, logiciel, installations et personnes et qui permet de satisfaire un besoin ou un objectif établi

3.38
couverture d'essai
degré de couverture des exigences du système ou du logiciel par les cas d'essai

3.39
aptitude aux essais
mesure dans laquelle un essai réalisable et objectif peut être conçu pour déterminer si une exigence est ou non remplie

3.29
request for proposal
tender
document used by the acquirer as the means to announce its intention to potential bidders to acquire a specified system, software product or software service

3.30
retirement
withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system

3.31
security
protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them

3.32
software product
set of computer programs, procedures, and possibly associated documentation and data

3.33
software service
performance of activities, work, or duties connected with a software product, such as its development, maintenance and operation

3.34
software unit
separately compilable piece of code

3.35
statement of work
document used by the acquirer as the means to describe and specify the tasks to be performed under the contract

3.36
supplier
organization that enters into a contract with the acquirer for the supply of a system, software product or software service under the terms of the contract

NOTE 1 The term "supplier" is synonymous with contractor, producer, seller or vendor.

NOTE 2 The acquirer may designate a part of its organization as supplier.

3.37
system
integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective

3.38
test coverage
extent to which the test cases test the requirements for the system or software product

3.39
testability
extent to which an objective and feasible test can be designed to determine whether a requirement is met

3.40
utilisateur
individu ou organisme utilisant le système opérationnel pour exécuter une fonction spécifique

NOTE L'utilisateur peut tenir d'autres rôles comme ceux d'acquéreur, de développeur ou de chargé de la maintenance.

3.41
validation
confirmation par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique sont satisfaites

NOTE 1 En conception et développement, la validation concerne le processus d'examen d'un produit en vue de déterminer la conformité aux besoins de l'utilisateur.

NOTE 2 La validation s'effectue normalement sur le produit final dans des conditions d'utilisation définies. Elle peut s'avérer nécessaire à des étapes antérieures.

NOTE 3 Le terme «validé» désigne le statut correspondant.

NOTE 4 Plusieurs validations peuvent être effectuées s'il y a différents usages prévus.

3.42
vérification
confirmation par examen et apport de preuves tangibles que les exigences spécifiées ont été satisfaites

NOTE 1 En conception et développement, la vérification concerne le processus d'examen de résultat d'une activité en vue de déterminer la conformité aux exigences requises pour ladite activité.

NOTE 2 Le terme «vérifié» désigne l'état correspondant.

3.43
version
état identifié d'un élément

NOTE La modification apportée à une version de logiciel, ayant pour résultat une nouvelle version, nécessite des actions de gestion de configuration.

4 Processus du cycle de vie d'un logiciel

Le processus du cycle de vie d'un logiciel est un ensemble d'activités ou de tâches planifiées nécessaires pour atteindre l'objectif déclaré d'un projet logiciel. Il existe trois groupes de processus: processus de base, de support et organisationnels, correspondant à des activités concernant un logiciel de sa conception à son retrait.

Les cinq processus de base fournissent un guide aux acquéreurs, aux fournisseurs, aux développeurs, aux chargés de l'exploitation et aux chargés de la maintenance des systèmes ou produits contenant des logiciels.

Les huit processus du cycle de vie de soutien viennent en support à un autre processus et peuvent être utilisés avec les cinq processus de base. Ces processus de soutien incluent la documentation, la gestion de la configuration, l'assurance de la qualité, la vérification, la validation, la revue conjointe, l'audit et la résolution des problèmes.

Les quatre processus organisationnels peuvent être utilisés par les parties les plus importantes ou les processus de base, en fonction des besoins organisationnels ou des projets. Les processus organisationnels sont la gestion, l'infrastructure, l'amélioration et la formation. Des précisions concernant les processus du cycle de vie d'un logiciel et leur utilisation sont données dans l'ISO/CEI 12207.

Les relations entre les processus du cycle de vie d'un logiciel et les éléments et tâches du programme de sûreté de fonctionnement décrits dans la CEI 60300-2, dans la mesure où ils concernent des produits contenant des logiciels, sont décrites dans la CEI 60300-2. Des renvois à des paragraphes spécifiques de la CEI 60300-2 sont indiqués à l'annexe A.

3.40
user
individual or organization that uses the operational system to perform a specific function

NOTE The user may perform other roles, such as acquirer, developer, or maintainer.

3.41
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

NOTE 1 In design and development, validation concerns the process of examining a product to determine conformity with user needs.

NOTE 2 Validation is normally performed on the final product under defined operating conditions. It may be necessary in earlier stages.

NOTE 3 "Validated" is used to designate the corresponding status.

NOTE 4 Multiple validations may be carried out if there are different intended uses.

3.42
verification
confirmation by examination and provision of objective evidence that specified requirements have been fulfilled

NOTE 1 In design and development, verification concerns the process of examining the result of a given activity to determine conformity with the stated requirements for that activity.

NOTE 2 "Verified" is used to designate the corresponding status.

3.43
version
identified instance of an item

NOTE Modification to a version of a software product, resulting in a new version, requires configuration management action.

4 Software life-cycle processes

A software life-cycle process is a set of planned activities or tasks necessary to achieve a stated objective of a software project. There are three groups of processes: primary, supporting and organizational, involving activities relating to a software product from its conception to its retirement.

The five primary processes provide guidance to acquirers, suppliers, developers, operators and maintainers of systems or products containing software.

The eight supporting life-cycle processes support another process and can be used with the five primary processes. The supporting processes are documentation, configuration management, quality assurance, verification, validation, joint review, audit and problem resolution.

The four organizational processes can be used by the major parties or primary processes depending upon the organizational or project needs. The organizational processes are management, infrastructure, improvement and training. Details of the software life-cycle processes and their use are given in ISO/IEC 12207.

The relationships of the software life-cycle processes with the dependability programme elements and tasks described in IEC 60300-2, as they relate to products containing software, is described in IEC 60300-2. Cross-references are made to specific subclauses of IEC 60300-2 in annex A.

5 Activités de sûreté de fonctionnement dans les processus de base

Pour obtenir des logiciels fiables, il est nécessaire d'identifier et de mettre en œuvre les activités et les tâches qui influencent tout particulièrement la sûreté de fonctionnement. Il est recommandé que ces activités prennent en compte l'utilisation prévue, l'application, l'exploitation et l'environnement du système ou du produit contenant le logiciel. Il est recommandé d'accorder l'attention nécessaire aux activités nécessaires dans chacun des cinq processus de base du cycle de vie; elles sont décrites aux paragraphes 5.1 à 5.5.

5.1 Processus d'acquisition

«Processus d'acquisition» est le terme utilisé pour décrire les activités et les tâches d'un acquéreur qui se procure un système ou un produit contenant un logiciel. En ce qui concerne la sûreté de fonctionnement, les performances de fiabilité, de maintenabilité du logiciel et de logistique de maintenance du fournisseur sont les principaux aspects à prendre en considération. Les éléments principaux du processus d'acquisition sont la spécification des exigences de sûreté de fonctionnement, l'évaluation et la sélection d'un fournisseur, la préparation des documents contractuels, l'audit, la surveillance du fournisseur, la réception et le contrôle. Ces éléments sont décrits dans les paragraphes 5.1.1 à 5.1.5.

5.1.1 Spécification des exigences de sûreté de fonctionnement

Il est recommandé que la spécification des exigences établies par l'acquéreur s'exprime selon les facteurs qui influencent la sûreté de fonctionnement du logiciel, c'est-à-dire que les exigences de sûreté de fonctionnement puissent être spécifiées en termes d'exigences de fiabilité, de maintenabilité et de logistique de maintenance. Il est donc recommandé que les exigences suivantes soient spécifiées par l'acquéreur ou conjointement avec le fournisseur:

a) Exigences de fiabilité logicielle

Exigences pour l'exploitation en continu du système: il est recommandé qu'elles soient clairement spécifiées en termes de temps écoulé par intervalle de temps, de nombre d'exploitations sans panne avant l'apparition d'une défaillance.

Disponibilité opérationnelle du système requise, c'est-à-dire proportion de temps d'exploitation pendant lequel le système est disponible pour assurer ses fonctions; il est recommandé que celle-ci soit exprimée en termes reconnaissables tels que «moyenne des temps pour la tâche de réparation» (mean time to repair MTTR) et «temps moyen entre défaillances» (mean time between failures MTBF); il est recommandé de définir également les conditions qui constituent une défaillance du système.

Tout facteur d'environnement qui impose une fiabilité spéciale, des exigences pour l'application de système prévue.

Conditions de reprise du système, c'est-à-dire temps de rétablissement ou conditions opérationnelles qu'il convient de remplir lorsqu'on redémarre un système après une défaillance.

Exigences de sécurité intrinsèque définies en tant que données qu'il convient de ne pas perdre ou états de sécurité qu'il est nécessaire d'atteindre ou exploitation dégradée en cas de défaillance système.

Il est recommandé d'identifier toute exigence pour évaluation, estimation ou certification par un organisme tiers. Il est recommandé de prendre en considération l'impact de telles exigences sur les exigences de conception du logiciel.

S'il existe un niveau minimal de service à assurer et des circonstances (durée, fréquence, etc.) dans lesquelles un retour à ce minimum serait acceptable, alors il est recommandé de les identifier et de les spécifier.

Il existe rarement des exigences de sûreté de fonctionnement égales pour tous les aspects d'un système; il est recommandé d'encourager les acquéreurs à identifier exactement quelles exigences s'appliquent à quelles parties d'un système.

5 Dependability activities in the primary software processes

In order to achieve dependable software, it is necessary to identify and implement those activities and tasks that particularly influence dependability. These activities should take account of the intended use, application, operation and environment of the system or product containing software. Consideration should be given, as appropriate, to activities necessary in each of the five primary life-cycle processes; these are described in 5.1 to 5.5.

5.1 Acquisition process

The acquisition process is the term used to describe the activities and tasks of an acquirer involved in acquiring a system or product containing software. From the dependability viewpoint, the software product reliability performance and maintainability performance and the supplier maintenance support performance are the main aspects to be considered. The acquisition process main elements are the specification of dependability requirements, the assessment and selection of a supplier, the preparation of contractual documents, supplier monitoring and acceptance and control. These elements are described in 5.1.1 to 5.1.5.

5.1.1 Specification of dependability requirements

The requirements specification prepared by the acquirer should be expressed in those factors that influence dependability of the software product, i.e. the dependability requirements can be specified in terms of reliability, maintainability and maintenance support requirements. The following requirements should therefore be specified by the acquirer or jointly with the supplier:

a) Software reliability requirements

Requirements for continuous system operation; these should be clearly specified in terms of elapsed time per given time interval, number of operations where no fault occurs before a failure occurs.

The required system operational availability performance i.e. the proportion of operational time when the system is available to perform its functions; this should be expressed in recognizable terms such as mean time to repair (MTTR) and mean time between failures (MTBF); the conditions that constitute failure of the system should also be defined.

Any environmental factors that impose special reliability, requirements for the intended system application.

The recovery conditions of the system, i.e. any time to restore or functional conditions that should be met when restarting a system following a system failure.

Defined fail-safe requirements such as data that should not be lost or safe function states that need to be attained or downgraded operation in the event of a system failure.

Any requirements for third-party evaluation, assessment or certification should be identified. The impact of such requirements on the software design requirements should be considered.

If there is a minimum level of service to be provided and the circumstances (length of time, frequency, etc.) under which reversion to that minimum would be acceptable, these should be identified and specified.

Equal dependability requirements rarely exist for all aspects of a system; acquirers should be encouraged to identify exactly what requirements apply to which parts of a system.

Il est recommandé que l'acquéreur détermine quels coûts, ressources supplémentaires, etc., découleront soit comme résultat direct de ses exigences, soit comme résultat d'une solution particulière apportée.

b) Exigences de maintenabilité logicielle

Tout facteur d'environnement qui impose des exigences de maintenabilité spéciales pour l'application de système prévue. De plus, il est recommandé de fixer le niveau de qualification et les exigences relatives à la formation pour la maintenabilité. Il convient d'exprimer les exigences de maintenabilité en des termes reconnaissables tels que «moyenne des temps pour la tâche de réparation» (MTTR).

c) Exigences de logistique de maintenance logicielle

Tout facteur d'environnement qui impose des exigences de logistique de maintenance spéciales pour l'application de système prévue. De plus, il est recommandé de fixer le niveau de qualification et les exigences relatives à la formation pour la maintenance. Il convient d'exprimer les exigences de maintenance en termes reconnaissables tels que «moyenne des temps pour la tâche de réparation» (MTTR) ou «retard logistique moyen» (mean logistic delay time MLDT).

5.1.2 Sélection du fournisseur

L'aptitude du fournisseur à développer ou fournir un logiciel fiable et à offrir un service de logistique efficace pendant la durée de vie du produit constitue une exigence de base. Si le fournisseur a déjà acquis ou développé des logiciels, alors les produits existants ou les services logistiques associés pourraient être utilement pris en compte lors de la sélection du fournisseur. Si le fournisseur est considéré comme un développeur potentiel de logiciel, il est recommandé d'estimer ses activités de processus de développement conformément aux directives de 5.3 pour développer des logiciels fiables. Lors de la sélection d'un fournisseur, il convient également de prendre en compte la compréhension du fournisseur en ce qui concerne: (1) les exigences techniques – les exigences relatives au logiciel découlant des exigences du système, (2) les exigences contractuelles – les accords, conditions, et termes qui affectent la partie logiciel de l'acquisition. Il convient que les autres critères de sélection du fournisseur comprennent les performances antérieures relatives (1) au développement de logiciels, (2) à la gestion de projets logiciels (y compris assurance de la qualité (AQ), gestion de la configuration (CM), essais de fiabilité et maintenance du logiciel, etc.), (3) au transfert du logiciel au support (utilisateur), (4) à l'évaluation des risques logiciel et la planification de leur réduction, et (5) à la confidentialité des logiciels. Lors de l'évaluation et de la sélection d'un fournisseur, il est recommandé de prendre en compte les aspects suivants:

a) Logiciel existant

Si les données sont disponibles, il est recommandé d'estimer la sûreté de fonctionnement des produits fournis antérieurement par le fournisseur, s'il s'agit d'un développeur de logiciels, c'est-à-dire les performances de fiabilité, de maintenabilité des produits et les performances de logistique de maintenance du fournisseur. Il est recommandé que le référentiel de configuration pour la mesure de ces performances soit constitué de mesures de disponibilité reconnaissables comme le MTTR pour la logistique de maintenance ou le MTBF pour la fiabilité. En l'absence de données concernant la sûreté de fonctionnement des produits fournis antérieurement, l'acquéreur pourrait avoir recours à une méthode indirecte d'estimation de la sûreté de fonctionnement du produit en estimant les processus de développement utilisés par le fournisseur pour créer ses logiciels. Cette approche est étudiée en 5.1.2b). Il convient d'évaluer la sûreté de fonctionnement du logiciel alors que le produit est installé dans son propre environnement système.

Il est recommandé de comparer la sûreté de fonctionnement d'un produit donné avec celle des produits concurrents. L'aptitude du fournisseur à fournir des logiciels au point a souvent des conséquences sur cet aspect du produit. Il est recommandé d'effectuer la comparaison avec des mesures similaires et, si possible, considérées dans des conditions similaires.

The acquirer should determine what additional costs, resources, etc., will arise either as a direct result of his requirements or as a result of any particular solution to it.

b) Software maintainability requirements

Any environmental factors that impose special maintainability requirements for the intended system application. In addition, the skill level and training level for maintainability should be stated. The maintainability requirements should be expressed in recognizable terms such as mean time to repair (MTTR).

c) Software maintenance support requirements

Any environmental factors that impose special maintenance support requirements for the intended system application. In addition, the skill level and training requirements for maintenance support should be stated. The maintenance support requirements should be expressed in recognizable terms such as mean time to repair (MTTR) or mean logistic delay time (MLDT).

5.1.2 Selection of supplier

The ability of the supplier to develop or supply dependable software and to provide an effective support service during the lifetime of the product is a prime requirement. If the supplier has already acquired or developed software products then the existing products or support services associated with them could be usefully considered when selecting a supplier. If the supplier is being considered as a potential software developer, his development process activities should be assessed according to the guidelines given in 5.3 for developing dependable software products. The selection of supplier should also include the supplier understanding of: (1) technical requirements – software requirements flow-down from system requirement, (2) contractual requirements – agreements, conditions, and terms which affect the software portion of the acquisition. Other supplier selection criteria should also include the past performances on (1) software development, (2) software project management (including software QA, configuration management CM, reliability testing, and maintenance, etc.), (3) software transition to (user) support, (4) software risk assessment and mitigation planning, and (5) software security. When assessing and selecting a supplier, consideration should be given to the following aspects:

a) Existing software product

If data is available, the dependability of products previously provided by the supplier should be assessed if he is a software developer, i.e. the reliability performance, maintainability performance of the products and maintenance support performance of the supplier. The measurement baseline for these performance characteristics should be recognizable availability measures such as MTTR for measuring maintenance support performance or MTBF for measuring reliability performance. If data on the dependability of previously supplied products is not available, the acquirer could consider an indirect method of assessing product dependability by assessing the development processes used by the supplier to produce software products. This approach is discussed in 5.1.2b). The dependability of the software product should be assessed whilst the product is in its defined system environment.

The dependability of the product under consideration should be compared with those of competing products. The ability of the supplier to provide mature software products often has a bearing on this aspect of the product. The comparison should be made using similar measures, if possible considered under similar conditions.

Si le fournisseur est un développeur de logiciel, il est alors recommandé d'estimer sa structure organisationnelle de sa logistique de maintenance et ses procédures de soutien pour le produit conformément aux directives de sûreté de fonctionnement du processus de maintenance en 5.5.

Si le fournisseur est un développeur de logiciel, alors effectue-t-il des essais de croissance de fiabilité pour améliorer la sûreté de fonctionnement de ses produits par identification, analyse et correction des pannes et la vérification de l'efficacité des actions correctives? Des informations complémentaires concernant les méthodologies pour les essais de croissance de fiabilité telles que les modèles de croissance de la fiabilité sont données en 6.8.4 de la CEI 60300-3-6. Il est recommandé de revoir tout programme de croissance de la fiabilité mis en place par le fournisseur pour comparer l'état actuel avec les objectifs de sûreté de fonctionnement recherchés.

b) Nouveau logiciel

Si le fournisseur est un développeur de logiciel, il est alors recommandé que les méthodes qu'il utilisera pour mesurer la sûreté de fonctionnement comme défini dans les exigences fassent l'objet d'une estimation quant à leur cohérence et à leur exhaustivité.

Si le logiciel doit être développé, il est recommandé que les processus de développement et de mise en place du logiciel par le fournisseur soient revus en conformité avec les recommandations de sûreté de fonctionnement du processus de développement (voir 5.3). Ces recommandations donnent des conseils concernant les approches pour l'estimation des méthodes et procédures des développeurs et pour l'analyse, la spécification, la conception, le codage, les essais et l'installation de logiciels fiables.

c) Maturité du processus logiciel

Si le développeur de logiciel obtient des taux de maturité du processus logiciel comparables à ceux du modèle d'aptitude à la maturité (CMM) du Software Engineering Institute, il convient qu'ils puissent être examinés et pris en considération dans les critères d'évaluation. Ce type de modèle fournit des mesures relatives à la qualification d'un développeur de logiciel particulier pour la réalisation de travaux sur les logiciels ou la surveillance de l'état du processus logiciel utilisé lors de l'utilisation d'un logiciel existant.

5.1.3 Préparation des contrats

L'évaluation et la sélection d'un fournisseur (voir 5.2), entraîneront souvent une négociation concernant la logistique et les conditions de fourniture, c'est pourquoi il est essentiel que les documents contractuels incluent des exigences complètes pour la sûreté de fonctionnement, en particulier lorsque le contrat inclut le développement de logiciel. Dans le cas de certains petits fournisseurs, il se pourrait que les documents contractuels ne correspondent pas à un contrat formel mais qu'ils puissent être limités à un appel d'offres ou à une commande. Dans de tels cas, le terme «contrat» est étendu pour couvrir l'appel d'offres ou les commandes. Il est recommandé que les aspects suivants relatifs à la sûreté de fonctionnement soient spécifiés dans le contrat après négociation des termes mutuellement acceptables et lorsqu'ils peuvent être définis de manière explicite:

a) conditions de réception, exigences de fiabilité, exigences de maintenabilité et exigences de logistique de maintenance;

b) indication de disponibilité en termes d'exigences de disponibilité. Si le logiciel doit être fourni comme partie d'un système, alors il est recommandé d'indiquer les exigences de sûreté de fonctionnement pour l'exploitation dans l'environnement du système. S'il existe des normes de sûreté de fonctionnement particulières applicables, il est recommandé qu'elles soient spécifiées;

c) il est recommandé que l'acquéreur définisse les exigences de disponibilité. Ainsi, les exigences originales de disponibilité seront définies. Si le fournisseur ne peut pas ou n'atteint pas les exigences définies, alors celles-ci seront réexaminées avec modification du contrat ou révision de la spécification reflétant les modifications;

If the supplier is a software developer, then his maintenance support organization structure and product support procedures should be assessed in accordance with the maintenance process dependability guidelines in 5.5.

If the supplier is a software developer, then does he perform any kind of reliability growth testing for the purpose of enhancing product dependability through identification, analysis and correction of faults, and the verification of the effectiveness of the corrective action? Further information on methodologies for reliability growth testing such as the use of reliability growth models is given in 6.8.4 of IEC 60300-3-6. Any reliability growth programme implemented by the supplier should be reviewed to compare current achieved status with projected dependability targets.

b) New software product

If the supplier is a software developer, then the methods he will use to measure dependability as defined in the requirement specification should be assessed for consistency and completeness.

If software is to be developed, the supplier's software development and implementation process should be reviewed in accordance with the development process dependability guidelines (see 5.3). These guidelines advise on the approaches for assessing the developer's methods and procedures for analyzing, specifying, designing, coding, testing and installing dependable software.

c) Software process maturity

If the software developer obtains certain software process maturity ratings, such as the Software Engineering Institute's capability maturity model (CMM), it should be made available for review and taken into consideration as part of the evaluation criteria. This type of model provides some measurements of an individual software developer qualification to perform the software work or to monitor the state of the software process used on an existing software effort.

5.1.3 Preparation of contracts

Evaluation and selection of a supplier (see 5.2) will often involve negotiation on support and supply conditions, it is essential therefore that contractual documents should include comprehensive requirements for dependability, particularly where the contract includes the development of software. With some smaller supplier companies, the contractual documents might not be a formal contract but could be limited to a tender or an order document. In these cases, the term "contract" is extended to cover tender or order documents. The following aspects related to dependability should be specified in the contract after negotiation of mutually acceptable terms and where they can be explicitly defined:

a) the conditions for acceptance, reliability requirements, maintainability requirements and maintenance support requirements;

b) a statement of availability in terms of availability requirements. If the software is to be supplied as part of a system, then the dependability requirements, when operating in the system environment, should be stated. If there are particular dependability standards applicable, these should be specified;

c) an acquirer should state the availability requirements. This will ensure the original availability requirements are stated. If the supplier cannot or will not achieve the stated requirements, then these will be re-negotiated with contract modification or specification revision to reflect the changes;

d) le processus de modification d'un produit par un fournisseur nécessite un accord avec l'acquéreur. Il est recommandé que le processus d'enregistrement et de suivi d'avancement des modifications à un logiciel soit un processus de modification formel, de telle sorte que la procédure de gestion de configuration du logiciel qui sera utilisée et qu'un bureau de contrôle des modifications du logiciel (SCCB) puissent être mis en place en accord avec le fournisseur;

e) des exigences de sûreté de fonctionnement spécifiées, bien qu'elles soient rarement absolues, sont nécessaires dans le contrat. Par exemple, une sûreté de fonctionnement amoindrie dans une zone d'un système complet peut être à l'origine de surcoûts dans une autre zone, par exemple fourniture d'une station de supervision, plus de personnel de maintenance, détention accrue d'éléments de rechange etc. Il y a souvent un point de compromis où le coût que représente leur fourniture pour le niveau de sûreté de fonctionnement requis dans un système peut dépasser le coût de compensation de leur absence. Il est recommandé qu'un contrat permette la proposition et l'estimation du coût d'un compromis en définissant les contraintes associées (par exemple en spécifiant un niveau minimal de service à fournir par la partie du système qu'on entend se procurer, ou en indiquant que le personnel de service ne peut être augmenté/réduit, etc.). Il est recommandé d'encourager les acquéreurs à spécifier aussi clairement que possible le problème qu'ils ont besoin de résoudre et toute contrainte s'appliquant à la solution.

   En principe, il est recommandé que l'acquéreur spécifie la disponibilité mais le fournisseur pourrait négocier les termes du contrat en raison de l'incapacité à maîtriser la fiabilité, la maintenabilité ou la logistique de maintenance. Si la disponibilité est exprimée comme une fonction de la fiabilité, de la maintenabilité et de la logistique de maintenance, alors

   Disponibilité (A) = *f* (Fiabilité (R), Maintenabilité (M), Logistique de maintenance (MS))

   Pour certaines applications critiques du système, il est important que la disponibilité (A) et la maintenabilité (M) soient spécifiées avec soin. La disponibilité, par exemple, est l'une des informations les plus critiques pour les applications militaires. Dans le domaine médical, la disponibilité d'un dispositif médical contenant du logiciel est souvent critique en ce qui concerne la vie du patient;

f) exigences et conditions de la logistique de maintenance: si des exigences spécifiques de maintenance ou de disponibilité existent, telles que le temps de réaction ou la fréquence de maintenance sur le système ou le produit contenant un logiciel, il est recommandé de les spécifier. Si des réglements particuliers ou des normes particulières existent, il est recommandé de les spécifier.

5.1.4 Surveillance du fournisseur

La surveillance des revues, l'audit, la vérification et la validation des activités du fournisseur (voir article 6) par l'acquéreur contribuera à la réalisation de la sûreté de fonctionnement du logiciel acquis par la vérification et la validation des fonctions de sûreté de fonctionnement spécifiées. Il convient également que l'acquéreur coopère pleinement avec le fournisseur en lui fournissant toutes les informations nécessaires relatives à la sûreté de fonctionnement de manière appropriée et après avoir résolu tous les problèmes en suspens.

5.1.5 Réception et réalisation

Il convient que l'acquéreur s'assure que les aspects relatifs à la sûreté de fonctionnement définis dans la spécification des exigences sont bien inclus dans la préparation et la réalisation de l'essai de réception. L'acquéreur n'acceptera la livraison du logiciel par le fournisseur que lorsque toutes les conditions de réception relatives à la sûreté de fonctionnement seront remplies.

d) the process for a supplier to make changes to a product needs to be agreed with the acquirer. The process for recording and controlling changes to a software product should be a formal change process such as the software configuration management procedure that will be used and a software change control board (SCCB) to be agreed with the supplier;

e) specified dependability requirements, though rarely absolute, are needed in the contract. For instance, decreased dependability in one area of a total system can cause increased costs in another, for example provision of a hot-standby terminal, more maintenance staff, increased spares holding, etc. There is often a trade-off point where the cost of providing the level of dependability asked for in a system can exceed the cost of compensating for its absence. A contract should allow trade-off to be proposed and costed, and should define the associated constraints (perhaps by specifying a minimum level of service to be provided by the part of the system being procured, or by stating that service personnel cannot be increased/decreased, etc.). Acquirers should be encouraged to specify as explicitly as possible the problem they need to have solved, and any constraints which apply to the solution.

   In principle, the acquirer should specify availability but the supplier might negotiate contract terms due to the inability to control reliability, maintainability and or maintenance support. If availability is expressed as a function of reliability, maintainability and maintenance support,

   Availability (A) = *f* (Reliability (R), Maintainability (M), Maintenance support (MS))

   For some critical system applications, it is important that availability (A) and maintainability (M) are carefully specified. Availability, for instance, is one of the most critical informations needed for the military. In the medical community, availability of a medical device containing software is often critical to a patient's life;

f) the requirements and conditions for maintenance support: if there are specific maintenance or availability requirements such as time to respond or frequency of maintenance on the system or product containing software, these should be specified. If there are particular regulations or standards these should be specified.

5.1.4 Supplier monitoring

Monitoring of the supplier's review, audit, verification and validation activities (see clause 6) by the acquirer will contribute to the achievement of the dependability of the software being acquired through the verification and validation of the specified dependability functions. The acquirer also should co-operate fully with the supplier by providing any necessary dependability-related information in a timely manner and resolving any pending issues.

5.1.5 Acceptance and completion

The acquirer should ensure that the defined dependability aspects of the requirement specification are included in the preparation and conductance of the acceptance test. The acquirer will accept the deliverable software from the supplier when all the defined dependability acceptance conditions are satisfied.

5.2 Processus de fourniture

Le processus de fourniture couvre les activités du fournisseur. Du point de vue de la sûreté de fonctionnement, il est recommandé de prendre en compte les aspects supplémentaires suivants de fiabilité (R), de maintenabilité (M) et de logistique de maintenance (MS) des activités du processus de fourniture. De plus, un programme de croissance de la fiabilité pourrait être nécessaire, par exemple si cela a été négocié pendant la sélection du fournisseur (voir 5.1.2) ou la négociation du contrat.

5.2.1 Initialisation

Il est recommandé que le fournisseur revoie de manière spécifique les exigences de sûreté de fonctionnement de l'acquéreur et identifie les exigences de support de fiabilité, de maintenabilité et de logistique de maintenance en examinant si elles peuvent être remplies par un nouveau produit ou un produit existant.

Il est recommandé que le fournisseur prenne une décision en fonction des résultats de cet examen en ce qui concerne le niveau de logistique nécessaire pour remplir les exigences de fiabilité, de maintenabilité et de logistique de maintenance et les coûts induits avant de décider de faire une offre ou d'accepter le contrat ou de proposer des solutions alternatives appropriées.

5.2.2 Préparation de la réponse

Points concernant la préparation de la réponse par le fournisseur:

a) Il est recommandé que la proposition du fournisseur réponde aux exigences de sûreté de fonctionnement ou aux normes spécifiées par l'acquéreur. Dans le cas contraire, il est recommandé d'identifier les compromis proposés ainsi que les différences entre les exigences du compromis et les exigences initiales (en termes de niveau de service, par exemple) de manière à ce que leur valeur puisse être jugée par l'acquéreur.

b) Si les propositions du fournisseur nécessitent un développement logiciel, il est recommandé qu'il spécifie un programme ou un essai de croissance de la fiabilité.

c) Il est recommandé que la proposition du fournisseur comprenne une réponse technique avec une description des problèmes de fiabilité, de maintenabilité et de logistique de maintenance tels que compris, avec les solutions proposées, et qu'elle indique si les exigences de sûreté de fonctionnement sont complètement remplies.

d) Il est recommandé que la proposition du fournisseur comprenne une réponse de gestion qui inclue une description de l'approche, les étapes du projet et le calendrier.

e) Il est recommandé que la proposition du fournisseur comprenne une réponse financière.

f) Il est recommandé que la proposition du fournisseur comprenne une réponse concernant la formation, décrivant les types de formation offerts et leur interconnexion pour fournir et conserver du personnel formé pour les processus d'acquisition, de fourniture, de développement, d'exploitation et de maintenance.

5.2.3 Contrat

Il est recommandé que le fournisseur établisse un contrat avec l'acquéreur pour fournir le logiciel ou la prestation logicielle. Il est recommandé que les exigences de sûreté de fonctionnement du logiciel ou de la prestation logicielle soient définies comme décrit en 5.1.3.

5.2.4 Planification

Il convient que le fournisseur développe et documente les plans basés sur les exigences relatives à la planification. Il convient de considérer les articles et exemples de plans en se référant aux plans de gestion du projet. Ces articles de planification de gestion du projet sont critiques et ont des conséquences sur la fiabilité, la maintenabilité, et la logistique de maintenance.

5.2 Supply process

The supply process covers the activities of the supplier. From the dependability viewpoint, the following additional reliability (R), maintainability (M) and maintenance support (MS) aspects of the supply process activities should be considered. In addition, a reliability growth programme could be required if, for example, this was negotiated during supplier selection (see 5.1.2) or contract negotiation.

5.2.1 Initiation

The supplier should specifically review the dependability requirements of the acquirer and identify the reliability, maintainability and maintenance support requirements and whether these requirements can be met with a new or existing product.

Depending on the results of the review the supplier should make a decision on the level of support required to meet the reliability, maintainability and maintenance support requirements and the resulting costs before deciding whether to bid or accept the contract or propose appropriate alternative solutions.

5.2.2 Preparation of response

With regard to the preparation of a response by the supplier:

a) The supplier's proposal should meet the dependability requirements or standards specified by the acquirer. Where the proposal does not, proposed trade-offs should be identified along with differences between the trade-offs and the initial requirements (in terms of service level, for instance) in order that their value may be judged by the acquirer.

b) If the supplier's proposal requires software development, it should specify if a reliability growth programme or trial is to be implemented by the supplier.

c) The supplier's proposal should include a technical response, which should include a description of the understood reliability, maintainability and maintenance support problems, the proposed solution and whether it fully meets the dependability requirements.

d) The supplier's proposal should include a management response which should include a description of the approach, project milestones and schedule.

e) The supplier's proposal should include a financial response.

f) The supplier's proposal should include a training response which should describe the types of training being offered and their relationship to providing and maintaining trained personnel for the acquisition, supply, development, operation and maintenance processes.

5.2.3 Contract

The supplier should enter into a contract with the acquirer to supply the software product or service. The software product or service dependability requirements should be defined as described in 5.1.3.

5.2.4 Planning

The supplier should develop and document plans based upon the planning requirements. Items and example of plans should be considered under the umbrella of the project management plans. These project management planning items are critical and have an effect on the system reliability, maintainability, and maintenance support.

Les éléments de planification à considérer dans les plans de gestion du projet sont.

a) Planification de la gestion du projet – structure organisationnelle du projet, responsabilité et autorité – (plan de gestion de projet)

b) Environnement d'ingénierie pour le développement, l'exploitation ou la maintenance – (plan de gestion de l'ingénierie du système-SEMP, plan de développement du logiciel-SDP)

c) Structure de décomposition des travaux, y compris les logiciels, les services, les ressources, la taille du logiciel, etc. – (WBS)

d) Gestion des caractéristiques de qualité du logiciel – (plan AQ du logiciel)

e) Programme de fiabilité, y compris essai de croissance de la fiabilité, essai sous contrainte du logiciel, etc. – (plan du programme de fiabilité)

f) Analyse des modes de défaillance et de leur criticité, défaillance unique et localisation de la panne – FMECA du logiciel

g) Gestion de la sécurité, de la confidentialité et des autres exigences critiques – (plan de sécurité du logiciel, plan de confidentialité informatique)

h) Plan de gestion du sous-traitant

i) Approche et agent de vérification et validation – (plan IV&V)

j) Gestion du risque, impliquant les risques techniques potentiels, les risques relatifs au coût, et les risques relatifs au programme de travail – (plan de gestion du risque)

k) Formation du personnel – (plan de formation)

5.2.5 Exécution et maîtrise

Il convient que le fournisseur tienne compte de l'exécution et du contrôle des activités de sûreté de fonctionnement suivantes.

a) Il est recommandé que le fournisseur mette en application et exécute les plans de gestion de projet auxquels il est fait référence en 5.2.4.

b) Si le fournisseur développe un logiciel, alors il est recommandé d'effectuer les activités de sûreté de fonctionnement définies en 5.3.

c) Si le fournisseur utilise lui même des fournisseurs de logiciels, il agira en tant qu'acquéreur lorsqu'il se procurera le logiciel auprès de ses fournisseurs. C'est pourquoi il est important que le fournisseur effectue les activités de sûreté de fonctionnement définies en 5.1 vis à vis de ses propres fournisseurs de logiciels.

d) Si le fournisseur exploite le logiciel ou la prestation logicielle, alors il est recommandé que les activités de sûreté de fonctionnement définies en 5.4 soient effectuées.

e) Si le fournisseur effectue la maintenance du logiciel, alors il est recommandé d'effectuer les activités de sûreté de fonctionnement définies en 5.5.

f) Si le fournisseur assure la logistique pour le logiciel, alors il est recommandé d'identifier les services de logistique nécessaires pour maintenir le niveau de disponibilité spécifié, ou qu'ils soient le résultat d'une prescription spécifiée ou une solution à une prescription. Il est recommandé que le fournisseur conseille l'acquéreur en ce qui concerne les coûts supplémentaires qui résulteront de tels services de logistique.

g) Il convient d'inclure dans les domaines de maîtrise la surveillance et le contrôle de la l'avancement des exigences de sûreté de fonctionnement, de la progression des performances techniques, des coûts qui leur sont associés, et des programmes de travail et rapports relatifs à l'état du projet. Par exemple, on suivra les mesure des performances techniques (TPM) des profils de fiabilité et de maintenabilité. Il convient également que cette section comprenne l'identification des problèmes relatifs à la fonction de sûreté de fonctionnement, leur enregistrement, l'analyse qui en est faite et leur résolution.

Planning items to be considered under Project Management Plans are.

a) Project management planning – project organizational structure, responsibility and authority – (project management plan)

b) Engineering environment for development, operation or maintenance – (system engineering management plan-SEMP, software development plan-SDP)

c) Work breakdown structure including software products, services, resources, software size, etc. – (WBS)

d) Management of the quality characteristics of the software product – (software QA plan)

e) Reliability program including reliability growth test, software stress testing, etc – (reliability program plan)

f) Failure mode and criticality analysis, single-point failure and isolation fault – software FMECA

g) Management of the safety, security, and other critical requirements – (software safety plan, computer security plan)

h) Subcontractor management plan

i) Verification and validation approach and agent – (IV&V plan)

j) Risk management, which involves potential technical, cost, and schedule risks – (risk management plan)

k) Training of personnel – (training plan)

5.2.5 Execution and control

The supplier should consider the execution and control of the following dependability activities.

a) The supplier should implement and execute the project management plans referred to in 5.2.4.

b) If the supplier is developing a software product, then the dependability activities defined in 5.3 should be carried out.

c) If the supplier is using software contractors, he will act as an acquirer when acquiring the software from the contractors. It is important therefore that the supplier, with respect to his software contractors, should carry out the dependability activities defined in 5.1.

d) If the supplier is operating the software product or service, then the dependability activities defined in 5.4 should be carried out.

e) If the supplier is maintaining the software product, then the dependability activities defined in 5.5 should be carried out.

f) If the supplier is supporting the software product, then the support services required to maintain the specified availability level, or which are the result of a specified requirement or solution to a requirement, should be identified. The supplier should advise the acquirer what additional costs will arise as a result of such support services being provided.

g) The areas of control should include monitoring and controlling the progress of these dependability requirements, the progress of technical performance, their associate costs, and schedules and reporting of project status. An example will be to track the technical performance measurements (TPM) of reliability and maintainability profiles. This section should also include problem identification relating to the dependability function, recording, analysis and resolution.

5.2.6 Revue et évaluation

La revue et l'évaluation des aspects de fiabilité, de maintenabilité et de logistique de maintenance du logiciel sont des activités importantes pour le processus de soutien du cycle de vie. Les processus de soutien du cycle de vie concernés sont le processus de documentation, le processus de gestion de configuration, le processus d'assurance de la qualité, le processus de vérification, le processus de validation, le processus de revue conjointe, le processus d'audit et le processus de résolution des problèmes. L'organisme du fournisseur a la responsabilité de l'existence et de la mise en œuvre des processus. Les activités de revue et d'évaluation peuvent être internes ou externes selon qu'elles sont liées à la gestion du fournisseur ou, respectivement, de l'acquéreur. Les processus de soutien du cycle de vie concernent évidemment tous les aspects des processus d'acquisition, de fourniture, de développement, d'exploitation et de maintenance et assurent ainsi une contribution indirecte majeure au niveau atteint par la fiabilité, la maintenabilité et la logistique de maintenance. C'est pourquoi il est recommandé que l'acquéreur s'intéresse à toutes les activités de revue et d'évaluation ainsi qu'à celles associées directement à la fiabilité, la maintenabilité et la logistique de maintenance.

Les activités de revue et d'évaluation à considérer sont les suivantes.

a) Il est recommandé que le fournisseur effectue les activités de revue et d'évaluation définies dans le plan de projet et communique les résultats documentés à l'acquéreur si cela est spécifié dans le contrat ou si cela est demandé par l'acquéreur. Il est recommandé que cela inclue toutes les activités de revue et d'évaluation à la fois internes et externes. S'il n'est pas spécifié que les résultats de la revue et de l'évaluation doivent être communiqués à l'acquéreur, il est recommandé qu'ils fassent dans tous les cas l'objet d'une documentation et soient disponibles pour l'acquéreur sur demande.

b) Il est recommandé que les activités de revue comprennent une référence spécifique aux exigences de sûreté de fonctionnement.

c) Il est recommandé que le respect des demandes de sûreté de fonctionnement ou des normes ou règlements spécifiques soit démontré à l'acquéreur. Dans la plupart des cas, pour les gros systèmes, le fournisseur aura besoin de temps pour démontrer que les exigences de sûreté de fonctionnement ont été remplies. Un programme de croissance de la fiabilité fournira un moyen pour le démontrer ou l'évaluer sur une certaine durée.

5.2.7 Fourniture et achèvement du contrat

Il est recommandé que l'acquéreur s'assure que toutes les activités spécifiées ou inscrites dans le contrat qui sont liées au logiciel ont été achevées ou ont atteint un état mutuellement acceptable avant que le logiciel ou la prestation logicielle soient livrés. Cela pourrait par exemple comprendre l'achèvement d'un programme de croissance de la fiabilité ou la continuation d'un programme dans le cadre d'un plan ayant fait l'objet d'un accord.

Les activités liées au logiciel à considérer à l'achèvement et à la fourniture du produit par le fournisseur sont les suivantes.

a) Il est recommandé que le fournisseur livre le logiciel ou la prestation logicielle comme spécifié dans le contrat et conformément aux activités de sûreté de fonctionnement du processus de fourniture décrites dans les paragraphes 5.2.1 à 5.2.6.

b) Il est recommandé que le fournisseur assure un support pour le logiciel livré conformément aux activités de sûreté de fonctionnement définies en 5.5.

5.3 Processus de développement

Le processus de développement décrit les activités du développeur, de l'organisme qui définit et développe le logiciel. Si l'acquéreur demande au fournisseur de développer un logiciel, il est important que toutes les activités concernées du processus de développement (voir ISO/CEI 12207) et les processus de soutien du cycle de vie soient effectués. Il est en particulier recommandé que les activités de revue et d'évaluation du processus de soutien

5.2.6 Review and evaluation

Review and evaluation of the reliability, maintainability and maintenance support aspects of the software product are important supporting life-cycle process activities. The supporting life-cycle processes involved are the documentation process, configuration management process, quality assurance process, verification process, validation process, joint review process, audit process and problem resolution process. The supplier organization is responsible for ensuring that the processes are in existence and functional. The review and evaluation activities can be internal or external depending upon whether they are in conjunction with the management of the supplier or acquirer respectively. The supporting life-cycle processes do, of course, support all aspects of the acquisition, supply, development, operation and maintenance processes and as a result provide a major indirect contribution to the level of reliability, maintainability and maintenance support achieved. The acquirer should therefore take an interest in all review and evaluation activities as well as those directly associated with reliability, maintainability and maintenance support.

Review and evaluation activities to be considered are the following.

a) The supplier should carry out the review and evaluation activities defined in the project plan and communicate the documented results to the acquirer if it is specified in the contract or is required by the acquirer. This should include both internal and external review and evaluation activities. If it is not specified that the review and evaluation results be communicated to the acquirer, they should always be documented and be available to the acquirer on demand.

b) The review activities should include specific reference to dependability requirements.

c) Satisfaction of dependability requests or specific standards or regulations should be demonstrated to the acquirer. In most cases, for large systems, the supplier will need time to demonstrate that dependability requirements have been met. A reliability growth programme will provide a means of demonstrating or evaluating this over a period of time.

5.2.7 Delivery and completion

The acquirer should ensure that all specified or contracted software-related activities have been completed or have achieved a mutually acceptable state before the software product or service is delivered. This could, for example, involve the completion of a reliability growth programme or the continuation of a programme to an agreed plan.

Software related activities to be considered at completion and delivery of the product by the supplier are the following.

a) The supplier should deliver the software product or service as specified in the contract and which has been the subject of the supply process dependability activities described in 5.2.1 to 5.2.6.

b) The supplier should support the delivered software product according to the dependability activities defined in 5.5.

5.3 Development process

The development process describes the activities of the developer, the organization that defines and develops the software product. If the acquirer requires the supplier to develop a software product, it is important that all the relevant activities of the development process (see ISO/IEC 12207) and the supporting life-cycle processes are carried out. In particular, the review and evaluation activities of the supporting life-cycle processes (see 5.2.6)

du cycle de vie (voir 5.2.6) soient effectuées par le fournisseur dans la mesure où elles peuvent avoir une influence directe sur les performances de sûreté de fonctionnement du logiciel en développement. Le type de technologie et les outils logiciels utilisés par le fournisseur auront une influence sur les performances de sûreté de fonctionnement en aidant le fournisseur à atteindre un processus de développement reproductible et maîtrisé.

Il est recommandé que la méthodologie de conception de logiciel soit une norme industrielle reconnue (par exemple conception orientée objet) appropriée au logiciel en développement. Cela renforcera la perspective d'une conception bien structurée. Il est recommandé que le type de technologie utilisé soit moderne et adapté aux méthodologies de conception utilisées. Un exemple de cela pourrait être les stations de travail en réseau qui permettent un travail efficace et avec un bon rendement. Il est recommandé que les outils logiciels soient des standards industriels reconnus et suivis par un fournisseur industriel reconnu dans ce domaine. Comme exemple, on pourrait citer les compilateurs de langage de haut niveau compatibles avec la méthodologie de conception ou la gestion de la configuration et des outils de base de données qui permettront une gestion efficace des révisions de logiciels.

L'utilisation de technologies modernes et sophistiquées représente un facteur de risque. Par conséquent, il est recommandé de mettre en œuvre des méthodes systématiques d'identification, d'ordonnancement, de surveillance, de gestion et de recherche des risques.

Il convient d'inclure dans les activités du développeur du logiciel l'utilisation de prototypes, de modèles et de simulations. Ces pratiques sont parfois nécessaires pour définir, clarifier les exigences de l'utilisateur et valider l'aspect pratique de la mise en œuvre du système et les concepts d'interface utilisateur.

De nombreux aspects du processus de développement peuvent influencer les performances de sûreté de fonctionnement d'un logiciel; il est recommandé d'exécuter les activités mentionnées ci-dessous.

5.3.1 Mise en œuvre du processus

L'activité de mise en œuvre du processus définit ou sélectionne un modèle de cycle de vie de logiciel approprié au domaine d'application, à l'importance et la complexité du projet. Les activités et les tâches du processus de développement sont indiquées sur le modèle de cycle de vie choisi et les outils, méthodes, langages logiciels et normes appropriés choisis par le développeur pour permettre les activités du processus de développement. C'est pourquoi la sélection du modèle approprié de cycle de vie est importante pour la mise en œuvre la plus efficace du processus du cycle de vie et des activités de sûreté de fonctionnement associées décrites dans les articles suivants.

Les références suivantes aideront à la sélection des activités de mise en œuvre du processus approprié.

a) Les informations concernant l'application des processus du cycle de vie du logiciel aux phases du cycle de vie d'un logiciel peuvent être trouvées en se référant à la CEI 60300-3-6.

b) Si le développeur a un programme de sûreté de fonctionnement (voir CEI 60300-2), il est recommandé que le processus de développement pour les logiciels soit documenté et référencé dans le programme de sûreté de fonctionnement. Des informations supplémentaires peuvent être obtenues en se référant à la CEI 60300-3-6.

5.3.2 Analyse des exigences du système

Il est recommandé que l'objectif de l'analyse des exigences du système soit de produire une spécification homogène précise et complète des fonctions. Il est recommandé que les exigences de sûreté de fonctionnement soient incluses spécifiquement dans l'analyse.

should be carried out by the supplier, as these can have a direct influence on the dependability performance of the software product under development. The type of technology and software tools used by the supplier will have an influence on the dependability performance by helping the supplier to achieve a repeatable and controlled development process.

The software design methodology should be a recognized industry standard (for example object-oriented design) which is appropriate to the software product under development. This will enhance the prospect of a well-structured design. The type of technology should be modern and suited to the design methodologies being used. An example of this would be networked workstations that allow efficient and effective group working. The software tools should be to recognized industry standards and supported by a recognized industry supplier of tools. Examples of this would be high-level language compilers compatible with the design methodology or configuration management and database tools that will allow efficient management of software revisions.

The use of modern and sophisticated technologies does carry an element of risk. Therefore, methods for continuously identifying, prioritizing, monitoring, managing and tracking risks is recommended.

The software developer's activities should include the use of prototyping, modelling and simulation. These practices are sometimes necessary for defining, clarifying user requirements and validating implementation practicality of system and user interface concepts.

Many aspects of the development process can influence the dependability performance of a software product; the following activities should be implemented.

5.3.1 Process implementation

The process implementation activity defines or selects a software life-cycle model appropriate to the scope, magnitude and complexity of the project. The activities and tasks of the development process are mapped onto the selected life-cycle model and appropriate tools, methods, software languages and standards selected by the developer to enable the activities of the development process to be carried out. Selection of the appropriate life-cycle model is therefore important for the most effective implementation of the life-cycle processes and associated dependability activities described in the following clauses.

The following references will assist in the selection of appropriate process implementation activities.

a) Information on mapping of software life-cycle processes onto software life-cycle phases can be found by referring to IEC 60300-3-6.

b) If the developer has a dependability programme (see IEC 60300-2), the development process for software products should be documented and referenced in the dependability programme. Further information can be obtained by referring to IEC 60300-3-6.

5.3.2 System requirement analysis

The objective of the system requirements analysis should be to produce a precise and complete self-consistent specification of functions. The dependability requirements should be specifically included in this analysis.

Il convient de considérer les activités d'analyse des exigences du système suivantes.

a) Il est recommandé d'analyser l'exigence globale de sûreté de fonctionnement du système à développer en termes de fiabilité, de maintenabilité et de logistique de maintenance et d'identifier chaque fonction de sûreté de fonctionnement, liée au logiciel. Il est recommandé d'identifier les fonctions de sûreté de fonctionnement suivantes comme cela est approprié:
   - Fonctions liées à la détection et à la gestion des pannes dans le logiciel et le matériel associé.
   - Fonctions liées aux essais périodiques des fonctions de secours ou soutien en ligne et hors ligne.
   - Fonctions permettant la maintenance du logiciel.
   - Fonctions concernant la logistique de maintenance.
   - Fonctions spécifiant la disponibilité du logiciel.
   - Fonctions spécifiant la capacité du logiciel à être testé.
   - Fonctions liées à la préparation de la documentation.
   - Fonctions liées aux règlements et normes de sûreté de fonctionnement.
   - Fonctions liées aux essais de qualification.
   - Fonctions liées à l'exploitation du logiciel.
   - Fonctions liées au lancement et à l'arrêt du logiciel.
   - Fonctions liées au soutien utilisateur.
b) Il est recommandé que chaque fonction de sûreté de fonctionnement identifiée soit spécifiée à la fois de manière précise et cohérente. Le degré de précision spécifié pour chaque fonction dépendra du type de logiciel et de son application.
c) Il est recommandé d'effectuer une vérification pour voir si la spécification des fonctions de sûreté de fonctionnement est complète en s'assurant que chaque fonction identifiée a une spécification associée.
d) Il est recommandé que tout règlement ou toute norme de sûreté de fonctionnement appropriés soit pris en compte dans l'analyse des exigences relatives à l'analyse des systèmes et de la spécification des fonctions de sûreté de fonctionnement.

5.3.3 Conception de l'architecture du système

Si on prend en compte l'architecture globale du système, les exigences de performances de sûreté de fonctionnement identifiées comme fonctions de sûreté de fonctionnement (voir 5.3.2) doivent être considérées. Les critères de conception peuvent avoir une influence sur les aspects qualitatifs des performances de disponibilité et de maintenabilité mais peuvent également être complémentaires aux exigences de sûreté de fonctionnement quantitatives, par exemple lorsque le produit doit être tel qu'aucune panne ne puisse conduire à un état critique du produit. C'est pourquoi il convient que la conception architecturale de haut niveau du système tienne compte des conceptions bien établies ou éprouvées qui présentent de préférence des enregistrements probants d'exploitation et de maintenance et qui sont appropriés pour les fonctions de sûreté de fonctionnement identifiées. S'ils sont disponibles, les résultats des programmes de croissance de la fiabilité pourraient aider à identifier la bonne adaptabilité des architectures particulières de système. Pour les produits existants, il convient que la conception architecturale de haut niveau prenne en compte les risques tels que l'instabilité de la conception résultant de la mise à jour d'un vendeur ou la disponibilité du produit pour le cycle de vie prévu du système.

5.3.4 Analyse des exigences du logiciel

Il est recommandé que l'objectif de l'analyse des exigences du logiciel soit de produire une spécification homogène précise et complète des fonctions pour chaque module ou élément de logiciel. Il est recommandé que les exigences de sûreté de fonctionnement soient incluses de manière spécifique dans l'analyse.

The following system requirement analysis activities should be considered.

a) The overall dependability requirement of the system to be developed should be analyzed in terms of reliability, maintainability and maintenance support and each dependability function, related in any way to software, identified. The following dependability functions should be identified as appropriate:
   - Functions related to the detection and management of faults in the software product and associated hardware.
   - Functions related to the periodic testing of backup or supporting functions on-line and off-line.
   - Functions that allow the software product to be maintained.
   - Functions related to maintenance support.
   - Functions that specify availability of the software product.
   - Functions that specify the software product testability.
   - Functions related to the preparation of documentation.
   - Functions related to dependability regulations or standards.
   - Functions related to qualification testing.
   - Functions related to the operation of the software product.
   - Functions related to the start-up and shutdown of the software product.
   - Functions related to user support.
b) Each identified dependability function should be specified in precise and consistent terms. The degree of precision with which each function can be specified will depend upon the type of software product and its application.
c) A check should be made that the specification of dependability functions is complete by ensuring that each identified function has an associated specification.
d) Every relevant regulation or dependability standard should be taken into account in the analysis of systems analysis requirements and dependability function specification.

5.3.3 System architectural design

When considering the overall system architecture the dependability performance requirements identified as dependability functions (see 5.3.2) are to be taken into account. Design criteria can have a bearing on the qualitative aspects of availability and maintainability performance but can also be complementary to any quantitative dependability requirements such as whether the product has to be such that no single fault can lead to a critical state of the product. Top-level architectural design of the system therefore should take account of known established or proven system designs which preferably have proven records for operation and maintenance and are appropriate for the identified dependability functions. If available, the results of reliability growth programmes might help identify the suitability of particular system architectures. For existing products, the top-level architectural design should take into account risks such as instability in the design following a vendor update or availability of the product for the projected life cycle of the system.

5.3.4 Software requirements analysis

The objective of the software requirements analysis should be to produce a precise and complete self-consistent specification of functions for each module or item of software. The dependability requirements should be specifically included in this analysis.

Il convient que l'analyse des exigences du logiciel comprenne ce qui suit.

a) Il est recommandé que l'exigence de sûreté de fonctionnement du logiciel à développer soit analysée en termes de fiabilité, de maintenabilité et de logistique de maintenance et que chaque fonction de sûreté de fonctionnement soit identifiée.

b) Il est recommandé que chaque fonction de sûreté de fonctionnement identifiée soit spécifiée en termes précis et homogènes. Le degré de précision avec lequel chaque fonction peut être spécifiée dépendra du type de logiciel et de son application.

c) Il est recommandé qu'une vérification soit effectuée pour voir si la spécification des fonctions de sûreté de fonctionnement est complète en s'assurant que chaque fonction identifiée a une spécification associée.

d) Il est recommandé que les spécifications pour les exigences de conception d'ingénierie couvrent les exigences de qualification, les normes applicables, les exigences de disponibilité et de maintenance.

5.3.5 Conception de l'architecture du logiciel

Lorsqu'on étudie l'architecture d'un logiciel, il y a lieu de prendre en compte les exigences de sûreté de fonctionnement identifiées comme fonctions de sûreté de fonctionnement (voir 5.3.2*)*, en examinant les aspects de la conception qui affectent les fonctions définies de sûreté de fonctionnement. Comme pour la conception de l'architecture du système, il est recommandé que la conception de l'architecture du logiciel prenne en compte les conceptions connues ou éprouvées qui sont appropriées aux fonctions de sûreté de fonctionnement identifiées.

5.3.6 Conception détaillée du logiciel

Il est recommandé que la conception détaillée d'un logiciel se fonde sur l'architecture du système et du logiciel décrite ci-dessus. Il est recommandé que la méthode de conception facilite l'incorporation des caractéristiques suivantes dans les conceptions de logiciels:

a) Il est recommandé que le développeur ait des activités de conception détaillée de logiciel bien documentées et établies qui facilitent la conception du logiciel et qui reflètent de manière non ambiguë les exigences des fonctions de sûreté de fonctionnement spécifiées.

b) Il est recommandé que la conception facilite la prise en compte de caractéristiques telles que la modularité, la maintenabilité, l'aptitude aux essais, la vérification et la validation.

c) Il est recommandé que les données d'entrée et de sortie de conception à chaque étape du processus de développement du logiciel soient enregistrées, analysées et documentées pour être utilisées dans la revue de projet et pour aider les améliorations à la conception de produit.

d) Il est recommandé que les procédures pour la maîtrise des modifications de la conception et les revues soient spécifiées et mises en application (voir CEI 61160).

e) Il est recommandé que le processus de vérification de la conception soit documenté et mis en application.

f) Il est recommandé que les méthodologies de conception établies et les outils de développement qui facilitent l'expression du flux d'informations entre les modules, les structures de données et les sujétions spécifiées dans les fonctions identifiées de sûreté de fonctionnement soient utilisés de manière spécifique.

g) Il est recommandé que la documentation utilisateur soit développée et mise à jour comme cela est exigé, simultanément avec le logiciel. Il est recommandé qu'elle soit cohérente avec le niveau de révision du logiciel.

5.3.7 Codage et essais du logiciel

Il est recommandé qu'un jeu convenable d'outils intégrés tels que les compilateurs de langage, les outils de gestion de configuration et les outils automatisés soient utilisés pendant le développement du logiciel. Il est recommandé que la sélection du jeu d'outils soit fondée sur des produits éprouvés bien suivis par les fabricants de logiciels établis.

The software requirements analysis should include the following.

a) The dependability requirement of the software to be developed should be analyzed in terms of reliability, maintainability and maintenance support and each dependability function identified.

b) Each identified dependability function should be specified in precise and consistent terms. The degree of precision with which each function can be specified will depend upon the type of software product and its application.

c) A check should be made that the specification of dependability functions is complete by ensuring that each identified function has an associated specification.

d) Specifications for engineering design requirements should cover qualification requirements and relevant standards, availability requirements and maintenance requirements.

5.3.5 Software architectural design

When considering the software architecture, the dependability performance requirements identified as dependability functions (see 5.3.2) are to be taken into account by considering those aspects of design which impinge upon the defined dependability functions. As for system architectural design, the software architectural design should take account of known or proven designs which are appropriate for the identified dependability functions.

5.3.6 Software detailed design

The detailed design of the software should be based on the above described system and software architecture. The design method should facilitate the inclusion of the following features in the software designs:

a) The developer should have well-documented and established software detailed design activities that facilitate the design of software that unambiguously reflects the requirements of the specified dependability functions.

b) The design should facilitate the addressing of such features as modularity, maintainability, testability, verification and validation.

c) The design input and output data at each stage of the software development process should be recorded, analyzed and documented for use in project review and to assist product design improvements.

d) The procedures for design change control and reviews should be specified and implemented (see IEC 61160).

e) The design verification process should be documented and implemented.

f) Established design methodologies and development tools should be used especially those that facilitate the expression of information flow between modules, data structures and dependencies specified in the identified dependability functions.

g) User documentation should be developed and updated as required in conjunction with the software. It should be consistent with the revision level of the software.

5.3.7 Software coding and testing

A suitable set of integrated tools such as language compilers, configuration management tools and automated testing tools should be used during the development of the software. Selection of the set of tools should be based on proven products that are well supported by established software manufacturers.

Il convient de considérer les activités suivantes de codage et d'essais.

a) Il est recommandé que le développeur ait des procédures de codage et d'essais des logiciels bien documentées et établies spécifiant une bonne pratique de programmation et une bonne documentation.

b) Il est recommandé que la procédure pour les essais et la validation des logiciels soit documentée et qu'elle comprenne une procédure d'action corrective. S'il existe des exigences de sûreté de fonctionnement spécifiées, il est recommandé que les essais en liaison directe avec ces exigences soient inclus.

c) Il est recommandé qu'il y ait une procédure bien documentée, coordonnée pour la prise en compte des défauts logiciels et le suivi des corrections qui en résultent. Il est important pour la sûreté de fonctionnement du logiciel que cette procédure soit bien établie et mise en œuvre de manière efficace pour s'assurer que tout défaut ayant un impact sur la disponibilité de la fonctionnalité logicielle exigée soit corrigé de manière rapide et efficace. Dans le but de fournir une analyse des types d'erreurs, le développeur peut également utiliser les données collectées lors du rapport/du suivi de défauts, la fréquence d'occurrence et les schémas d'erreur par élément de configuration ou ceux qui sont utilisés pour démontrer la croissance de fiabilité.

5.3.8 Intégration du logiciel

Il est recommandé que l'intégration de logiciel permette d'essayer de manière spécifique la mise en œuvre correcte de toutes les fonctions de sûreté de fonctionnement identifiées. Il est recommandé que cet essai démontre que les composants associés interagissent correctement pour assurer les fonctions de sûreté de fonctionnement identifiées. Il est recommandé que les résultats d'essais d'intégration soient présentés sous une forme permettant un audit.

Il est recommandé que la procédure d'intégration de logiciel, les essais de système et l'installation fassent l'objet d'une documentation complète.

5.3.9 Essais de qualification du logiciel

S'il existe des cibles de qualification de sûreté de fonctionnement quantitatives ou qualitatives spécifiques définies dans la spécification d'exigences, il est recommandé qu'elles aient été incluses dans les essais des fonctions de sûreté de fonctionnement spécifiées et dans les essais d'intégration associés. Compte tenu de la nature de la sûreté de fonctionnement, il pourrait y avoir un accord entre le fournisseur et l'acquéreur prévoyant que les essais de qualification du logiciel soient effectués sur une période pendant laquelle le système est en utilisation (ou selon des essais plus complets, suivant ce qui est le mieux approprié au contexte). Il est recommandé que les résultats de ces essais de qualification fassent l'objet d'un audit pour étudier leur conformité avec les cibles de qualification spécifiées.

Les aspects des essais de qualification du logiciel a considérer sont les suivants.

a) Il est recommandé que le développeur conduise des essais de qualification conformément à toute prescription de sûreté de fonctionnement de qualification spécifique.

b) Il est recommandé que le développeur évalue l'étendue des essais et la conformité avec toute prescription de sûreté de fonctionnement.

c) Il est recommandé qu'il y ait un programme complet de revues techniques, d'audits internes et de revues de suivi d'avancement des modifications pour tout essai de qualification spécifique, pour assurer que les essais de qualification sont en relation précise avec les exigences de qualification de sûreté de fonctionnement spécifiées et que toute modification proposée aux essais de qualification ne remette pas en question l'exactitude de leur relation avec les objectifs de qualification de sûreté de fonctionnement exigée.

The following coding and testing activities should be considered.

a) The developer should have well-documented and established software coding and testing procedures which specify good programming practice and documentation.

b) The procedure for software product test and validation should be documented and should include a corrective action procedure. If there are specified dependability requirements, tests should be included that relate directly to these requirements.

c) There should be a fully documented, coordinated procedure for reporting software defects and tracking their subsequent correction. It is important for software dependability that this procedure is well established and efficiently implemented in order to ensure that any defects that impact the availability of the required software functionality are corrected quickly and efficiently. The developer, to provide an analysis of fault types, can also use the data collected by the defect reporter/tracker, frequency of occurrence and fault patterns per configuration item or be used to demonstrate reliability growth.

5.3.8 Software integration

Software integration should specifically test for correct implementation of all the identified dependability functions. The test should demonstrate that associated components interact correctly to perform the specified dependability functions. The integration test results should be presented in an auditable form.

The procedure for software integration, system test and installation should be fully documented.

5.3.9 Software qualification testing

If there are specific quantitative or qualitative dependability qualification targets defined in the requirement specification, these should have been included in the specified dependability functions and the associated integration tests. Because of the nature of dependability, it might be mutually agreed between supplier and acquirer that software qualification testing be carried out over a period of time when the system is in use (or in extended trials, whichever is most appropriate to the context). The results of these qualification tests should be audited for compliance with the specified qualification targets.

Aspects of software qualification testing to be considered are the following.

a) The developer should conduct qualification testing in accordance with any specific dependability qualification requirements.

b) The developer should evaluate test coverage and conformance with any dependability requirements.

c) There should be a full programme of technical reviews, internal audits and change control reviews for any specific qualification tests to ensure that the qualification tests relate accurately to the specified dependability qualification requirements and that any proposed changes to the qualification tests do not compromise the accuracy of their relationship with the required dependability qualification targets.

5.3.10 Intégration du système

«Système» est le terme utilisé pour décrire la combinaison d'exploitation finale du logiciel avec le matériel. L'intégration du système signifiera l'intégration du logiciel avec les composants du matériel. On essaie les performances de sûreté de fonctionnement du système intégré et on les vérifie par rapport aux exigences globales qualitatives et quantitatives de sûreté de fonctionnement. Il est recommandé, par conséquent, de soumettre les performances de fiabilité et de maintenabilité du système à des essais et d'obtenir la confirmation qu'elles répondent aux fonctions de sûreté de fonctionnements identifiées.

Il convient que l'intégration du système comprenne les activités suivantes.

a) Il est recommandé que la procédure d'intégration du système et les essais fassent l'objet d'une documentation complète.

b) Il est recommandé que les résultats de l'essai d'intégration du système soient soumis à un programme complet de revues techniques, d'audits internes et externes pour vérifier la conformité avec les exigences de sûreté de fonctionnement spécifiées quantitatives et qualitatives du système.

5.3.11 Essais de qualification du système

L'objectif des essais de qualification du système est de s'assurer qu'après l'intégration du système, chaque exigence du système est essayée quant à sa conformité et que le système est prêt à être livré. Les essais de qualification du système pour les performances de sûreté de fonctionnement peuvent être effectués en essayant la conformité de chaque fonction de sûreté de fonctionnement identifiée. Il est recommandé d'évaluer les exigences de fonction de sûreté de fonctionnement du système par rapport aux exigences de fiabilité et de maintenabilité pour les fonctions de sûreté de fonctionnement identifiées. Compte tenu de la nature de la sûreté de fonctionnement, il pourrait y avoir un accord entre le fournisseur et l'acquéreur pour que les essais de qualification du système soient effectués sur une période pendant laquelle le système est en utilisation (ou selon des essais plus complets, suivant ce qui est le mieux approprié au contexte). Une autre méthode pour déterminer si la fiabilité globale d'un système est conforme aux exigences est d'estimer la fiabilité du logiciel du système intégré au moyen d'une technique qui modélise le processus de développement et/ou les propriétés de code source. On établit un cadre de gestion et une procédure pour rassembler des données et les données qui en résultent sont combinées avec le modèle pour produire une estimation de la fiabilité globale du système. Il est recommandé que les résultats d'essai de qualification fassent l'objet d'un audit pour vérifier leur conformité avec les exigences de sûreté de fonctionnement de qualification et qu'un rapport de qualification soit préparé. Dans certains cas, le fournisseur et le client pourraient arriver à un accord pour démarrer un programme de croissance de la fiabilité si les résultats des essais de qualification indiquent que les améliorations des performances de sûreté de fonctionnement sont nécessaires avant que le système soit conforme aux exigences et qu'elles peuvent être obtenues par un programme de coopération.

Il convient que les activités d'essais de qualification du système comprennent ce qui suit.

a) Il est recommandé que le développeur conduise des essais de qualification du système global conformément aux exigences de sûreté de fonctionnement de qualification spécifiques.

b) Il est recommandé que le développeur évalue ce que couvre l'essai et la conformité avec toute prescription de sûreté de fonctionnement du système global.

5.3.12 Installation du logiciel

Les essais concernant l'installation du logiciel sont intimement liés aux essais de qualification du système et font partie des vérifications effectuées pour s'assurer que le logiciel est prêt pour la livraison. Les conditions dans lesquelles le logiciel est installé et exploité auront une influence sur les performances de fiabilité et de maintenabilité obtenues. Il est donc recommandé que les essais d'installation soient effectués dans les conditions d'installation spécifiées.

5.3.10 System integration

The system is the term used to describe the final operating combination of the software with the product hardware. System integration will involve the integration of the software with the product hardware components. It is the dependability performance of the integrated system that is tested and checked against overall qualitative and quantitative dependability requirements. The system reliability and maintainability performance should therefore be tested and confirmed to meet the identified dependability functions.

System integration should include the following activities.

a) The procedure for system integration and test should be fully documented.

b) The system integration test results should be subject to a full programme of technical reviews, internal and external audits for compliance with specified system quantitative and qualitative dependability requirements.

5.3.11 System qualification testing

The objective of system qualification testing is to ensure that, after system integration, each system requirement is tested for compliance and that the system is ready for delivery. System qualification testing of dependability performance can be achieved by testing each identified dependability function requirement for compliance. The system dependability function requirements should be evaluated for compliance with respect to reliability and maintainability requirements through the identified dependability functions. Because of the nature of dependability, it might be mutually agreed between supplier and acquirer that system qualification testing be carried out over a period of time when the system is in use (or in extended trials, whichever is most appropriate to the context). Another method for determining whether the overall system reliability complies with requirements is to assess the software reliability of the integrated system by means of a technique which models the development process and/or source code properties. A management framework and data collection procedure is set up and the resulting data is combined with the model to produce an assessment of the overall system reliability. The qualification test results should be audited for compliance with dependability qualification requirements and a qualification report prepared. In some cases, the supplier and customer might reach a mutual agreement to initiate a reliability growth programme if qualification test results indicate that dependability performance improvements are required before the system is compliant with requirements and can be achieved through a cooperative programme of work.

System qualification testing activities should include the following.

a) The developer should conduct overall system qualification testing in accordance with any specific dependability qualification requirements.

b) The developer should evaluate the test coverage and conformance with any overall system dependability requirements.

5.3.12 Software installation

Software installation testing is closely coupled with system qualification testing and is part of the checks carried out to check that the software product is ready for delivery. The conditions under which software is installed and operated will have a bearing on the reliability and maintainability performance achieved. Installation testing should therefore be carried out under the installation conditions specified.

Il convient que les activités d'installation du logiciel comprennent ce qui suit.

a) Il est recommandé que le développeur installe le logiciel ou le système conformément à la documentation d'installation et vérifie qu'il est installé et fonctionne comme prescrit. Compte tenu de la nature de la sûreté de fonctionnement, il pourrait y avoir un accord entre le fournisseur et l'acquéreur pour que les essais d'installation du logiciel soient effectués sur une période pendant laquelle le système est en utilisation (ou selon des essais plus complets, suivant ce qui est le mieux approprié au contexte).

b) Il est recommandé que la conformité avec toute prescription de sûreté de fonctionnement liée à l'installation soit vérifiée et documentée.

5.3.13 Assistance à la réception du logiciel

L'assistance à la réception du logiciel est une activité importante du développeur qui permet à l'acquéreur d'effectuer une revue conjointe efficace et des essais de qualification du logiciel. Il est recommandé que le développeur s'engage dans l'assistance à la réception du logiciel, en particulier si des exigences d'essais de conformité de sûreté de fonctionnement longues ou difficiles sont prévisibles.

Il est recommandé que le développeur fournisse un soutien initial approprié et continu à l'acquéreur jusqu'à ce que les exigences de sûreté de fonctionnement spécifiées aient été démontrées.

5.4 Processus d'exploitation

Le processus d'exploitation définit les activités du chargé de l'exploitation et de l'organisme qui exploite le système ou le produit dans son environnement. Ce processus fait référence au système ou au produit et non pas au seul logiciel car l'exploitation du logiciel fait partie intégrante du système ou du produit. Les performances de sûreté de fonctionnement du logiciel pendant son exploitation dépendront des procédures d'exploitation du logiciel et de maintenance mises en application dans l'environnement du système. Il est recommandé d'identifier les procédures d'exploitation et de maintenance nécessaires pour remplir les fonctions de sûreté de fonctionnement identifiées et les actions prises pour vérifier qu'elles sont effectuées pendant l'exploitation du système. Les activités du processus d'exploitation sont la mise en œuvre du processus, les essais d'exploitation, l'exploitation du système et l'assistance fournie à l'utilisateur. Les procédures d'exploitation et de maintenance du logiciel seront étudiées dans ces rubriques.

5.4.1 Mise en œuvre du processus

Pour mettre en œuvre le processus d'exploitation, il est recommandé que le chargé de l'exploitation planifie et définisse les tâches et activités qu'il effectuera pour mettre en œuvre les activités qui le constituent. Pour les performances de sûreté de fonctionnement, il est recommandé que le plan comprenne les éléments suivants.

a) Il est recommandé que les procédures d'exploitation fassent l'objet d'une documentation et soient disponibles pour les utilisateurs. Il est recommandé que les manuels soient maintenus à jour par un service actif de mise à jour des documents utilisateur.

b) Il est recommandé que la formation à l'exploitation du système soit fournie, le cas échéant, pour les chargés de l'exploitation.

c) Il est recommandé que les plaintes des clients pendant l'exploitation du système et l'entretien soient enregistrées selon une procédure documentée, et analysées pour faire l'objet d'une action corrective rapide, le cas échéant.

d) Il est recommandé que les procédures soient définies pour spécifier toute action de routine (par exemple copie de secours ou initialisation de données, actions de lancement ou d'arrêt) nécessaire pour être conforme aux fonctions de sûreté de fonctionnement identifiées.

Software installation activities should include the following.

a) The developer should install the software product or system according to the installation documentation and verify that it is installed and operating as required. Because of the nature of dependability, it might be mutually agreed between supplier and acquirer that software installation testing be carried out over a period of time when the system is in use (or in extended trials, whichever is most appropriate to the context).

b) Conformance with any specified installation related dependability requirements should be verified and documented.

5.3.13 Software acceptance support

Software acceptance support is an important developer activity which allows the acquirer to carry out effective joint review and qualification testing of the software product. The commitment to support acceptance testing should be given by the developer especially if prolonged or difficult dependability requirements compliance testing is expected.

The developer should provide appropriate initial and continuing support to the acquirer until the specified dependability requirements have been demonstrated.

5.4 Operation process

The operation process defines the activities of the operator and the organization that operates the system or product in its live environment. This process refers to the system or product and not the software alone because the operation of the software product is an integral part of the system or product. The dependability performance of the software during its operation will depend on the software operation and maintenance procedures implemented within the system environment. The operation and maintenance procedures required to meet the identified dependability functions should be identified and actions taken to check that they are being carried out during the operation of the system. The operation process constituent activities are process implementation, operational testing, system operation and user support. The software operation and maintenance procedures will be considered under these headings.

5.4.1 Process implementation

To implement the operation process the operator should plan and define the tasks and activities he will carry out to implement the constituent activities. When considering dependability performance, the plan should include the following.

a) The operation procedures should be documented and available to the users. The manuals should be kept up to date via an active user document update service.

b) Training for system operation, where necessary, should be provided to the operators.

c) Customers' complaints during system operation and servicing should be retained via a documented reporting procedure and analyzed for prompt corrective action where appropriate.

d) Procedures should be defined which specify any routine actions (for example backing up or initializing data, start-up or shutdown actions) which are necessary in order to meet the identified dependability functions.

e) Il est recommandé de spécifier le domaine d'application des activités concernant le logiciel.

f) Il est recommandé de définir des procédures qui spécifient comment il convient d'essayer le logiciel dans son environnement d'exploitation et comment les résultats des essais doivent être liés aux actions de maintenance ou à tout programme de croissance de la fiabilité qui est mis en œuvre.

Si un développeur spécifie les essais d'exploitation, il est recommandé que les résultats soient liés à l'estimation qui permet de décider si le logiciel est prêt pour une utilisation opérationnelle.

5.4.2 Les essais d'exploitation

Les essais d'exploitation sont effectués pour vérifier si le système ou le logiciel répond aux critères spécifiés pour autoriser son utilisation opérationnelle. Dans le cadre de la sûreté de fonctionnement en exploitation, les performances de fiabilité et maintenabilité nécessaires au système ou au logiciel sont prises en compte. Les exigences de fiabilité et de maintenance ont été spécifiées en termes de fonctions de sûreté de fonctionnement (voir 5.3.2). Il est recommandé que les essais d'exploitation soient effectués pour vérifier si les exigences de fonction de sûreté de fonctionnement du système ont été remplies.

Il convient que les activités d'essais d'exploitation comprennent ce qui suit.

a) L'estimation de la sûreté de fonctionnement du système nécessitera l'établissement d'un cadre pour la collecte de données, la sélection de techniques d'estimation de fiabilité logicielle appropriées et la comparaison de la sûreté de fonctionnement estimée avec les exigences de fonction de sûreté de fonctionnement du système spécifiées. S'il y a des exigences de conformité avec des normes et règlements de sûreté de fonctionnement spécifiques, il est recommandé qu'elles soient couvertes par les exigences de la fonction de sûreté de fonctionnement du système.

   NOTE Des détails concernant la sélection de la méthode appropriée de collecte des données et de la technique d'estimation de fiabilité, par exemple sélection d'un produit approprié ou d'un modèle de fiabilité pour traiter les données rassemblées, sont donnés dans la BS 5760: Partie 8.

b) Selon l'environnement d'exploitation du système et l'usage, il pourrait être nécessaire de rassembler des données sur une période plus longue avant de pouvoir estimer la fiabilité logicielle du système. Il convient que le fournisseur et l'acquéreur conviennent de la période nécessaire à la collecte des données. Lorsqu'il n'est pas possible de spécifier et d'essayer le système par rapport aux exigences de sûreté de fonctionnement quantitatives, l'acquéreur et le fournisseur pourraient se mettre d'accord sur la livraison du logiciel après estimation de fiabilité qualitative initiale sous réserve d'une mise en œuvre à plus long terme d'une collecte de données et d'un programme de croissance de la fiabilité pour atteindre les buts de sûreté de fonctionnement.

c) La performance de sûreté de fonctionnement du système après livraison à l'utilisateur peut également être affectée par les erreurs ou omissions dans les procédures d'exploitation utilisées par le chargé de l'exploitation. Il est recommandé de conserver des enregistrements de toute modification dans les procédures d'exploitation de manière à pouvoir identifier toute modification liée à la fiabilité du système et à améliorer les procédures d'exploitation.

5.4.3 Exploitation du système

L'activité d'exploitation du système est définie comme l'exploitation du système dans son environnement prévu conformément à la documentation utilisateur. C'est pourquoi il est recommandé de tenir compte de la vérification de conformité aux exigences de fonction de sûreté de fonctionnement qui définissent l'environnement dans lequel le système va fonctionner et aussi que la documentation utilisateur spécifie de manière précise comment le système devrait être mis en œuvre.

e) The scope of the software activities should be specified.

f) Procedures should be defined which specify how the software should be tested in its operational environment and how the results of the testing are to be linked to maintenance actions or to any reliability growth programme that is being implemented.

If a developer is specifying the operational testing, the results should be linked to assessing whether the software product is ready for operational use.

5.4.2 Operational testing

Operational testing is carried out to check whether the system or software product has met the specified criteria for releasing it for operational use. When considering operational dependability, the required reliability and maintainability performance of the system or software product is considered. The reliability and maintenance requirements have been specified in terms of dependability functions (see 5.3.2). Operational testing should be carried out to check whether the specified system dependability function requirements have been met.

Operational testing activities should include the following.

a) Assessment of the system dependability will require the establishment of a framework for collection of data, selection of the appropriate software reliability assessment technique and comparing the assessed dependability with the specified system dependability function requirements. If there are requirements for conformance with specific dependability standards or regulations, these should be covered by the system dependability function requirements.

   NOTE Details on selection of the appropriate data collection method and reliability assessment technique, for example, selection of an appropriate product or reliability model to process the collected data, are given in BS 5760: Part 8.

b) Depending upon the system operational environment and usage it might be necessary to collect data over an extended period of time before system software reliability can be assessed. Supplier and acquirer should mutually agree the required period of data collection. Where it is not possible to specify and test the system against quantitative dependability requirements, the acquirer and supplier might mutually agree to the delivery of the software product following initial qualitative reliability assessment subject to the longer term implementation of a data collection and reliability growth programme to achieve dependability goals.

c) The dependability performance of the system after delivery to the user can also be affected by errors or omissions in the operational procedures used by the operator. Records should be kept of any changes in operational procedure so that any related changes in system reliability can be identified and operational procedures improved.

5.4.3 System operation

The system operation activity is defined as the operation of the system in its intended environment according to the user documentation. Consideration should therefore be given to checking for compliance with those dependability function requirements which define the environment that the system is to operate in and also that the user documentation accurately specifies how the system should be operated.

Les vérification d'activités d'exploitation du système sont les suivantes.

a) Il est recommandé d'effectuer la vérification de conformité avec les fonctions de sûreté de fonctionnement qui spécifient le type et la fréquence des activités de logistique de maintenance. Les activités typiques de logistique de maintenance, qui peuvent avoir un impact important sur la sûreté de fonctionnement ou la disponibilité, sont les copies de sauvegarde périodiques des données du système, la mise à jour systématique du logiciel aux niveaux de la dernière révision ou la maintenance régulière du matériel. L'objectif de ces vérifications est d'assurer que toutes les fonctions de maintenance définies sont effectuées de telle manière que le logiciel soit exploité avec la dernière révision du logiciel où les erreurs sont corrigées sur le matériel bien entretenu avec des copies de sauvegarde régulières du système de telle façon que le système puisse être rétabli avec une interruption minimale en cas de défaillance de celui-ci. Il est recommandé d'effectuer certaines activités de maintenance telles que les copies de sauvegarde lorsque le risque est minimal pour l'exploitation du système, par exemple lorsqu'il est hors-ligne ou lorsqu'il y a un minimum d'opérateurs ou d'activités.

b) Il est recommandé que la documentation utilisateur soit vérifiée quant à sa précision, son caractère complet et sa facilité d'utilisation par le chargé de l'exploitation, dans la mesure où une documentation incorrecte, incomplète ou difficile d'utilisation peut conduire à des erreurs de la part du chargé de l'exploitation ou à des défaillances d'exploitation du système. Il est recommandé que le fournisseur effectue si possible un audit des fonctions du chargé de l'exploitation identifiées selon chaque section de la documentation et note toute erreur et omission. Il est recommandé de faire un rapport à l'acquéreur des résultats avec toutes les actions correctives.

c) Il peut s'avérer impossible d'identifier les erreurs ou omissions dans la documentation utilisateur avant la livraison du système à l'utilisateur. C'est pourquoi il est recommandé de conserver des enregistrements de toute modification dans la procédure d'exploitation après la livraison, de telle manière que toute modification liée à la fiabilité du système puisse être identifiée et les procédures d'exploitation améliorées.

5.4.4 Assistance fournie à l'utilisateur

L'activité d'assistance fournie à l'utilisateur est définie comme les tâches du fournisseur qui consistent à assurer une assistance et une consultation à l'utilisateur ainsi que le suivi des demandes des utilisateurs ou des rapports de problèmes pour le processus de maintenance (voir 5.5). L'activité d'assistance à l'utilisateur peut agir de façon importante sur les performances de disponibilité et de sûreté de fonctionnement du logiciel en fournissant par exemple des conseils rapides et experts si l'utilisateur a besoin d'assistance, ou un processus efficace de suivi des rapports des problèmes rencontrés par l'utilisateur vers les processus de développement de logiciel et de mise à jour. Il est recommandé que l'activité d'assistance fournie à l'utilisateur comprenne les tâches détaillées ci-dessous.

a) Il est recommandé que le fournisseur offre un service d'assistance bien organisé et avec une bonne expertise, capable de répondre rapidement et de manière efficace aux demandes d'assistance de l'utilisateur. Il est recommandé que le service d'assistance permette de répondre aux demandes d'assistance téléphoniques ou de fournir une assistance sur site dans les délais si ce service a été négocié entre l'utilisateur et le fournisseur.

b) Il est recommandé que le fournisseur soit prêt à fournir des services d'assistance pour le logiciel en dehors des heures normales de travail s'il existe une prescription spécifique en la matière ou si l'analyse de la fonction de sûreté de fonctionnement aboutit à un accord qui le prévoit.

c) Il est recommandé que le fournisseur ait une procédure spécifiée et éprouvée pour recevoir les rapports de problèmes ou les demandes d'améliorations de l'utilisateur, avec création de solutions et mise en œuvre de la mise à jour logicielle correspondante sur le système des utilisateurs.

Recommended system operational activity checks are the following.

a) The check for compliance with those dependability functions that specify the type and frequency of the maintenance support activities should therefore be carried out. Typical maintenance support activities, which can have an important impact on dependability or availability, are periodic backup of system data, systematic update of the software to the latest revision levels or regular maintenance of the product hardware. The objective of these checks is to ensure that all defined maintenance functions are carried out in such a way that the software is operated with the latest error-corrected software revisions on the well maintained hardware with regular system backups so that the system can be restored with minimum disruption in the event of a system failure. Some maintenance activities such as backups should be carried out when there is least risk to the system operation, for example when the system is off-line or when there is minimum operator or system activity.

b) The user documentation should be checked for accuracy, completeness and ease of use by the operator, as incorrect, incomplete or difficult to use documentation can lead to operator error or system operational failure. If possible an audit of the identified operator functions against each section of the documentation should be conducted by the supplier and any errors and omissions noted. The results with a report of any corrective actions should be reported to the acquirer.

c) It might not be possible to identify errors or omissions in the user documentation prior to delivery of the system to the user. Records should therefore be kept of any changes in operational procedure after delivery, so that any related changes in system reliability can be identified and operational procedures improved.

5.4.4 User support

The user support activity is defined as those supplier tasks which provide assistance and consultation to the user and the feedback of user requests or problem reports to the maintenance process (see 5.5). The user support activity can have a significant effect on the availability and dependability performance of the software product by, for example, providing rapid and expert advice if the user requests support or providing an efficient process for feedback of user problem reports to the software development and update processes. The user support activity should include the following tasks.

a) The supplier should provide a well-organized and expert support service that is capable of responding quickly and efficiently to requests for support from a user. The support service should be able to respond over the phone to calls for support or provide timely on-site assistance if this service has been negotiated between user and supplier.

b) The supplier should be prepared to provide software support services outside normal working hours if there is a specific requirement for this or if analysis of the dependability functions results in a mutual agreement to provide this.

c) The supplier should have a well-specified and proven procedure for receiving problem reports or enhancement requests from the user, generating solutions and implementing the resulting software update on the user's system.

d) Dans la mesure du possible, il est recommandé que le fournisseur donne à l'utilisateur les moyens qui lui permettront d'améliorer la performance de sûreté de fonctionnement en accédant de manière plus efficace aux informations d'exploitation du produit qui lui sont destinées. Comme exemple, on peut citer l'accès par l'utilisateur via Internet ou service d'assistance rapide par retour Fax à un système expert maintenu par le fournisseur.

e) Il est recommandé que le fournisseur enregistre tous les incidents ayant requis une assistance pour l'analyse et le suivi dans le cadre des processus de développement et de maintenance. Si un programme de croissance de fiabilité existe, il est recommandé que les résultats de l'analyse des incidents ayant requis une assistance soient inclus dans ce programme.

f) Il est recommandé que le fournisseur propose un programme complet de formation utilisateur pour l'exploitation du système soit selon les demandes spécifiques de l'utilisateur soit selon l'estimation du fournisseur en ce qui concerne ces exigences. Il est recommandé que le fournisseur propose un suivi de formation utilisateur supplémentaire sur site si les fonctions de sûreté de fonctionnement identifiées et les exigences de performance impliquent des actions critiques du chargé de l'exploitation.

5.5 Processus de maintenance

Le processus de maintenance définit les activités et tâches des personnes chargées de la maintenance du logiciel. Les facteurs d'influence de la sûreté de fonctionnement ont été définis comme étant la fiabilité, la maintenabilité et la logistique de maintenance et, en conséquence, la mise en œuvre correcte des activités et des tâches du processus de maintenance exercent une influence critique sur l'obtention de la sûreté de fonctionnement du logiciel. Les activités de ce processus sont la mise en œuvre du processus, l'analyse des problèmes et des modifications, la mise en œuvre des modifications, la revue et la réception de la maintenance, la migration et le retrait du logiciel.

Chacune de ces activités sera prise en compte dans les paragraphes suivants du point de vue de la sûreté de fonctionnement et l'accent sera mis sur l'importance de la mise en œuvre des activités susceptibles d'être coûteuses et sur l'importance de la vérification de conformité avec toutes les exigences de maintenance identifiées. Compte tenu de leur grande influence sur la sûreté de fonctionnement logicielle, il est important que les coûts des activités du processus de maintenance ne réduisent pas la probabilité qu'elles soient effectuées.

5.5.1 Mise en œuvre du processus

L'activité de mise en œuvre du processus comprend des tâches permettant au chargé de la maintenance de développer, de documenter et d'exécuter les procédures pour effectuer les activités du processus de maintenance décrites dans les paragraphes 5.5.2 à 5.5.6. Il est recommandé que le fournisseur s'assure qu'il y a un jeu de procédures avec leur documentation en place pour recevoir, enregistrer et suivre les rapports de problèmes et les demandes de modification des utilisateurs, et leur fournir un suivi. Il est recommandé que le fournisseur s'assure que les procédures documentées sont mises en œuvre à la fois par l'utilisateur et le fournisseur, dans la mesure où il y a un lien direct entre la disponibilité du système, la sûreté de fonctionnement, un rapport efficace et la correction des problèmes logiciels. Lorsqu'on prend en compte l'aspect sûreté de fonctionnement de cette activité, il est recommandé que les fonctions de sûreté de fonctionnement couvrant ces exigences soient identifiées et vérifiées quant à leur conformité comme partie des essais d'exploitation (voir 5.4.2). Parmi les tâches de mise en œuvre du processus figure la formation des personnes chargées de l'entretien du système pour s'assurer, le cas échéant, qu'elles sont capables de mettre en œuvre les procédures documentées de manière compétente.

d) Where possible, the supplier should provide facilities to the user that will enable him to improve dependability performance by accessing product functional information more efficiently for himself. User access via Internet or Fax back to a knowledge database that is maintained by the supplier is an example of this.

e) The supplier should record all support incidents for analysis and feedback to the development and maintenance processes. Where there is a reliability growth programme, the results of support incident analysis should be included in that programme.

f) The supplier should provide a full programme of user training on system operation either according to specific request from the user or according to the supplier's assessment of the requirements. The supplier should provide further follow-up user training on site if the identified dependability functions and performance requirements involve critical operator actions.

5.5 Maintenance process

The maintenance process defines the activities and tasks of the software maintainer. The influencing factors of dependability have been defined as reliability, maintainability and maintenance support, and, hence, correct implementation of the maintenance process activities and tasks have a critical influence on the achievement of software dependability. The process activities are process implementation, problem and modification analysis, modification implementation, maintenance review/acceptance, migration and software retirement.

Each of these activities will be considered from a dependability point of view in the following subclauses, and emphasis placed on the importance of implementing what are likely to be costly activities and checking for compliance with all identified maintenance requirements. In view of their strong influence on software dependability, it is important that the costly nature of the maintenance process activities does not reduce the likelihood of them being carried out.

5.5.1 Process implementation

The process implementation activity consists of the tasks that enable the maintainer to develop, document and execute procedures for carrying out the activities of the maintenance process described in 5.5.2 to 5.5.6. The supplier should ensure that there is a set of documented procedures in place for receiving, recording and tracking problem reports and modification requests from users and providing feedback to users. The supplier should ensure that the documented procedures are being implemented by both user and supplier as there is a direct connection between system availability and dependability and the efficient reporting and correction of software problems. When considering the dependability aspect of this activity, dependability functions covering these requirements should have been identified and checked for compliance as part of the operational testing (see 5.4.2). Included in the process implementation tasks is training of the system maintainers, where necessary, to ensure that they are able to implement the documented procedures competently.

5.5.2 Analyse des modifications et des problèmes

L'activité d'analyse des modifications et des problèmes consiste à analyser le rapport des problèmes ou les demandes de modification en ce qui concerne leur impact sur le système en relation avec la taille, le coût, le temps de modification et l'effet sur les performances. Lorsqu'on étudie la sûreté de fonctionnement logicielle, il est recommandé de considérer l'impact du rapport des problèmes ou des demandes de modifications sur la performance de sûreté de fonctionnement en fonction de l'impact sur chaque fonction de sûreté de fonctionnement identifiée. Il est recommandé que le fournisseur vérifie la conformité avec les exigences de la fonction de sûreté de fonctionnement d'origine. En cas de conflit entre les résultats de l'analyse et l'obtention de la conformité avec les exigences de la fonction de sûreté de fonctionnement, il est recommandé qu'il y ait un accord et un agrément avant de procéder à la mise en œuvre d'une modification.

Il est recommandé que le chargé de la maintenance établisse une documentation concernant chaque rapport de problèmes ou demande de modification, les résultats de l'analyse et les options de mise en œuvre développées à partir des résultats de l'analyse. Si le développeur a un programme de croissance de la fiabilité, il est recommandé d'inclure les résultats de cette analyse dans ce programme.

5.5.3 Mise en œuvre des modifications

L'activité de mise en œuvre des modifications consiste en une analyse pour déterminer quelle documentation et quels éléments logiciels associés ont besoin d'être modifiés, puis la mise en œuvre des modifications identifiées, l'essai et l'évaluation du logiciel modifié et des éléments de documentation. Il est recommandé que le processus de développement et toutes ses activités associées (voir 5.3) soient utilisés pour produire les éléments logiciels modifiés. Les considérations de sûreté de fonctionnement logicielle sont similaires à celles décrites dans le processus de développement (voir 5.3) en ce sens qu'il est recommandé de considérer les fonctions de sûreté de fonctionnements associées aux éléments logiciels à modifier de la même manière que celle décrite pour chaque activité du processus de développement.

Il est recommandé que l'objectif de la revue soit de déterminer que la conformité avec les exigences de la fonction de sûreté de fonctionnement originelles et toute modification de celles-ci est atteinte. C'est pourquoi il est recommandé que le développeur

a) détermine si l'amélioration demandée ou la modification demandées exige une modification associée des spécifications de la fonction de sûreté de fonctionnement;

b) revoie la conception du système et du logiciel à la lumière de toute modification effectuée sur les spécifications de la fonction de sûreté de fonctionnement;

c) revoie les exigences de sûreté de fonctionnement à la lumière de toute amélioration ou modification demandées;

d) mette en œuvre et essaie toute modification de codage du logiciel en utilisant les procédures et outils établis par le développeur (voir 5.3.7);

e) effectue l'intégration du logiciel, les essais de qualification et d'installation pour vérifier que toutes les fonctions de sûreté de fonctionnement modifiée ou cibles de qualification sont mises en œuvre correctement et qu'aucune fonction de sûreté de fonctionnement non modifiée n'a été affectée.

5.5.4 Revues et réception de la maintenance

L'activité de revues/de réception de la maintenance est effectuée par le chargé de la maintenance pour déterminer l'intégrité du système modifié et pour obtenir l'agrément pour l'achèvement de la modification. Lorsqu'on étudie la sûreté de fonctionnement logiciel, l'estimation de l'intégrité du système se fera en termes de conformité avec à la fois les exigences de la fonction de sûreté de fonctionnement modifiées et non modifiées pendant l'intégration du système, les essais de qualification et d'installation. C'est pourquoi il est

5.5.2 Problem and modification analysis

The problem and modification analysis activity consists of the analysis of the problem report or modification request for its impact on the system in relation to its size, its cost, the time for modification and the effect on performance. When considering software dependability, the impact of the problem report or modification request on dependability performance should be considered by viewing the impact on each of the identified dependability functions. The supplier should check for compliance with the original dependability function requirements. If there is a conflict between the results of the analysis and achieving compliance with dependability function requirements, there should be agreement and approval before proceeding with the implementation of a modification.

The maintainer should document each problem report or modification request, the results of the analysis and the implementation options developed from the analysis results. If the developer has a reliability growth programme, the results of the analysis should be included in that programme.

5.5.3 Modification implementation

The modification implementation activity consists of an analysis to determine which documentation and associated software items need to be modified, followed by implementation of the identified modifications, test and evaluation of the modified software and documentation items. The development process and all its associated activities (see 5.3) should be used to produce the modified software items. The software dependability considerations are similar to those described for the development process (see 5.3) in that the dependability functions associated with the software items to be modified should be considered in a similar manner to that described for each activity of the development process.

The objective of the review should be to determine that the compliance with the original and any revised dependability function requirements has been achieved. The developer should therefore

a) determine whether the requested enhancement or modification requires an associated modification to the dependability function specifications;

b) review the system and software design from the point of view of any modifications made to the dependability function specifications;

c) review the dependability requirement specifications in the light of any requested enhancements or modifications;

d) implement and test any software coding changes using the developer's established procedures and tools (see 5.3.7);

e) carry out software integration, qualification and installation testing to check that any modified dependability functions or qualification targets are correctly implemented and that any unmodified dependability functions have not been affected.

5.5.4 Maintenance review/acceptance

The maintenance review/acceptance activity is carried out by the maintainer to determine the integrity of the modified system and to obtain approval for completion of the modification. When considering software dependability, the assessment of system integrity will be in terms of compliance with both modified and unmodified dependability function requirements during system integration, qualification and installation testing. A review of the integration, qualification and installation test results for dependability function compliance should

recommandé qu'une revue des résultats d'essai d'intégration, de qualification et d'installation pour la conformité à la fonction de sûreté de fonctionnement soit effectuée après achèvement des tâches de mise en œuvre de la modification (voir 5.5.3). Si un niveau de conformité acceptable est atteint, l'agrément attestant que la modification a été réalisée conformément à la spécification du contrat peut être donné au chargé de la maintenance.

5.5.5 Migration

L'activité de migration définit les tâches qu'il est recommandé d'accomplir pour faire migrer un système ou un logiciel (avec les données) d'un environnement d'exploitation ancien vers un nouveau.

Dans le cadre de la sûreté de fonctionnement logicielle, il est recommandé que le chargé de la maintenance tienne compte des implications des tâches de l'activité de migration sur les fonctions de sûreté de fonctionnement.

Des exemples des activités des tâches de migration qu'il convient de considérer sont les suivants.

a) Si un logiciel ou des données sont créés ou modifiés pendant la migration d'un système ou d'un logiciel, il est recommandé que la production et la considération de ses fonctions de sûreté de fonctionnement correspondent à celles décrites pour les activités et tâches définies pour l'analyse des problèmes et modifications (5.5.2), la mise en œuvre des modifications (5.5.3) et les revues/la réception de la maintenance (5.5.4). Il est recommandé que l'objectif global soit de vérifier les résultats d'essai d'intégration, de qualification et d'installation pour la conformité de la fonction de sûreté de fonctionnement.

b) Il est recommandé de développer, d'établir une documentation et d'exécuter un plan de migration. Dans l'analyse des exigences de migration, il est recommandé d'inclure les exigences de la fonction de sûreté de fonctionnement et les spécifications d'exigences de la fonction de sûreté de fonctionnement produites. Il est recommandé que la planification de l'exécution de la migration soit effectuée en coopération avec l'utilisateur s'il existe des exigences spécifiques, en matière de disponibilité du système, à observer pendant la migration.

c) Il est important que l'utilisateur reçoive des informations complètes sur le moment et la raison de la migration et sur le niveau d'assistance pour l'ancien environnement après la migration vers le nouvel environnement. Il est recommandé que le chargé de la maintenance s'assure que l'utilisateur est parfaitement au fait de toute modification dans le niveau de soutien de l'ancien environnement de manière à ce que l'utilisateur puisse estimer les implications possibles sur la disponibilité du système s'il ne migre pas vers le nouvel environnement et s'il y a une modification dans la fonction de logistique de maintenance offerte par le chargé de la maintenance.

5.5.6 Retrait du logiciel

L'activité de retrait du logiciel définit les tâches qu'il est recommandé d'effectuer si un système ou un logiciel doit être retiré de l'assistance active par les organismes d'exploitation et de maintenance à la demande du propriétaire du logiciel. Un des facteurs les plus importants de sûreté de fonctionnement est la logistique de maintenance. C'est pourquoi il est recommandé que les organismes d'exploitation et de maintenance tiennent compte des implications du retrait de l'assistance active sur les exigences de la fonction de sûreté de fonctionnement logicielle.

Il est recommandé de développer un plan avec la documentation afférente pour le retrait de l'assistance active des organismes d'exploitation et de maintenance. Il est recommandé que le calendrier de ce retrait fasse l'objet d'un accord entre l'utilisateur et le chargé de la maintenance de manière à ce que les fonctions de logistique de maintenance spécifiées soient maintenues jusqu'au retrait du logiciel ou, selon le cas, jusqu'au moment où l'utilisateur aura migré vers un logiciel de remplacement. Il est recommandé que l'utilisateur inclue l'archivage du logiciel retiré, de la documentation et des données dans le plan de retrait.