

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60880

Deuxième édition
Second edition
2006-05

**Centrales nucléaires de puissance –
Instrumentation et contrôle-commande
importants pour la sûreté –
Aspects logiciels des systèmes programmés
réalisant des fonctions de catégorie A**

**Nuclear power plants –
Instrumentation and control systems
important to safety –
Software aspects for computer-based
systems performing category A functions**



Numéro de référence
Reference number
CEI/IEC 60880:2006

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions 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.

Informations supplémentaires sur les publications de la CEI

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 cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- Site web de la CEI (www.iec.ch)
- Catalogue des publications de la CEI

Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- IEC Just Published

Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- Service clients

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. 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.

Further information on IEC publications

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 this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. 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 also available from the following:

- IEC Web Site (www.iec.ch)
- Catalogue of IEC publications

The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- IEC Just Published

This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- Customer Service Centre

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60880

Deuxième édition
Second edition
2006-05

**Centrales nucléaires de puissance –
Instrumentation et contrôle-commande
importants pour la sûreté –
Aspects logiciels des systèmes programmés
réalisant des fonctions de catégorie A**

**Nuclear power plants –
Instrumentation and control systems
important to safety –
Software aspects for computer-based
systems performing category A functions**

© IEC 2006 Droits de reproduction réservés — Copyright - all rights reserved

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

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

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE **XE**

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

SOMMAIRE

AVANT-PROPOS.....	6
INTRODUCTION.....	10
1 Domaine d'application et objet.....	16
2 Références normatives.....	16
3 Termes et définitions.....	18
4 Symboles et abréviations.....	28
5 Exigences générales pour les projets logiciel.....	28
5.1 Généralités.....	28
5.2 Types de logiciel.....	32
5.3 Principe de développement du logiciel.....	34
5.4 Gestion du projet logiciel.....	38
5.5 Plan d'assurance qualité logiciel.....	38
5.6 Gestion de configuration.....	40
5.7 Sécurité du logiciel.....	42
6 Exigences du logiciel.....	46
6.1 Spécification des exigences du logiciel.....	46
6.2 Auto-surveillance.....	48
6.3 Test périodique.....	48
6.4 Documentation.....	50
7 Conception et réalisation.....	50
7.1 Principes pour la conception et la réalisation.....	52
7.2 Langages, traducteurs et outils associés.....	56
7.3 Recommandations détaillées.....	58
7.4 Documentation.....	62
8 Vérification du logiciel.....	62
8.1 Processus de vérification du logiciel.....	62
8.2 Activités de vérification du logiciel.....	64
9 Aspects logiciels de l'intégration du système.....	72
9.1 Aspects logiciels du plan d'intégration du système.....	74
9.2 Intégration du système.....	76
9.3 Vérification du système intégré.....	76
9.4 Procédures de résolution de défaut.....	78
9.5 Aspects logiciels du compte rendu de vérification du système intégré.....	78
10 Aspects logiciels du plan de validation.....	80
10.1 Aspects logiciels du plan de validation système.....	80
10.2 Validation du système.....	80
10.3 Aspects logiciels du compte rendu de validation du système.....	82
10.4 Procédures de résolution de défaut.....	82
11 Modification du logiciel.....	82
11.1 Procédure de demande de modification.....	84
11.2 Procédure d'exécution d'une modification du logiciel.....	86
11.3 Modification du logiciel après livraison.....	88

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	11
1 Scope and object.....	17
2 Normative references	17
3 Terms and definitions	19
4 Symbols and abbreviations.....	29
5 General requirements for software projects	29
5.1 General.....	29
5.2 Software types	33
5.3 Software development approach	35
5.4 Software project management	39
5.5 Software quality assurance plan.....	39
5.6 Configuration management.....	41
5.7 Software security.....	43
6 Software requirements.....	47
6.1 Specification of software requirements	47
6.2 Self-supervision	49
6.3 Periodic testing	49
6.4 Documentation	51
7 Design and implementation	51
7.1 Principles for design and implementation	53
7.2 Language and associated translators and tools	57
7.3 Detailed recommendations	59
7.4 Documentation	63
8 Software Verification	63
8.1 Software verification process.....	63
8.2 Software verification activities	65
9 Software aspects of system integration.....	73
9.1 Software aspects of system integration plan.....	75
9.2 System integration	77
9.3 Integrated system verification.....	77
9.4 Fault resolution procedures	79
9.5 Software aspects of integrated system verification report	79
10 Software aspects of system validation	81
10.1 Software aspects of the system validation plan.....	81
10.2 System validation	81
10.3 Software aspects of the system validation report.....	83
10.4 Fault resolution procedures	83
11 Software modification	83
11.1 Modification request procedure	85
11.2 Procedure for executing a software modification.....	87
11.3 Software modification after delivery.....	89

12	Aspects logiciels de l'installation et de l'exploitation	90
12.1	Installation du logiciel sur site	90
12.2	Sécurité informatique sur site	90
12.3	Adaptation du logiciel aux conditions sur site	92
12.4	Formation des opérateurs.....	92
13	Moyens de défense contre les défaillances logicielles de cause commune	94
13.1	Généralités.....	94
13.2	Conception du logiciel pour éviter les CCF	96
13.3	Sources et effets des CCF logicielles	96
13.4	Mise en oeuvre de la diversité	98
13.5	Pondération des inconvénients et des avantages liés à l'utilisation de la diversité	98
14	Outils logiciels pour le développement de logiciels	98
14.1	Généralités.....	98
14.2	Sélection des outils	100
14.3	Exigences applicables aux outils	102
15	Qualification de logiciels prédéveloppés	112
15.1	Généralités.....	112
15.2	Exigences générales	112
15.3	Processus d'évaluation et d'agrément	114
15.4	Exigences liées à l'intégration dans le système et à la maintenance des PDS	130
	Annexe A (normative) Cycle de vie et de sûreté du logiciel et détails des exigences du logiciel	132
	Annexe B (normative) Exigences et recommandations détaillées relatives à la conception et à la réalisation	136
	Annexe C (informative) Exemple d'ingénierie à base de logiciel orienté application (développement de logiciel avec un langage orienté application)	162
	Annexe D (informative) Langage, traducteur, éditeur de liens	170
	Annexe E (informative) Vérification et test du logiciel.....	174
	Annexe F (informative) Liste typique des documents relatifs au logiciel	190
	Annexe G (informative) Considérations sur les CCF et la diversification	192
	Annexe H (informative) Outils pour la production et la vérification des spécifications, de la conception et du code	200
	Annexe I (informative) Exigences concernant les logiciels prédéveloppés (PDS)	206
	Annexe J (informative) Correspondance entre la CEI 61513 et cette norme	210

12	Software aspects of installation and operation	91
12.1	On-site installation of the software	91
12.2	On-site software security	91
12.3	Adaptation of the software to on-site conditions	93
12.4	Operator training	93
13	Defences against common cause failure due to software	95
13.1	General	95
13.2	Design of software against CCF	97
13.3	Sources and effects of CCF due to software	97
13.4	Implementation of diversity	99
13.5	Balance of drawbacks and benefits connected with the use of diversity	99
14	Software tools for the development of software	99
14.1	Introduction	99
14.2	Selection of tools	101
14.3	Requirements for tools	103
15	Qualification of pre-developed software	113
15.1	General	113
15.2	General requirements	113
15.3	Evaluation and assessment process	115
15.4	Requirements for integration in the system and modification of PDS	131
	Annex A (normative) Software safety life cycle and details of software requirements	133
	Annex B (normative) Detailed requirements and recommendations for design and implementation	137
	Annex C (informative) Example of application oriented software engineering (software development with application-oriented language)	163
	Annex D (informative) Language, translator, linkage editor	171
	Annex E (informative) Software verification and testing	175
	Annex F (informative) Typical list of software documentation	191
	Annex G (informative) Considerations of CCF and diversity	193
	Annex H (informative) Tools for production and checking of specification, design and implementation	201
	Annex I (informative) Requirements concerning pre-developed software (PDS)	207
	Annex J (informative) Correspondence between IEC 61513 and this standard	211

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ASPECTS LOGICIELS DES SYSTÈMES PROGRAMMÉS RÉALISANT DES FONCTIONS DE CATÉGORIE A

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (CEI) 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, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). 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 de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI 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 60880 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition publiée en 1986 ainsi que la CEI 60880-2 publiée en 2000. Elle constitue une révision technique.

L'objectif de la révision de la norme est de:

- Prendre en compte le fait que les techniques de génie logiciel ont progressé de façon significative ces dernières années.
- Mettre en cohérence la norme avec les nouvelles révisions des documents de l'AIEA NS-R-1 et NS-G-1.3, ceci comprenant autant que possible une adaptation des définitions.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY A FUNCTIONS

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 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 IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60880 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1986 and IEC 60880-2 published in 2000. It constitutes a technical revision.

The revision of the standard is intended to accomplish the following:

- To take into account the fact that software engineering techniques advanced significantly in the intervening years.
- To align the standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3. This includes as far as possible adaptation of the definitions.

- Remplacer, autant que possible, les exigences associées aux normes publiées depuis la parution de la première édition de la CEI 60880, plus particulièrement la CEI 61513, la CEI 61226 édition 2, la CEI 62138 et la CEI 60987.
- Intégrer complètement au niveau des chapitres 13, 14, 15 et des Annexes G, H, I, la CEI 60880-2 publiée en 2000.
- Faire la revue des exigences existantes et mettre à jour les définitions et la terminologie.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/613/FDIS	45A/621/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 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «<http://webstore.iec.ch>» dans les données relatives à la publication recherchée. A cette date, la publication sera

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

- To replace, as far as possible, requirements associated with standards published since the first edition of IEC 60880, especially IEC 61513, IEC 61226 edition 2, IEC 62138 and IEC 60987.
- To fully integrate IEC 60880-2 published in 2000 as chapters 13, 14, 15 and annexes G, H, I.
- To review the existing requirements and to update the terminology and definitions.

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

FDIS	Report on voting
45A/613/FDIS	45A/621/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 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

INTRODUCTION

a) Contexte technique, questions importantes et structure du document

Le développement des logiciels des systèmes de contrôle-commande numériques employés à des fins de sûreté nucléaire est un défi du fait des exigences de sûreté à satisfaire. Les logiciels de sûreté employés dans les centrales nucléaires, qui, souvent, ne sont sollicités qu'en cas d'urgence doivent être totalement validés et qualifiés avant leur mise en exploitation. Afin d'atteindre le haut niveau de fiabilité requis, une attention particulière doit être apportée durant tout le cycle de vie, depuis la spécification des exigences de base jusqu'à l'exploitation et la maintenance, en passant par les différentes étapes de conception et de V&V. L'objectif principal de cette norme est de traiter des différents aspects de sûreté correspondants et d'énoncer les exigences permettant d'atteindre le haut niveau de qualité logicielle nécessaire.

La première édition de cette norme, publiée en 1986, avait été développée pour interpréter les principes de sûreté de base jusqu'alors applicables aux systèmes câblés, pour les systèmes numériques – systèmes multiprocesseurs répartis, grands systèmes mono-processeurs – employés dans les systèmes de sûreté des centrales nucléaires.

Elle fut largement utilisée par l'industrie nucléaire pour fournir des exigences et des recommandations applicables aux logiciels des systèmes de contrôle commande des centrales nucléaires.

Bien que la plupart des exigences de cette première édition soient toujours pertinentes, des éléments significatifs ont justifié le développement de cette seconde édition:

- Depuis 1986 un certain nombre de nouvelles normes ont été produites; celles-ci traitent en détail des exigences générales portant sur les systèmes (CEI 61513) et des exigences relatives au matériel (CEI 60987). Une norme traite du logiciel des systèmes de contrôle-commande réalisant des fonctions de catégories B ou C pour les systèmes importants pour la sûreté des centrales nucléaires (CEI 62138). Le Guide de sûreté de l'AIEA 50-SG-D3 a été remplacé par le guide NS-G-1.3. Enfin, la CEI 60880-2 a été diffusée.
- Les techniques de génie logiciel ont progressé de façon significative au cours des dernières années.

Lors du développement de cette norme, le plus grand soin a été apporté au maintien de la transparence par rapport à la première édition. Lorsque cela a été possible, la formulation des exigences a été conservée, sinon elle a été modifiée tout en maintenant la traçabilité. De la même façon, la CEI 60880-2 traitant des aspects logiciels relatifs à la défense contre les défaillances de cause commune, à l'utilisation des d'outils logiciels et de logiciels prédéveloppés, a été intégrée de telle façon que la présente norme couvre aujourd'hui la totalité des sujets considérés.

L'objectif de cette norme est d'être utilisée par les développeurs de systèmes, les acheteurs et les utilisateurs de systèmes (exploitants), les évaluateurs de systèmes et autorités réglementaires.

b) Position de la présente norme dans la collection de normes du SC 45A

La CEI 61513, qui traite des systèmes de contrôle-commande numériques de haute intégrité employés dans les systèmes de sûreté des centrales nucléaires de puissance fait référence à la CEI 60880.

La CEI 60880 est le document de deuxième niveau qui traite les aspects logiciels des systèmes de contrôle-commande réalisant des fonctions de catégorie A.

INTRODUCTION

a) Technical background, main issues and organisation of the standard

Engineering of software based Instrumentation and Control (I&C) systems to be used for nuclear safety purposes is a challenge due to the safety requirements to be fulfilled. The safety software used in nuclear power plants (NPP) which are often required only in emergency cases, have to be fully validated and qualified before being used in operation. In order to achieve the high reliability required, special care has to be taken throughout the entire life cycle, from the basic requirements, the various design phases and V&V procedures for operation and maintenance. It is the main aim of this standard to address the related safety aspects and to provide requirements for achieving the high software quality necessary.

The first edition of this standard was issued in 1986 to interpret the basic safety principles applied so far in hardwired systems for the utilisation of digital systems — multiprocessor distributed systems as well as larger scale central processor systems — in the safety systems of nuclear power plants.

It has been used extensively within the nuclear industry to provide requirements and guidance for software of NPP safety I&C systems.

Although many of the requirements within the first edition continued to be relevant, there were significant factors which justified the development of this second edition:

- Since 1986, a number of new standards have been produced which address in detail the general requirements for systems (IEC 61513), hardware requirements (IEC 60987) and a standard to address software for I&C systems performing category B or C functions for NPP systems important to safety (IEC 62138). The Safety Guide 50-SG-D3 of the IAEA has been superseded by the guide NS-G-1.3. Additionally, IEC 60880-2 has been issued.
- Software engineering techniques have advanced significantly in the intervening years.

In this standard, utmost care has been taken to keep transparency with respect to the first edition. Where possible, the phrasing of requirements has been kept, otherwise it has been extended in a traceable way. In the same manner, IEC 60880-2 dealing with software aspects of defence against common cause failures, use of software tools and pre-developed software has been integrated, so that now this current standard covers entirely the software safety issues to be addressed.

It is intended that the standard be used by systems developers, systems purchasers/users (utilities), systems assessors and by licensors.

b) Situation of the current standard in the structure of the SC 45A standard series

IEC 60880 is directly referenced by IEC 61513 which deals with the system aspects of high integrity computer-based I&C used in safety systems of nuclear power plants together.

IEC 60880 is the second level SC 45A document tackling the issue of software aspects for I&C systems performing category A functions.

Le logiciel relatif aux fonctions de catégories B et C est traité dans la CEI 62138.

Prises ensemble, la CEI 60880 et la CEI 62138 couvrent les aspects logiciels relatifs aux systèmes numériques employés dans les centrales nucléaires de puissance pour réaliser les fonctions importantes pour la sûreté.

Cette seconde édition de la CEI 60880 doit être lue conjointement avec la CEI 60987 et la CEI 61226, qui sont les normes du SC 45A traitant des aspects matériels et du classement des systèmes.

Pour plus de détails sur la collection de normes du SC 45A, voir le point d) de cette introduction.

c) Recommandations et limites relatives à l'application de cette norme

Il est important de noter que cette norme n'établit pas d'exigences fonctionnelles supplémentaires pour les systèmes de sûreté.

Les aspects pour lesquels des exigences et des recommandations particulières ont été produites sont:

- 1) une approche générale du développement logiciel pour garantir une production de logiciel hautement fiable prenant en compte les interdépendances entre le matériel et le logiciel;
- 2) une approche générale pour la vérification du logiciel et pour les aspects logiciels de la validation du système programmé;
- 3) des procédures pour le contrôle des modifications et des configurations du logiciel;
- 4) des exigences applicables à l'utilisation des outils;
- 5) des procédures pour la qualification des logiciels prédéveloppés.

Il est reconnu que les techniques logicielles se développent de façon continue à un rythme soutenu et qu'il n'est pas possible, pour une norme, de faire référence à toutes les techniques et technologies nouvelles de conception.

Pour garantir la pertinence de la norme pour les années futures, l'accent a été mis sur les principes, plutôt que sur les techniques logicielles.

Si de nouvelles techniques sont développées, l'application des principes devrait permettre d'en apprécier l'utilité.

d) Description de la structure de la collection des normes du SC 45A et relations avec d'autres documents de la CEI et d'autres organisations (AIEA, ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A est la CEI 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A.

La CEI 61513 fait directement référence aux autres normes du SC 45A traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la CEI 61513, un ensemble documentaire cohérent.

Software for categories B and C functions is dealt with in IEC 62138.

IEC 60880 and IEC 62138 together cover the domain of the software aspects of computer-based systems used in nuclear power plants to perform functions important to safety.

This second edition of IEC 60880 is to be read in conjunction with IEC 60987 and IEC 61226, the appropriate SC 45A standards on computer hardware and on classification.

For more details on the structure of the SC 45A standard series see item d) of this introduction.

c) Recommendation and limitation regarding the application of this standard

It is important to note that this standard establishes no additional functional requirements for safety systems.

Aspects for which special requirements and recommendations have been produced, are:

- 1) a general approach to software development to assure the production of the highly reliable software required including hardware and software interdependencies;
- 2) a general approach to software verification and to the software aspects of the computer-based system validation;
- 3) procedures for software modification and configuration control;
- 4) requirements for use of tools;
- 5) procedures for qualification of pre-developed software.

It is recognised that software technology is continuing to develop at a rapid pace and that it is not possible for a standard such as this to include references to all modern design technologies and techniques.

To ensure that the standard will continue to be relevant in future years the emphasis has been placed on issues of principle, rather than specific software technologies.

If new techniques are developed then it should be possible to assess the suitability of such techniques by applying the safety principles contained within this standard.

d) Description of the structure of the SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top level document of the SC 45A standard series is IEC 61513. This standard deals with requirements for NPP I&C systems important to safety and lays out the SC 45A standards series.

IEC 61513 refers directly to other SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

Au troisième niveau, les normes du SC 45A, qui ne sont généralement pas référencées directement par la CEI 61513, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent, pour l'application au secteur nucléaire, à la CEI 61508-3.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier le guide NS-R-1 «Safety of Nuclear Power Plants: Design – Requirements» et le guide NS-G-1.3 «Instrumentation and Control Systems Important to Safety in Nuclear Power Plants». La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

At a third level, SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods or specific activities. Usually these documents, which make reference to second level documents for general topics, can be used on their own.

A fourth level extending the SC 45A standard series corresponds to the technical reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508 parts 1, 2 and 4, for the nuclear application sector. Compliance with this standard will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508, part 3 for the nuclear application sector.

IEC 61513 refers to ISO standards as well as to IAEA 50-C-QA for topics related to quality assurance.

The SC 45A standards series consistently implement and detail the principles and basic safety aspects provided in the IAEA Code on the safety of nuclear power plants and in the IAEA safety series, in particular the Requirements NS-R-1, "Safety of Nuclear Power Plants: Design" and the Safety Guide NS-G-1.3, "Instrumentation and control systems important to safety in Nuclear Power Plants". The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTES POUR LA SÛRETÉ – ASPECTS LOGICIELS DES SYSTÈMES PROGRAMMÉS RÉALISANT DES FONCTIONS DE CATÉGORIE A

1 Domaine d'application et objet

Cette Norme internationale énonce des exigences pour les logiciels des systèmes d'instrumentation et de contrôle-commande (I&C) programmés des centrales nucléaires de puissance, réalisant des fonctions de catégorie A telle que définie par la CEI 61226.

Selon la définition donnée par la CEI 61513, les systèmes d'I&C de sûreté de classe 1 sont, à la base, destinés aux fonctions de catégorie A, mais peuvent également réaliser des fonctions de catégories inférieures. Cependant, les exigences des systèmes sont toujours déterminées par les fonctions de la plus haute catégorie concernée.

Pour les logiciels des systèmes d'I&C réalisant uniquement des fonctions de catégories B et C, telles que définies par la CEI 61226, les exigences et recommandations de la CEI 62138 sont applicables.

La présente norme énonce des exigences pour la production de logiciels de haute fiabilité. Elle prend en compte chaque étape de développement et de documentation du logiciel, c'est-à-dire la spécification des exigences, la conception, le développement, la vérification, la validation et l'exploitation.

Les principes appliqués pour développer ces exigences comprennent:

- l'utilisation des meilleures pratiques existantes;
- l'utilisation de méthodes de conception descendante;
- la modularité;
- la vérification de chaque phase;
- la clarté de la documentation;
- la vérifiabilité des documents;
- la réalisation de tests de validation.

Des recommandations et informations supplémentaires sur la façon de se conformer aux exigences de la partie principale de cette norme sont données dans les Annexes A à I.

2 Références normatives

Les documents référencés ci-après sont indispensables à l'application de cette norme. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document référencé (y compris les amendements) s'applique.

CEI 60671, *Essais périodiques et surveillance du système de protection des réacteurs nucléaires*

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope and object

This International Standard provides requirements for the software of computer-based I&C systems of nuclear power plants performing functions of safety category A as defined by IEC 61226.

According to the definition in IEC 61513, I&C systems of safety class 1 are basically intended to support category A functions, but may also support functions of lower categories. However the system requirements are always determined by the functions of the highest category implemented.

For software of I&C system performing only category B and C functions in NPP as defined by IEC 61226, requirements and guidance of IEC 62138 are applicable.

This standard provides requirements for the purpose of achieving highly reliable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation.

The principles applied in developing these requirements include:

- best available practices;
- top-down design methods;
- modularity;
- verification of each phase;
- clear documentation;
- auditable documents;
- validation testing.

Additional guidance and information on how to comply with the requirements of the main part of this standard is given in Annexes A to I.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60671, *Periodic tests and monitoring of the protection system of nuclear reactors*

CEI 61069-2:1993, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 2: Méthodologie à appliquer pour l'évaluation*

CEI 61226, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

CEI 61508-4, *Sécurité fonctionnelle des systèmes électriques/électroniques/programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61513, *Centrales nucléaires – Instrumentation et contrôle-commande des systèmes importants pour la sûreté – Exigences générales pour les systèmes*

ISO/CEI 9126, *Génie logiciel – Qualité du produit*

Guide AIEA NS-G-1.2, *Evaluation de sûreté et vérification pour les centrales nucléaires*

Guide AIEA NS-G-1.3, *Instrumentation et systèmes de commande importants pour la sûreté dans les centrales nucléaires*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1

animation

processus par lequel le comportement défini par une spécification est visualisé avec ses valeurs effectives dérivées des équations de comportement et des valeurs d'entrée

3.2

fonction d'application

fonction d'un système d'I&C qui accomplit une tâche relative au processus sous contrôle plutôt qu'au fonctionnement du système lui-même

[CEI 61513, 3.1]

3.3

langage orienté application

langage informatique spécifiquement conçu pour un certain type d'application et pour être utilisé par les spécialistes de ce type d'application

[CEI 62138, 3.3]

NOTE 1 Les familles d'équipements offrent en général des langages orientés application de façon à faciliter l'adaptation des équipements à des exigences particulières.

NOTE 2 Les langages orientés application peuvent être utilisés pour la spécification d'exigences fonctionnelles que doit satisfaire un système d'I&C, et/ou pour spécifier ou concevoir le logiciel d'application. Ils peuvent être basés sur du texte, des diagrammes ou une combinaison des deux.

NOTE 3 Exemples: les langages à blocs fonctionnels, les langages définis par la CEI 61131-3.

3.4

logiciel d'application

partie du logiciel d'un système d'I&C qui exécute des fonctions d'application

[CEI 61513, 3.2]

IEC 61069-2:1993, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

IEC 61226, *Nuclear power plants – Instrumentation and control systems important for safety – Classification of instrumentation and control functions*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

ISO/IEC 9126, *Software engineering – Product quality*

IAEA guide NS-G-1.2, *Safety Assessment and Verification for Nuclear power Plant*

IAEA guide NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

animation

process by which the behaviour defined by a specification is displayed with actual values derived from the stated behaviour expressions and from some input values

3.2

application function

function of an I&C system that performs a task related to the process being controlled rather than to the functioning of the system itself

[IEC 61513, 3.1]

3.3

application-oriented language

computer language specifically designed to address a certain type of application and to be used by persons who are specialists of this type of application

[IEC 62138, 3.3]

NOTE 1 Equipment families usually feature application-oriented languages so as to provide easy to use capability for adjusting the equipment to specific requirements.

NOTE 2 Application-oriented languages may be used to specify the functional requirements of an I&C system, and/or to specify or design application software. They may be based on texts, on graphics, or on both.

NOTE 3 Examples: function block diagram languages, language defined by IEC 61131-3.

3.4

application software

part of the software of an I&C system that implements the application functions

[IEC 61513, 3.2]

3.5

génération automatique de code

fonction d'outils automatiques permettant une transformation du langage orienté application en un langage de programmation généraliste apte à une compilation en format exécutable

3.6

canal

ensemble de composants interconnectés dans un système générant un signal de sortie unique. Un canal perd son identité lorsque plusieurs signaux de ce type sont combinés avec des signaux provenant d'autres canaux, tels que les canaux de surveillance ou les canaux des actionneurs de sûreté

[AIEA NS-G-1.3, Glossaire]

3.7

compactage de code

réduction voulue de l'espace mémoire nécessaire à un programme, obtenue par élimination des instructions redondantes ou sans rapport avec ledit programme

3.8

défaillance de cause commune (CCF)

défaillance de deux ou plusieurs structures, systèmes ou composants due à un seul événement ou cause spécifique

[AIEA NS-G-1.3, Glossaire]

3.9

ordinateur

unité fonctionnelle programmable se composant d'une ou plusieurs unités de traitement associées et de périphériques, qui est commandée par des programmes rangés en mémoire interne et qui peut effectuer des traitements importants, comportant de nombreuses opérations arithmétiques ou logiques, sans intervention humaine pendant l'exécution

[ISO 2382/1]

NOTE Un ordinateur peut être composé d'une unité isolée ou de plusieurs unités interconnectées.

3.10

programme (d'ordinateur)

ensemble ordonné d'instructions et de données qui spécifie des opérations sous une forme adaptée à l'exécution par un ordinateur

3.11

système informatique

système d'I&C dont les fonctions dépendent en grande partie ou sont totalement effectuées à l'aide de microprocesseurs, d'un matériel électronique programmé ou d'ordinateurs

[CEI 61513, 3.10]

NOTE Équivalent à: système numérique, système programmé.

3.12

données

représentation d'informations ou d'instructions adaptée à la communication, l'interprétation, ou le traitement au moyen d'un ordinateur

[IEEE 610, modifiée]

NOTE Les données qui sont nécessaires pour définir des paramètres et initier des fonctions d'application et de service dans le système, sont appelées «données d'application».

3.5**automated code generation**

function of automated tools allowing transformation of the application-oriented language into a form suitable for compilation or execution

3.6**channel**

arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where single output signals are combined with signals from other channels, e.g., from a monitoring channel, or a safety actuation channel.

[IAEA NS-G-1.3, Glossary]

3.7**code compaction**

purposeful reduction in memory size required for a program by the elimination of redundant or extraneous instructions

3.8**common cause failure (CCF)**

failure of two or more structures, systems or components due to a single specific event or cause

[IAEA NS-G-1.3, Glossary]

3.9**computer**

programmable functional unit that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs and that can perform substantial computation, including numerous arithmetic operations or logic operations, without human intervention during a run

[ISO 2382/1]

NOTE A computer may be a standalone unit or may consist of several interconnected units.

3.10**computer program**

set of ordered instructions and data that specify operations in a form suitable for execution by a computer

3.11**computer-based system**

I&C system whose functions are mostly dependent on, or completely performed by using microprocessors, programmed electronic equipment or computers

[IEC 61513, 3.10]

NOTE Equivalent to: digital systems, software-based system, programmed system.

3.12**data**

presentation of information or instructions in a manner suitable for communication, interpretation, or processing by computers

[IEEE 610, modified]

NOTE Data which are required to define parameters and to instantiate application and service functions in the system are called "application data".

3.13

défense en profondeur

mise en œuvre de plusieurs mesures de protections en vue d'un même objectif de sûreté, de façon à atteindre l'objectif même en cas d'échec d'une des mesures

[AIEA Safety Glossary]

3.14

diversité

existence de deux ou plusieurs manières différentes d'atteindre un objectif donné. La diversité est en particulier utilisée comme moyen de défense contre une défaillance de cause commune. Elle peut être réalisée par la mise en œuvre de systèmes physiquement différents les uns des autres, ou par une diversité fonctionnelle dans laquelle des systèmes similaires réalisent l'objectif spécifié de manière différente

3.15

analyse dynamique

processus consistant à évaluer un système ou un composant sur la base de son comportement pendant l'exécution. S'oppose à l'analyse statique

[IEEE 610]

3.16

défaillance

déviations du service délivré par rapport au service attendu

[CEI 61513, 3.21, modifiée]

3.17

défaut

imperfection dans un composant matériel, logiciel ou système

[CEI 61513, 3.22]

3.18

tolérance aux fautes

capacité intrinsèque d'un système de fonctionner correctement de manière continue en présence d'un nombre limité de défauts matériels ou logiciels

3.19

diversité fonctionnelle

application de la diversité au niveau fonctionnel (par exemple le déclenchement d'une action de protection sur seuil de pression ou sur seuil de température)

3.20

langage généraliste

langage informatique conçu pour s'adresser à tout type de besoin

[CEI 62138, 3.17]

NOTE 1 Le logiciel système d'une famille d'équipements est en général réalisé à l'aide de langages généralistes.

NOTE 2 Exemples: Ada, C, Pascal.

3.21

erreur humaine

action humaine conduisant à un résultat indésirable

3.22

initialiser

forcer les compteurs, clés, adresses ou contenus des dispositifs de stockage à zéro ou à des valeurs prédéterminées au début ou en certains points prescrits du fonctionnement d'un programme

3.13**defence in depth**

application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails

[IAEA Safety Glossary]

3.14**diversity**

existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common cause failure. It may be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

3.15**dynamic analysis**

process of evaluating a system or component based on its behaviour during execution. In contrast to static analysis

[IEEE 610]

3.16**failure**

deviation of the delivered service from the intended one

[IEC 61513, 3.21, modified]

3.17**fault**

defect in a hardware, software or system component

[IEC 61513, 3.22]

3.18**fault tolerance**

built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults

3.19**functional diversity**

application of the diversity at the functional level (for example, to have trip activation on both pressure and temperature limit)

3.20**general-purpose language**

computer language designed to address all types of usage

[IEC 62138, 3.17]

NOTE 1 The operational system software of equipment families is usually implemented using general-purpose languages.

NOTE 2 Examples: Ada, C, Pascal.

3.21**human error**

human action that produces an unintended result

3.22**initialise**

to set counters, switches, addresses, or contents of storage devices to zero or other starting values at the beginning of, or at prescribed points in, the operation of a computer program

3.23

tests d'intégration

tests effectués lors du processus d'intégration du matériel et du logiciel avant la phase de validation du système programmé, pour vérifier la compatibilité du logiciel et du matériel du système programmé

3.24

bibliothèque

ensemble d'éléments logiciels connexes contenus dans un fichier unique mais sélectionnés individuellement pour inclusion dans le produit logiciel final

3.25

logiciel N-versions

ensemble de programmes différents, appelés versions, développés pour répondre à des exigences identiques et aux mêmes tests d'acceptation. L'exécution simultanée et indépendante de ces versions a lieu en général sur des matériels redondants. On utilise des entrées identiques dans les systèmes de test ou des entrées correspondantes dans des systèmes redondants. Une stratégie prédéterminée telle que le vote est utilisée pour choisir en cas de sorties contradictoires générées par les différentes versions

3.26

logiciel système opérationnel

logiciel fonctionnant sur le processeur cible en exploitation, comme des pilotes et services d'entrée/sortie, la gestion des interruptions, la gestion de l'ordonnancement, des pilotes de communication, des bibliothèques orientées application, le diagnostic en ligne, la redondance et la gestion des modes de fonctionnement dégradé

3.27

événement initiateur hypothétique

PIE

événement engendrant des incidents opérationnels prévus ou des situations accidentelles, ainsi que les effets de défaillances produites

[CEI 61513, 3.41]

3.28

logiciel prédéveloppé (PDS)

logiciel qui existe déjà, qui peut ou non être un produit commercial, et dont l'utilisation est envisagée

[CEI 62138, 3.24, modifiée]

3.29

redondance

présence de structures, de systèmes ou de composants supplémentaires (identiques ou différents), tels que chacun d'entre eux puisse remplir la fonction requise quel que soit l'état de fonctionnement ou de défaillance des autres

[AIEA NS-G-1.3, Glossaire]

3.30

contrôle d'accès «basé fonction»

contrôle d'accès basé sur des règles définissant les droits d'accès des utilisateurs aux objets (fonctions, données) sur la base de groupes d'utilisateurs assurant une fonction identique et non pas sur la base d'utilisateurs individuels

3.23**integration tests**

tests performed during the hardware/software integration process prior to computer-based system validation to verify compatibility of the software and the computer hardware

3.24**library**

collection of related software elements that are grouped together, but which are individually selected for inclusion in the final software product

3.25**N-version software**

set of different programs, known as versions, developed to meet a common requirement and common acceptance test. Concurrent and independent execution of these versions takes place, generally in redundant hardware. Identical inputs in test systems or corresponding inputs in redundant systems are used. A predetermined strategy such as voting is used to decide between conflicting outputs in different versions.

3.26**operational system software**

software running on the target processor during operation, such as: input/output drivers and services, interrupt management, scheduler, communication drivers, applications oriented libraries, on-line diagnostic, redundancy and graceful degradation management

3.27**postulated initiating event****PIE**

events that lead to anticipated operational occurrences or accident conditions and their consequential failure effects

[IEC 61513, 3.41]

3.28**pre-developed software****PDS**

software part that already exists, is available as a commercial or proprietary product, and is being considered for use

[IEC 62138, 3.24, modified]

3.29**redundancy**

provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other

[IAEA NS-G-1.3, Glossary]

3.30**role-based access control**

access control based on rules, defining the permitted access of users to objects (functions, data) on the basis of user groups with an identical role instead of individual users

3.31

fonction de sûreté

objectif particulier à satisfaire pour la sûreté

[AIEA NS-R-1, Glossaire]

3.32

système de sûreté

système important pour la sûreté assurant l'arrêt sûr du réacteur, ou l'évacuation de la chaleur résiduelle du cœur, ou la limitation des conséquences des incidents opérationnels prévus et des incidents de dimensionnement

[AIEA NS-R-1, Glossaire]

3.33

trajectoire de signal

historique de toutes les conditions des équipements, des états internes, des signaux d'entrée, et des entrées opérateur qui déterminent les valeurs de sortie d'un système

3.34

logiciel

programmes (ensembles ordonnés d'instructions), données, règles et toute documentation associée relatifs au fonctionnement d'un système informatique

[CEI 62138, 3.27]

3.35

développement logiciel

phase du cycle de vie du logiciel conduisant à la création du logiciel d'un système d'I&C ou d'un produit logiciel. Cette phase couvre toutes les activités, depuis la spécification d'exigences jusqu'à la validation et l'installation sur site

[CEI 62138, 3.30]

3.36

modification du logiciel

changement dans un document ou des documents déjà approuvés conduisant à un changement dans le code exécutable

NOTE Une modification du logiciel peut être effectuée durant le développement initial (par exemple pour éliminer des défauts mis en évidence dans les phases finales du développement) ou après la mise en service du logiciel.

3.37

cycle de vie et de sûreté du logiciel

activités nécessaires au développement et à l'exploitation du logiciel d'un système d'I&C important pour la sûreté. Elles couvrent la période allant de la spécification des exigences sur le logiciel au retrait de service du logiciel

[CEI 62138, 3.31]

3.38

version de logiciel

nouvelle édition d'un produit logiciel consécutive à une modification ou à une correction d'un produit logiciel précédent

[IEEE 610, modifiée]

3.31**safety function**

specific purpose that must be accomplished for safety

[IAEA NS-R-1, Glossary]

3.32**safety system**

system important to safety, provided to ensure the safety shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis incidents

[IAEA NS-R-1, Glossary]

3.33**signal trajectory**

time histories of all equipment conditions, internal states, input signals, and operator inputs which determine the outputs of a system

3.34**software**

programs (i.e. sets of ordered instructions), data, rules and any associated documentation pertaining to the operation of a computer-based I&C system

[IEC 62138, 3.27]

3.35**software development**

phase of the software lifecycle that leads to the creation of the software of an I&C system or of a software product. It covers all the activities from software requirements specification to validation and installation on site

[IEC 62138, 3.30]

3.36**software modification**

change in an already agreed document (or documents) leading to an alteration of the executable code

NOTE Software modifications may occur either during initial software development (e.g. to remove faults found in later stages of development), or after the software is already in service.

3.37**software safety life cycle**

necessary activities involved in the development and operation of the software of an I&C system important to safety occurring during a period of time that starts at a concept phase with the software requirements specification and finishes when the software is withdrawn from use

[IEC 62138, 3.31]

3.38**software version**

instance of a software product derived by modification or correction of a preceding software product instance

[IEEE 610, modified]

3.39

spécification

document qui spécifie de manière complète, précise et vérifiable les exigences, le comportement de la conception ou autres caractéristiques d'un système ou composant et, souvent, les procédures permettant de déterminer si ces dispositions ont été satisfaites

[IEEE 610]

NOTE Il existe différents types de spécifications, par exemple les spécifications d'exigence logicielle ou les spécifications de conception.

3.40

analyse statique

processus d'évaluation d'un système ou d'un composant basé sur sa forme, sa structure, son contenu ou sa documentation. S'oppose à l'analyse dynamique

3.41

logiciel système

partie du logiciel d'un système d'I&C, d'un équipement ou d'une famille d'équipements conçue pour faciliter le développement, l'exploitation et la modification de ces systèmes et des programmes associés

[CEI 62138, 3.33]

3.42

validation du système

confirmation par examen et apport d'autres éléments justificatifs qu'un système satisfait à la totalité des exigences spécifiées (fonctionnalités, temps de réponse, tolérance aux fautes, robustesse)

3.43

vérification

confirmation par examen et apport d'éléments objectifs que les résultats d'une activité sont conformes aux objectifs et exigences établis pour cette activité

[CEI 62138, 3.35]

4 Symboles et abréviations

CASE	Atelier de Génie Logiciel
CCF	Défaillance de Cause Commune (voir 3.8)
I&C	Instrumentation et Contrôle-Commande
PDS	Logiciel Prédéveloppé (voir 3.28)
PIE	Événement Initiateur Hypothétique (voir 3.27)
QA	Assurance Qualité
V&V	Vérification et Validation

5 Exigences générales pour les projets logiciel

5.1 Généralités

Le processus de production des systèmes d'instrumentation et de contrôle-commande destinés aux centrales nucléaires est décrit dans la CEI 61513 qui introduit la notion de cycle de vie et de sûreté du système comme moyen d'assurer la maîtrise du processus de développement et comme cadre permettant d'apporter les justifications nécessaires à la mise en service de ces systèmes. Le cycle de vie et de sûreté du système décrit par la CEI 61513 inclut et énonce des exigences sur les dispositions nécessaires à la production des systèmes, mais n'impose pas de disposition particulière (voir Figure 1).

3.39**specification**

document that specifies, in a complete, precise, verifiable manner, the requirements, design behaviour or other characteristics of a system or component and, often, the procedures for determining whether these provisions have been satisfied

[IEEE 610]

NOTE There are different types of specifications, for example software requirements specification or design specification.

3.40**static analysis**

process of evaluating a system or component based on its form, structure, content or documentation. In contrast to dynamic analysis

3.41**system software**

part of the software of an I&C system designed for a specific computer or equipment family to facilitate the development, operation and modification of these items and associated programs

[IEC 62138, 3.33]

3.42**system validation**

confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

3.43**verification**

confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

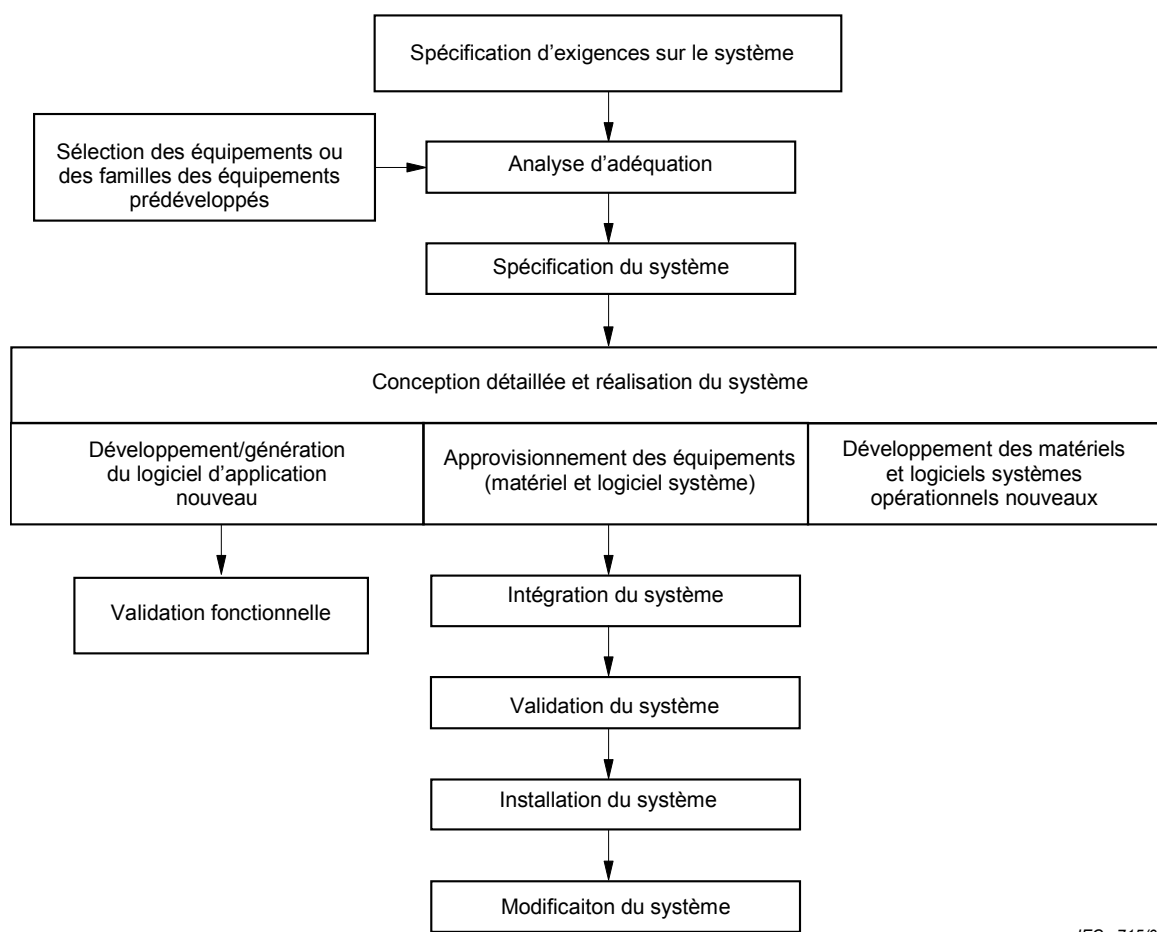
[IEC 62138, 3.35]

4 Symbols and abbreviations

CASE	Computer Aided Software Engineering
CCF	Common Cause Failure (see 3.8)
I&C	Instrumentation and Control
PDS	Pre-Developed Software (see 3.28)
PIE	Postulated Initiating Event (see 3.27)
QA	Quality Assurance
V&V	Verification and Validation

5 General requirements for software projects**5.1 General**

The process of producing instrumentation and control systems for use in nuclear power plants is set down in IEC 61513 that introduces the concept of the system safety lifecycle as a vehicle by which the development process can be controlled and whose adoption should also result in the evidence necessary to justify the operation of safety systems. The system safety lifecycle described in IEC 61513 includes and places requirements on, but does not dictate, the project arrangements to be used for production of systems (see Figure 1).



IEC 715/06

**Figure 1 – Activités du cycle de vie et de sûreté du système
(telles que définies par la CEI 61513)**

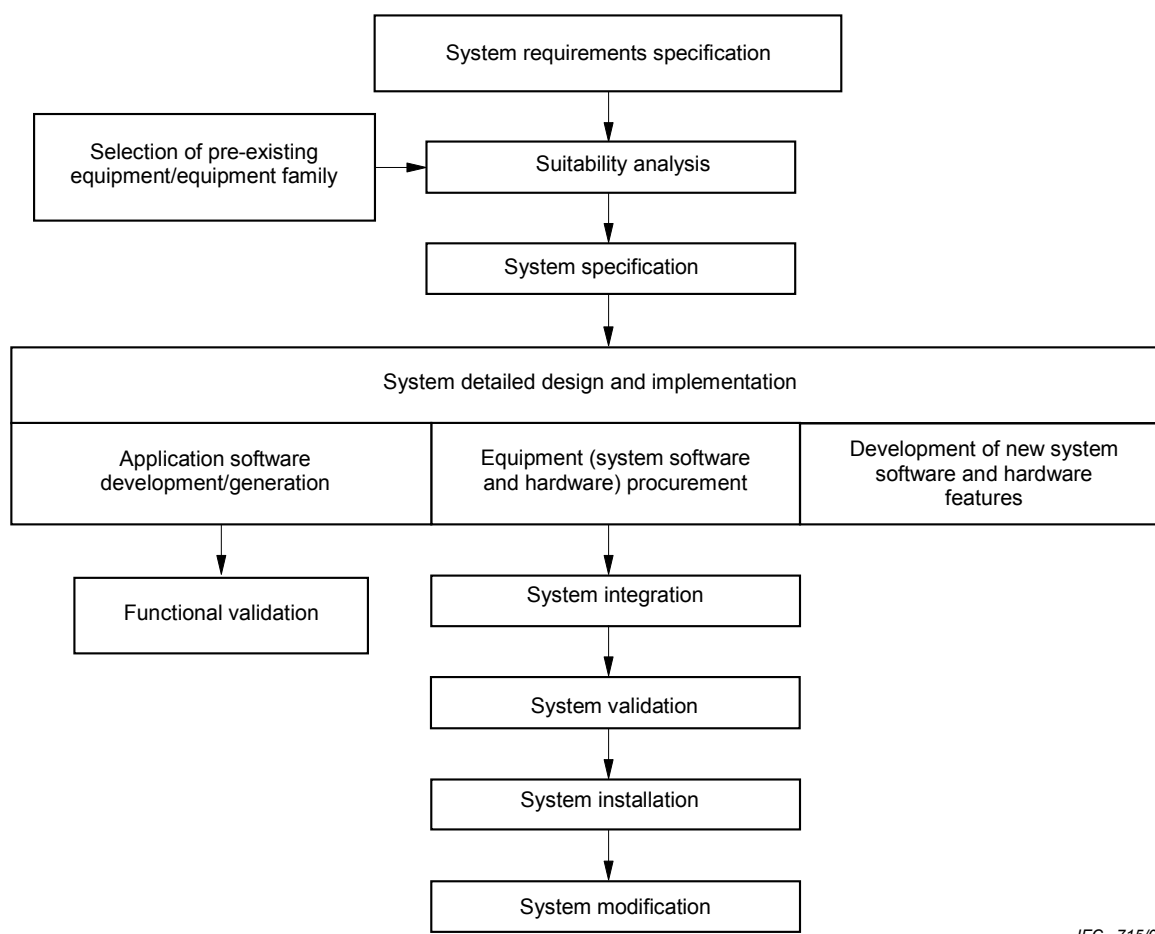
Pour les systèmes programmés (c'est-à-dire numériques), le cycle de vie et de sûreté du système est précisé pour introduire le concept de cycle de vie et de sûreté du logiciel (voir Figure 2 pour les activités). Il montre des développements matériel et logiciel pouvant être entrepris en parallèle à partir d'une spécification commune et se rejoignant aux phases d'intégration et d'installation.

Les processus suivants complètent le processus de développement en phases du logiciel:

- la gestion du projet logiciel (5.4);
- l'assurance qualité et le contrôle de la qualité du logiciel (5.5);
- la gestion de configuration du logiciel (5.6);
- la sécurité du logiciel (5.7);
- la vérification du logiciel (Article 8).

Il y a également des activités correspondant à la sélection de langages (7.2, Annexe D), la sélection des outils logiciels contribuant au développement (Article 14), la prévention des CCF (Article 13) et la production de la documentation (7.4, Annexe F).

Les activités relatives au logiciel dans le cycle de vie et de sûreté du système et les processus complémentaires sont décrits ci-dessous dans la Figure 2 (cases encadrées en gras avec référence aux paragraphes donnée entre parenthèses).



IEC 715/06

Figure 1 – Activities of the system safety lifecycle (as defined by IEC 61513)

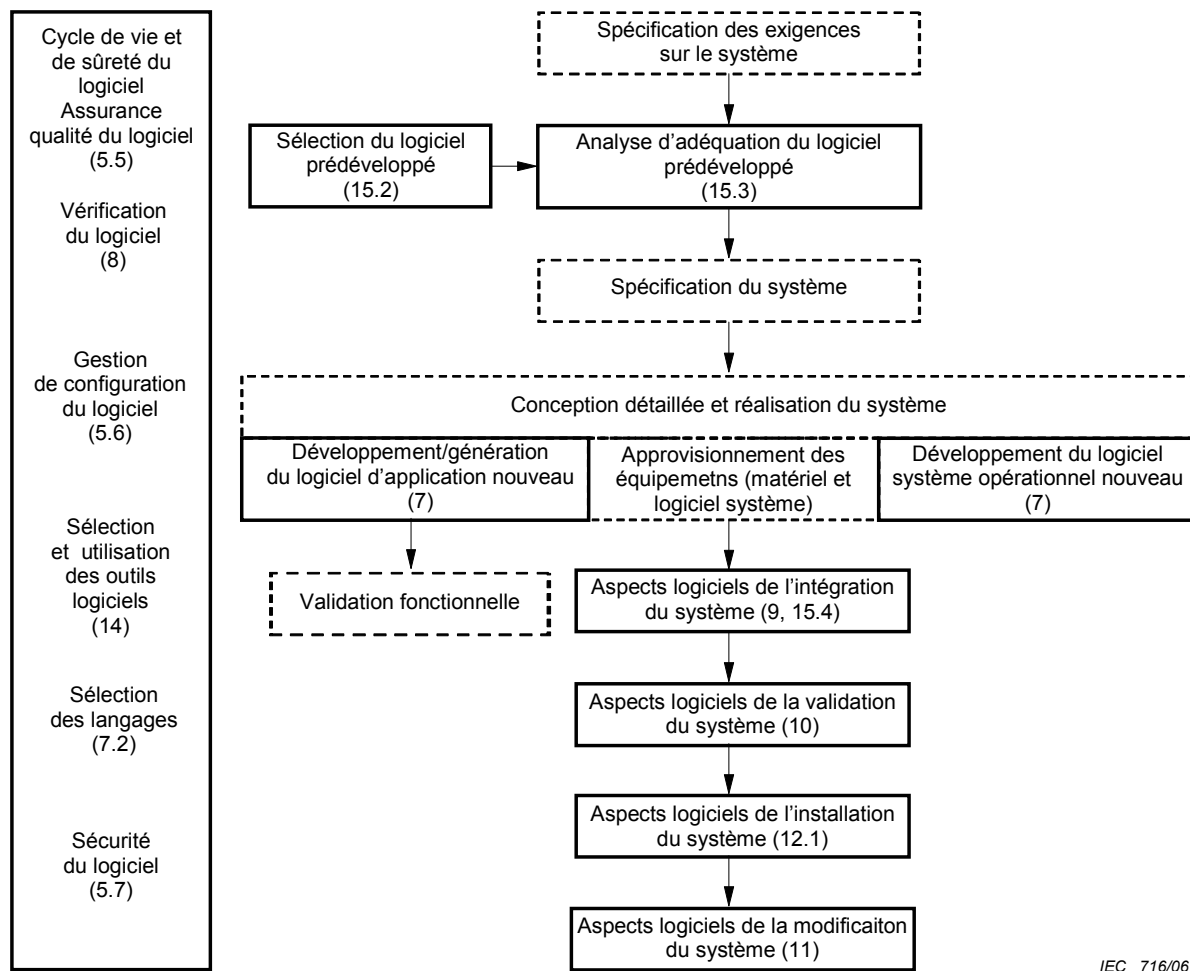
For computer-based (i.e. digital) systems the system safety lifecycle is further developed to introduce the concept of a software safety lifecycle (see Figure 2 for activities). This shows the hardware and software development being undertaken in parallel from a common specification but coming together at the integration and installation phases of the lifecycle.

The following processes support the phased development process of producing the software:

- software project management (5.4);
- software quality assurance and quality control (5.5);
- software configuration management (5.6);
- software security (5.7);
- software verification (Clause 8).

There are also activities involving selection of languages (7.2, Annex D), selection of software tools to support the development (Clause 14), prevention of CCF (Clause 13) and production of documentation (7.4, Annex F).

The resulting software related activities in the system safety lifecycle and the supporting processes are shown below in Figure 2 (boxes in bold lines with reference to related subclauses in brackets).



IEC 716/06

NOTE Les cases en pointillé représentent les activités du cycle de vie et de sûreté du système non traitées dans cette norme.

Figure 2 – Activités liées au logiciel, dans le cycle de vie et de sûreté du système

Il convient que le principe de développement du logiciel repose sur le modèle en «V» traditionnel, adopté par d'autres normes, notamment par le guide de sûreté AIEA NS-G-1.3, avec cependant les ajustements nécessaires lorsque certaines phases du développement sont faites automatiquement à l'aide d'outils ou lorsque le développement du logiciel suit un processus itératif.

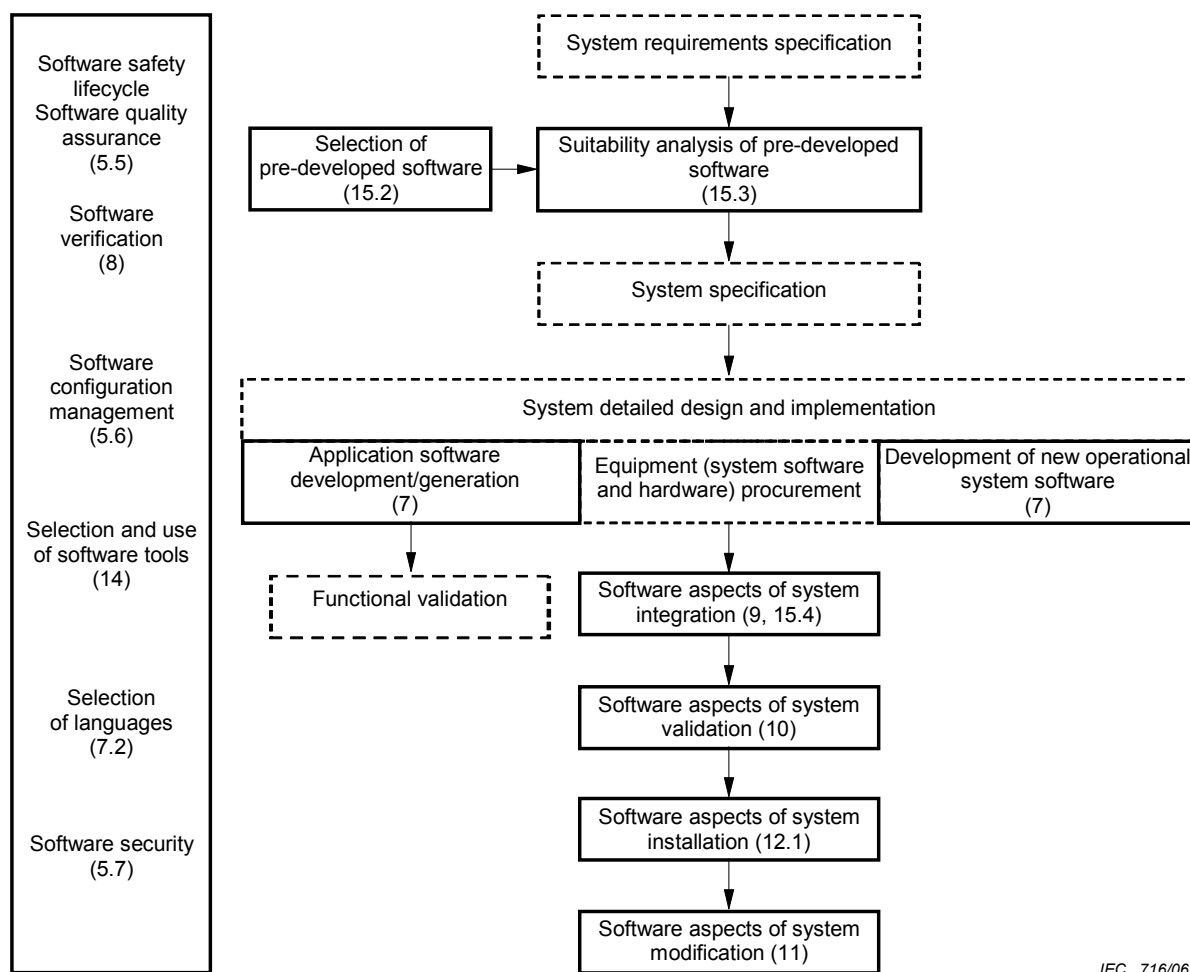
Les paragraphes 5.2 et 5.3 introduisent les différents types de logiciel et le principe de développement considérés dans cette norme.

5.2 Types de logiciel

Un composant logiciel d'un système programmé est souvent caractérisé comme étant soit du logiciel système opérationnel (gestion des communications, gestion des E/S, fonctions standards, fonctions d'auto-surveillance, etc.), soit du logiciel d'application (logique de verrouillage, boucles de commande, formats d'affichage, logique d'alarme, etc.).

Le logiciel d'application utilise généralement les fonctions fournies par le logiciel système opérationnel, réduisant ainsi le besoin de duplication de code et par conséquent la taille globale du logiciel.

Le logiciel d'application est généralement spécifique à un projet.



NOTE Boxes in thin dotted lines represent system activities not addressed in this standard.

Figure 2 – Software related activities in the system safety lifecycle

The approach to software development should be based on the traditional “V” model as this approach has been reflected and promulgated in other standards notably IAEA NS-G-1.3, but allowing necessary adjustments recognizing that some phases of the development can be done automatically by tools and that software development may be iterative.

Subclauses 5.2 and 5.3 introduce the different software types and the development approach considered in this standard.

5.2 Software types

The software components of a system are often defined as being either operational system software (communications, I/O management, standard functions, self-supervision, etc.) or application software (interlock logic, control loops, display formats, alarm logic, etc.).

Application software generally uses the facilities provided by the operational system software, thus reducing the need for duplication of code within modules and thus reducing the overall amount of software.

Application software is usually specific to one project.

Le logiciel système opérationnel peut être réutilisé dans différents projets.

De nombreuses conceptions de système font un usage important des données de configuration. Les données de configuration peuvent être associées au logiciel système opérationnel ou au logiciel d'application. Les données de configuration associées au logiciel d'application consistent principalement en données d'ingénierie résultant de la conception de l'installation, et sont souvent préparées par des concepteurs de centrale n'ayant pas nécessairement de compétences en logiciel.

Les données de configuration peuvent être divisées en:

- données qui ne sont pas destinées à être modifiées en ligne par des exploitants, et qui sont soumises aux mêmes exigences que le reste du logiciel,
- paramètres, c'est-à-dire des données pouvant être modifiées par des exploitants pendant le fonctionnement de l'installation (par exemple, des seuils d'alarme, des points de réglage, des données d'étalonnage de l'instrumentation), et qui nécessitent des exigences spécifiques.

De nombreuses familles d'équipements d'I&C modernes sont fournies avec des outils de développement complets qui permettent aux développeurs de systèmes de concevoir et produire des codes exécutables.

Par exemple, un système d'I&C typique développé en utilisant des composants d'une famille d'équipements comprend:

- des composants logiciels prédéveloppés, tels que le logiciel système opérationnel et les bibliothèques de fonctions d'application. Ces composants sont généralement développés avec des langages généralistes,
- les données de configuration nécessaires à l'adaptation du logiciel système opérationnel aux entrées-sorties et aux services exigés par l'application,
- le logiciel d'application, développé en langage orienté application.

5.3 Principe de développement du logiciel

Le logiciel contribue en général fortement aux fonctions réalisées par le système d'I&C. Il peut aussi contribuer à des fonctions supplémentaires introduites par la conception du système (par exemple l'initialisation et la surveillance du matériel, la communication entre et la synchronisation des sous-systèmes). C'est pourquoi le cycle de vie et de sûreté du logiciel est, dans la plupart des cas, fortement intégré au cycle de vie et de sûreté du système. En particulier, la spécification des exigences du logiciel fait partie, ou découle directement des spécifications du système et de sa conception.

Alors que la vérification des composants logiciels nouveaux fait clairement partie du cycle de vie et de sûreté du logiciel, il n'y a souvent pas de frontière nette entre l'intégration du logiciel et l'intégration du système. Par conséquent, dans cette norme, l'intégration du logiciel est considérée comme faisant partie de l'intégration du système. La validation du logiciel n'est pas non plus une activité purement logicielle: dans cette norme, elle est considérée comme faisant partie de l'intégration du système et/ou de la validation du système.

La norme considère que le cycle de vie du logiciel, conçu à l'origine pour des développements en langages généralistes, est également applicable aux développements en langages orientés application et à la configuration de logiciels prédéveloppés.

Cependant, des différences sont admises dans le processus de développement, par l'introduction, au niveau de la réalisation, de sous-processus dédiés pour chaque type de logiciel:

Operational system software may be used in different projects.

Many system designs make extensive use of configuration data. Configuration data may be associated with operational system software or with application software. Configuration data associated with application software consists mainly of plant engineering data resulting from the design of the plant, and is often prepared by plant designers who are not required to have software skills.

Configuration data can be divided into:

- data items which are not intended to be modified on-line by plant operators, and which are submitted to the same requirements as apply to the rest of the software;
- parameters, i.e. data items which may be modified by operators during plant operation (for example, alarm limits, set points, data required to calibrate instrumentation) and which need specific requirements.

Many modern I&C equipment platforms are provided with extensive development tools which enable system engineers to design and produce executable codes.

As an example, a typical I&C system, developed using components of an equipment family, includes the following:

- pre-developed software components, such as the operational system software kernel and the application function libraries. Generally, these components have been developed using general-purpose languages;
- configuration data needed to adapt the operational system software kernel to the I/O environment and to the services required by the application;
- application software developed using an application-oriented language.

5.3 Software development approach

Software usually contributes strongly to the functions performed by the I&C system. It may also support additional functions introduced by system design (e.g. initialisation and surveillance of hardware, communication between, and synchronisation of, subsystems). Thus, the software safety lifecycle is in most cases strongly integrated with the system safety lifecycle. In particular, the software requirements specification is a part of, or is derived directly from, system specification and system design.

Though the verification of new software components is definitely a part of the software safety lifecycle, there is often no separate and well-identified boundary between software integration and system integration. Therefore, in this standard, software integration is considered to be a part of system integration. Software validation too is not a purely software activity: in this standard, it is considered a part of system integration and/or system validation.

The standard assumes that the software life cycle, originally intended for the development of software with general-purpose languages, is also applicable to application-oriented languages and configuration of pre-developed software.

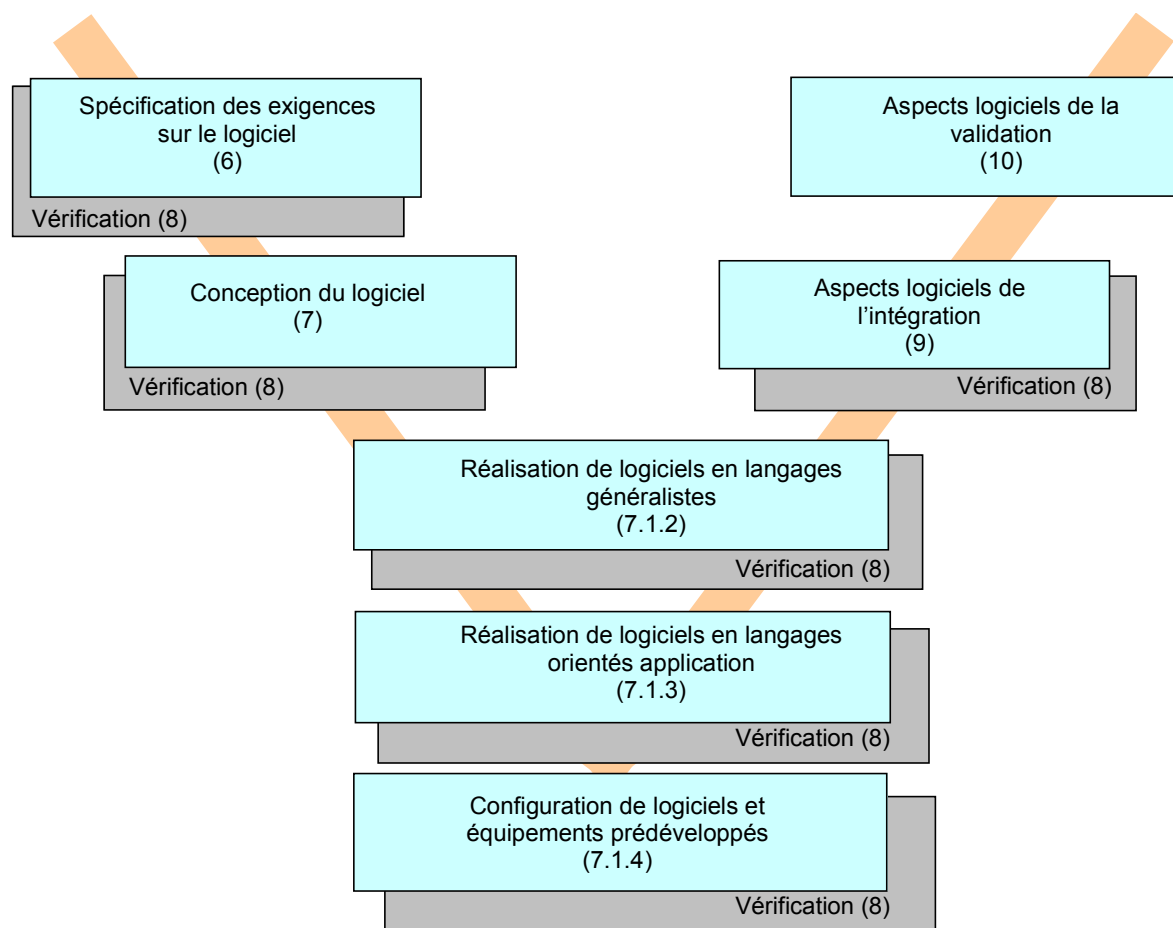
However, it recognises differences in the development process by introducing dedicated sub-processes for each software type at the implementation level:

- réalisation avec des langages généralistes;
- réalisation avec des langages orientés application, et des générateurs de code associés;
- sélection, utilisation et configuration de produits logiciels prédéveloppés.

Comme les encadrés «Développement/Génération du logiciel d'application nouveau» et «Développement du logiciel système opérationnel nouveau» de la Figure 2 représentent une part importante et essentielle du cycle de vie et de sûreté du logiciel, un «zoom» est fourni en Figure 3, illustrant avec plus de détails les activités entre la spécification des exigences du logiciel et la validation du logiciel, avec une représentation claire des trois différentes voies de réalisation. Dans cette figure, les références aux articles et paragraphes de cette norme sont entre parenthèses.

L'Annexe B de cette norme donne également des exigences supplémentaires pour le logiciel.

Les principes sous-tendus par les exigences de cette norme sont en relation avec la qualité du code final et sont applicables indépendamment du fait que le code soit développé avec des langages généralistes, avec des langages orientés application et une génération de code automatisée, ou par configuration de produits logiciels.



IEC 717/06

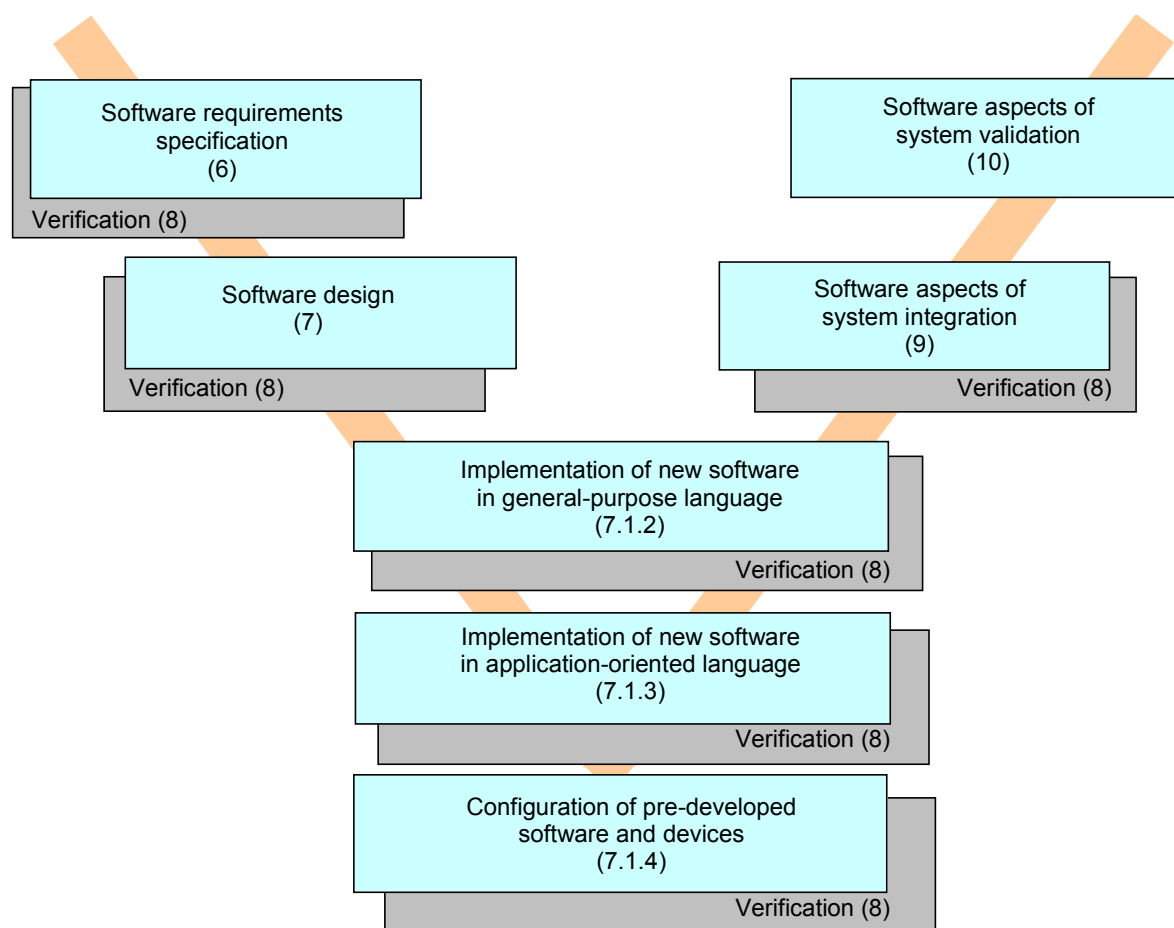
Figure 3 – Activités de développement dans le cycle de vie et de sûreté du logiciel pour la CEI 60880

- implementation using general-purpose languages;
- implementation using application-oriented languages with associated code generators;
- selection, use and configuration of pre-developed software products.

As boxes “Application software development/generation” and “Development of new operational system software” in Figure 2 represent a large and essential part of the software safety lifecycle, a “zoom” is provided in Figure 3, which illustrates in more detail the activities between software requirements specification and validation, with a clear representation of the three different implementation paths. In that figure, references to related subclauses of this standard are in brackets.

The standard also gives additional requirements for software in Annex B.

The principles, reflected in the requirements of this standard, are related to the quality of the final code, and are applicable regardless of whether the code is developed using general-purpose languages, application-oriented languages with automated code generation, or configuration.



IEC 717/06

Figure 3 – Development activities of the IEC 60880 software safety lifecycle

5.4 Gestion du projet logiciel

5.4.1 Tout projet logiciel doit être découpé en phases.

Chaque phase constitue une entité en soi, mais elle est dépendante de certaines phases, tandis que d'autres phases en dépendent. Ces phases sont caractérisées de manière informelle par les activités spécifiques qui s'y rapportent.

Les phases et activités associées définies pour un projet logiciel décrivent un processus appelé «développement logiciel» dans cette norme. Il est reconnu que ce processus peut être itératif sous réserve que l'exigence du dernier paragraphe d'introduction de l'Article 6 de la CEI 61513 soit satisfaite.

Les facteurs généraux suivants déterminent les activités et phases d'un projet logiciel.

5.4.2 Les activités réalisées lors du développement logiciel doivent être identifiées en accord avec l'approche choisie pour le projet (voir 5.2 et 5.3).

5.4.3 Les activités de développement du logiciel doivent concerner l'ensemble du cycle de vie et de sûreté du logiciel.

5.4.4 Chaque phase du développement logiciel identifiée en 5.4.1 doit être divisée en activités bien définies.

5.4.5 Les phases du développement logiciel doivent être formalisées, et aucune des phases identifiées ne doit être omise.

5.4.6 Quand des activités du développement logiciel sont automatisées à l'aide d'outils logiciels, les activités automatisées doivent être documentées, en explicitant en particulier les entrées et les sorties significatives pour la phase concernée.

5.4.7 Les entrées et les sorties de chaque phase doivent être définies et explicitées.

5.4.8 Les sorties de chaque phase doivent être systématiquement vérifiées (point c) de B.1 et point g) de B.4).

5.4.9 Chaque phase doit inclure la constitution d'une documentation appropriée (Annexe F).

5.4.10 Chaque phase doit systématiquement se terminer par une revue incluant l'examen des documents correspondants.

5.4.11 Une liste des documents requis durant le cycle de vie et de sûreté du logiciel doit être établie pendant le développement du logiciel. Un exemple de liste type est donné en annexe F.

5.5 Plan d'assurance qualité logiciel

5.5.1 Un plan d'assurance qualité doit exister ou être établi au plus tôt dans le cycle de vie et de sûreté du logiciel.

Des plans d'assurance qualité spécifiques peuvent être adoptés pour des phases concernant des produits particuliers ou pour des composants logiciels particuliers, en appliquant des normes nationales ou des règles d'entreprise, sous réserve que les principes définis dans cette norme soient pris en compte.

5.5.2 Tout écart par rapport aux exigences de cette norme et de ses annexes normatives doit être identifié et justifié.

5.4 Software project management

5.4.1 Any software project shall be structured into a number of phases.

Each phase is to some extent self-contained but will depend on other phases and will, in its turn, be depended on by others. These phases are informally recognizable by the specific activities pertinent to them.

The phases and associated activities defined for a software project describe a process called in this standard the "software development". It is recognized that this process may be iterative provided the requirement from the last paragraph of the introduction to Clause 6 of the IEC 61513 is fulfilled.

The following general factors determine the activities and phases in implementing a software project.

5.4.2 The activities performed during the phases of the development process shall be identified, according to the software development approach chosen for the project (see 5.2 and 5.3).

5.4.3 Software development activities shall address the whole software safety lifecycle.

5.4.4 Each phase of the software development identified in 5.4.1 shall be divided into well-defined activities.

5.4.5 The phases of the software development shall be formalised and none of the identified phases shall be omitted.

5.4.6 When activities of the software development are automated using software tools, the activities automated shall be documented including the documentation of the inputs and outputs relevant to the phase.

5.4.7 The inputs and outputs of each phase shall be defined and documented.

5.4.8 Every output of each phase shall be systematically checked (item c) of B.1 and item g) of B.4).

5.4.9 Each phase shall include generation of the appropriate documents (Annex F).

5.4.10 Each phase shall be systematically terminated by a review including examination of relevant documents.

5.4.11 A list of documents required through the software safety life cycle shall be established during the software development. An example of a typical list is given in Annex F.

5.5 Software quality assurance plan

5.5.1 A quality assurance plan shall exist or be established at an early stage of the software safety life cycle.

Special quality assurance plans may be adopted for individual product phases or particular software components according to national or company standards provided the principles defined in this standard are addressed.

5.5.2 Any deviations from the requirements of this standard and its normative annexes shall be identified and justified.

5.5.3 Si des pratiques différentes de celles figurant dans les annexes normatives sont utilisées, elles doivent être explicitées et pouvoir être vérifiées par rapport aux exigences de cette norme.

5.5.4 En particulier, l'impact de ces pratiques sur le système d'I&C et le logiciel doit être pris en considération.

5.5.5 Les procédures techniques nécessaires à chaque phase du cycle de vie et de sûreté du logiciel doivent être référencées par le plan d'assurance qualité.

5.5.6 Le plan d'assurance qualité doit exiger que la réalisation des activités soit confiée à des personnes compétentes disposant de ressources adéquates.

5.5.7 Le plan d'assurance qualité doit exiger que les modifications de documents déjà approuvés soient identifiées, revues et approuvées par les personnes autorisées.

5.5.8 Le plan d'assurance qualité doit exiger que les méthodes, langages, outils, règles et normes utilisées soient identifiés et documentés, et connus et maîtrisés par les personnes concernées.

5.5.9 Si plusieurs méthodes, langages, outils, règles et/ou normes sont utilisés, le plan d'assurance qualité doit exiger que ce qui a été utilisé pour chaque activité soit clairement établi.

5.5.10 Le plan d'assurance qualité doit exiger que les termes, expressions, abréviations et conventions utilisés dans un sens spécifique au projet soient explicitement définis.

5.5.11 Le plan d'assurance qualité doit exiger que tout problème de qualité rencontré soit suivi et résolu.

5.5.12 Le plan d'assurance qualité doit exiger que des enregistrements résultant de son application soient produits.

5.5.13 Chaque étape de vérification ou revue doit donner lieu à un rapport sur l'analyse réalisée, les conclusions atteintes et les décisions prises. Ce rapport doit être inclus dans la documentation.

5.5.14 Tout écart par rapport au plan d'assurance qualité doit être explicité et justifié.

5.6 Gestion de configuration

Le paragraphe 6.2.1.2 (plan de gestion de configuration du système) de la CEI 61513 énonce des exigences pour la gestion de configuration au niveau du système d'I&C. Le présent paragraphe énonce des exigences supplémentaires spécifiques ou d'une importance particulière pour le logiciel.

5.6.1 La gestion de configuration du logiciel doit être réalisée conformément aux dispositions d'un plan de gestion de configuration ou du plan d'assurance qualité.

5.6.2 Ces dispositions doivent être cohérentes avec celles de la gestion de configuration du niveau système.

5.6.3 Des procédures de gestion de configuration du logiciel doivent être établies et documentées au plus tôt dans le cycle de vie et de sûreté du projet logiciel pour répondre aux exigences suivantes.

5.5.3 If practices differing from those of normative annexes are used, they shall be documented and auditable according to the requirements of the main parts of this standard.

5.5.4 In particular, the impact of these practices on the I&C system and the software shall be considered.

5.5.5 All technical procedures required during each phase of the software safety life cycle shall be addressed by the quality assurance plan.

5.5.6 The quality assurance plan shall require that the implementation of the activities of the phases is assigned to competent persons equipped with adequate resources.

5.5.7 The quality assurance plan shall require that modifications in already approved documents are identified, reviewed and approved by authorized persons.

5.5.8 The quality assurance plan shall require that the methods, languages, tools, rules and standards used are identified and documented, and known to, and mastered by, the persons concerned.

5.5.9 The quality assurance plan shall require that when several methods, languages, tools, rules and/or standards are used, it is clear which ones were used for each activity.

5.5.10 The quality assurance plan shall require that project specific terms, expressions, abbreviations and conventions are explicitly defined.

5.5.11 The quality assurance plan shall require that any quality issues raised are tracked and resolved.

5.5.12 The quality assurance plan shall require that records resulting from its application are produced.

5.5.13 Every verification step or review shall result in a report on the analysis performed, the conclusions reached and the resolutions agreed. This report shall be included in the documentation.

5.5.14 Any deviation from the quality assurance plan shall be documented and justified.

5.6 Configuration management

Subclause 6.2.1.2 (system configuration management plan) of IEC 61513 provides requirements for configuration management at the I&C system level. This subclause provides additional requirements specific, or of particular importance, to software.

5.6.1 Configuration management for software shall be performed according to the provisions of a configuration management plan or of the quality assurance plan.

5.6.2 These provisions shall be consistent with those for system level configuration management.

5.6.3 Documented software configuration management procedures shall be established early in the lifecycle of a software project to address the following requirements.

5.6.4 Chaque version produite de chaque entité logicielle doit être identifiée de façon unique.

5.6.5 Il doit être possible d'identifier la version applicable de tout document associé à chaque entité logicielle.

5.6.6 Tout logiciel en développement doit être clairement séparé des logiciels mis en exploitation ou déjà vérifiés.

5.6.7 Il doit être possible d'identifier la version de toutes les entités logicielles qui collectivement constituent une version complète du produit final.

5.6.8 Il doit être possible de vérifier l'intégrité des entités logicielles.

5.6.9 Il doit être possible d'identifier la version du logiciel incorporé dans le système d'I&C cible.

5.6.10 Il doit être possible d'identifier a posteriori toutes les entités logicielles affectées par la réalisation d'une modification.

5.6.11 L'accès à toute entité logicielle placée sous gestion de configuration doit être soumis à des contrôles appropriés assurant que le logiciel n'est pas modifié par des personnes non autorisées et que la sécurité du logiciel est maintenue.

5.6.12 Il doit être possible d'identifier tous les outils de traduction et les versions d'outils utilisés pour produire chaque entité exécutable (voir 14.3.3).

5.7 Sécurité du logiciel

L'objectif de la sécurité est de protéger le logiciel et les données afin que des personnes et des systèmes non autorisés ne puissent pas les lire ou les modifier, et que l'accès par les personnes et les systèmes autorisés ne leur soit pas refusé.

Les paragraphes 5.4.2 (plan de sécurité globale) et 6.2.2 (plan de sécurité du système) de la CEI 61513 énoncent des exigences pour la sécurité au niveau de l'architecture globale de l'I&C et au niveau des systèmes d'I&C particuliers.

Bien que l'utilisation de logiciels présente des menaces potentielles pour la sécurité, les principales contre-mesures sont généralement réalisées au niveau du système, par exemple des mesures de protection physique ou des dispositifs de verrouillage câblés. Les principales exigences de sécurité sur le logiciel peuvent aider à minimiser la vulnérabilité et peuvent permettre et faciliter les mesures de protection au niveau système.

Ce paragraphe énonce des exigences de sécurité spécifiques ou d'une importante particulière pour le logiciel.

5.7.1 Analyse de sécurité

5.7.1.1 Une analyse des menaces potentielles pour la sécurité du logiciel doit être réalisée. Elle doit prendre en considération les phases concernées des cycles de vie et de sûreté du logiciel et du système. Elle doit déterminer les exigences concernant la protection et l'accessibilité des données et du logiciel, sur la base des exigences de ce paragraphe.

5.7.1.2 L'analyse de sécurité du logiciel doit être prise en compte dans le plan d'assurance qualité du système ou du logiciel, ou dans le plan de sécurité du système ou du logiciel.

5.6.4 Each produced version of each software entity shall be uniquely identified.

5.6.5 It shall be possible to identify the relevant versions of all software documentation associated with each software entity.

5.6.6 Software under development shall be segregated from software which has achieved release or verified status.

5.6.7 It shall be possible to identify the versions of all software entities which together constitute a complete version of the final product.

5.6.8 It shall be possible to verify the integrity of the software entities.

5.6.9 It shall be possible to identify the version of the software in the target system.

5.6.10 It shall be possible to retrospectively identify all software entities affected by the implementation of a modification.

5.6.11 Access to all software entities placed under configuration control shall be subject to adequate controls to ensure that software is not modified by unauthorised persons and that the security of the software is maintained.

5.6.12 It shall be possible to identify all translation tools and tool versions used to produce each executable entity (see 14.3.3).

5.7 Software security

The objective of security is to protect software and data so that unauthorised persons and systems cannot read or modify them and so that authorised persons and systems are not denied access to them.

Subclauses 5.4.2 (overall security plan) and 6.2.2 (system security plan) of IEC 61513 provide requirements for security at a level of the I&C architecture and of an individual I&C system.

Although the use of software does present certain potential security threats, the main countermeasures are usually on system level, for example physical protection measures, hardwired interlocking devices. The main security requirements put on the software may help minimizing the vulnerability and may enable and support the protective measures on the system level.

This subclause provides security requirements specific to or of particular importance to software.

5.7.1 Security analysis

5.7.1.1 An analysis of the potential security threats regarding the software shall be performed. It shall take into account the relevant phases of the system and software safety life cycles. It shall determine the requirements regarding the protection and the accessibility of data and software based upon the requirements of this subclause.

5.7.1.2 The software security analysis shall be taken into account in the software or system quality assurance plan or in the software or system security plan.

5.7.1.3 Si l'analyse montre que les contre-mesures au niveau du système ne sont pas suffisantes, elle doit déterminer des exigences pour des contre-mesures dans la conception du logiciel.

5.7.2 Conception de la sécurité

5.7.2.1 Les exigences pour des contre-mesures dans la conception du logiciel déterminées par l'analyse de sécurité doivent être incluses dans les exigences de conception du logiciel.

5.7.2.2 Il convient que tout nouveau logiciel soit conçu pour minimiser la vulnérabilité du système.

5.7.2.3 Il convient que tout logiciel prédéveloppé soit configuré et paramétré pour minimiser la vulnérabilité du système, par exemple en se limitant aux fonctions strictement nécessaires ou en utilisant les fonctions de sécurité existantes du logiciel.

5.7.2.4 L'opérateur ne doit pas pouvoir dégrader les logiciels résidants.

5.7.2.5 Si un accès direct de l'opérateur aux données est nécessaire pour l'exploitation des fonctions d'I&C, les dispositifs d'interface homme-machine doivent limiter cet accès au strict nécessaire.

5.7.2.6 Lorsqu'il est nécessaire de contrer des menaces de sécurité potentielles, des mesures de protection efficaces doivent être incluses dans la conception, la configuration et/ou le paramétrage du logiciel pour:

- le contrôle d'accès sélectif de l'utilisateur aux fonctions logicielles,
- les liaisons de données avec les systèmes ayant une importance moindre pour la sûreté,
- la traçabilité des modifications du logiciel ou des paramètres.

5.7.2.7 La documentation de la conception doit identifier et décrire les fonctions critiques pour la sécurité et les caractéristiques de sécurité intégrées au logiciel.

5.7.2.8 Pendant la vérification du logiciel, l'efficacité des fonctions de sécurité doit être confirmée.

5.7.2.9 Pendant la validation du système d'I&C, l'efficacité des fonctions de sécurité du logiciel doit être démontrée par des tests adaptés.

5.7.3 Accès de l'utilisateur

5.7.3.1 Lorsque cela est nécessaire, le logiciel doit comporter des mesures techniques pour une authentification efficace de l'utilisateur avant que l'accès lui soit autorisé.

5.7.3.2 Si le contrôle d'accès de l'utilisateur est une fonction critique pour la sécurité et s'il est réalisé par le logiciel, il convient que l'authentification repose sur une combinaison d'identifiants (par exemple mot de passe), de propriétés (par exemple clé, carte à puce) et/ou de caractéristiques personnelles (par exemple empreintes) plutôt que sur seulement un mot de passe.

5.7.3.3 Le logiciel et le contrôle d'accès «basé fonction» doivent être configurés et paramétrés de telle façon que les autorisations d'accès soient limitées aux fonctions et données nécessaires.

5.7.3.4 Les autorisations d'accès des utilisateurs doivent être protégées de façon appropriée contre les occurrences et les conséquences des menaces de sécurité potentielles.

5.7.1.3 If the analysis shows that the countermeasures on the system level are not sufficient then the security analysis shall identify requirements for software design countermeasures.

5.7.2 Security design

5.7.2.1 The requirements for design countermeasures in the software identified in the security analysis shall be included in the software design requirements.

5.7.2.2 Any new software should be designed so as to minimize the vulnerability of the system.

5.7.2.3 Any pre-developed software should be configured and parameterised so as to minimize the vulnerability of the system, for example by minimizing the functions to the necessary extent or using existing security functions of the software.

5.7.2.4 The operator shall be prevented from altering stored programs.

5.7.2.5 If operator access is required to change data to operate the I&C functions then the human-machine-interface devices shall restrict access to the necessary extent.

5.7.2.6 Where required to counter possible security threats then effective protection measures shall be included in the design, configuration and/or parameter assignment of the software concerning:

- user selective access control to the software functions;
- data connections to systems with lower safety importance;
- traceability of software or parameter modifications.

5.7.2.7 The design documentation shall identify and describe the functions critical for security and the security features implemented into the software.

5.7.2.8 During verification of the software the effectiveness of the security functions shall be confirmed.

5.7.2.9 During the validation of the I&C system, effectiveness of the security functions implemented in the software shall be demonstrated through suitable tests.

5.7.3 User access

5.7.3.1 Where required the software shall support technical measures for an effective authentication procedure before user access is permitted.

5.7.3.2 Where user access is a feature critical for security that is implemented in the software then the authentication procedure implemented in the software should support technical means for a combination of knowledge (e.g. password), property (e.g. key, smart-card) and/or personal features (e. g. fingerprint) rather than rely solely on a password.

5.7.3.3 The software and the role-based access control shall be configured and parameterised so as to minimize the user access permitted to the functions and data to the necessary extent.

5.7.3.4 User access capabilities shall be protected to an appropriate extent against the opportunities and the consequences of potential security threats.

Les méthodes cryptographiques (cryptage des données) sont un moyen pour répondre correctement à cette exigence.

5.7.3.5 Aucun accès à distance qui pourrait influencer sur les fonctions logicielles ou les données hors des locaux techniques de la centrale (par exemple depuis des bâtiments administratifs ou depuis l'extérieur de l'installation) ne doit être mis en place.

5.7.4 Sécurité pendant le développement

5.7.4.1 Il convient que le cycle de vie et de sûreté du logiciel traite les menaces de sécurité pendant le développement et la maintenance.

5.7.4.2 Des dispositions contre la présence de fonctions cachées dans le logiciel d'application ou dans le logiciel système doivent être prises (par exemple vérification du programme logiciel) parce qu'elles pourraient permettre des accès non autorisés.

5.7.4.3 Si de telles dispositions ne peuvent être mises en œuvre pour un logiciel prédéveloppé, l'utilisation de ce logiciel doit être justifiée, en considérant les menaces de sécurité potentielles, l'importance pour la sûreté des fonctions d'I&C concernées, et les caractéristiques du système et du logiciel.

5.7.4.4 Les moyens qui permettraient une modification délibérée d'un logiciel, pouvant provoquer un comportement erroné déclenché par des conditions temporelles ou de valeurs de données, doivent être identifiés et justifiés pour être détectables pendant les activités de vérification.

6 Exigences du logiciel

6.1 Spécification des exigences du logiciel

6.1.1 Les exigences du logiciel sont issues des exigences des systèmes de sûreté et constituent une partie des spécifications du système programmé.

6.1.2 Les exigences du logiciel doivent décrire ce que le logiciel doit faire et non comment il doit le faire.

6.1.3 Les exigences du logiciel doivent spécifier:

- les fonctions d'application à fournir par le logiciel;
- les différents modes de comportement du logiciel et les conditions correspondantes de transition;
- les interfaces et interactions du logiciel avec son environnement (par exemple les exploitants, le reste du système d'I&C, les éventuels autres systèmes avec lesquels il y a interaction ou partage de ressources), y compris les rôles, types, formats, domaines et contraintes des entrées et des sorties;
- les paramètres du logiciel, lorsqu'il y en a, qui peuvent être modifiés manuellement pendant l'exploitation, leurs rôles, types, formats, domaines et contraintes, et les vérifications à réaliser par le logiciel quand ils sont modifiés;
- les performances exigées, en particulier les exigences de temps de réponse;
- ce que le logiciel ne doit pas faire ou ce qu'il doit éviter, quand cela est approprié;
- les exigences prises en compte, ou les hypothèses faites, par le logiciel vis-à-vis de son environnement, lorsque cela est applicable;
- les éventuelles exigences relatives à des produits logiciels standards.

Cryptographic methods (data encryption) can be one of the possible ways to correctly implement this requirement.

5.7.3.5 No remote access that can influence the software functions or the data from outside the technical environment of the plant (e. g. from the administrative buildings or from outside of the plant) shall be implemented.

5.7.4 Security during development

5.7.4.1 The software safety development lifecycle should address potential security threats during development and maintenance activities.

5.7.4.2 There shall be provisions against hidden functions in the application software or system software (e.g. software code verification) because they could support potential unauthorised access.

5.7.4.3 If provisions could not be implemented for pre-developed software, the use of such software shall be justified considering the potential security threats, the safety importance of I&C functions concerned and the characteristics of the system and software.

5.7.4.4 Potential means for deliberate modification of software that may cause erroneous behaviour triggered by time or data conditions shall be identified and justified to be detectable during the verification activities.

6 Software requirements

6.1 Specification of software requirements

6.1.1 The software requirements shall be derived from requirements of the safety systems and are part of the computer-based system specification.

6.1.2 The software requirements shall describe what the software has to do and not how the software shall do it.

6.1.3 The software requirements shall specify:

- the application functions to be provided by the software;
- the different modes of behaviour of the software, and the corresponding conditions of transition;
- the interfaces and interactions of the software with its environment (e.g. with operators, with the rest of the I&C system, with the other systems, if any, with which it interacts or shares resources), including the roles, types, formats, ranges and constraints of inputs and outputs;
- the parameters of the software which can be modified manually during operation, if any, their roles, types, formats, ranges and constraints, and the checks to be performed by the software when they are modified;
- the required software performance, in particular response time requirements;
- what the software must not do or must avoid, when appropriate;
- the requirements of, or the assumptions made by, the software regarding its environment, when applicable;
- the requirements if any, of standard software packages.

6.1.4 Du fait de l'importance de cette phase de développement du logiciel, le processus d'établissement des exigences du logiciel doit être rigoureux.

6.1.5 La spécification des exigences du logiciel doit être telle que la conformité du système d'I&C aux exigences de la CEI 61513 peut être démontrée.

Des exigences supplémentaires pour la spécification des exigences du logiciel sont données en Annexe A.

6.1.6 Les contraintes entre matériel et logiciel doivent être décrites (A.2.1).

6.1.7 La spécification des exigences du logiciel doit faire référence à la spécification des exigences du matériel qui interagissent avec le logiciel.

6.1.8 Les conditions particulières de fonctionnement, telles que le démarrage de l'installation et le rechargement en combustible, doivent être décrites et déclinées au niveau logiciel pour les fonctions concernées.

6.2 Auto-surveillance

6.2.1 Le logiciel système du système programmé doit surveiller le matériel pendant l'exploitation, à intervalles de temps spécifiés, ainsi que le comportement du logiciel (A.2.2).

Ceci est considéré comme un facteur essentiel pour atteindre l'objectif de fiabilité de l'ensemble du système.

6.2.2 Les zones de la mémoire qui contiennent le code et les données invariables doivent être surveillées pour détecter les changements non prévus.

6.2.3 Il convient que l'auto-surveillance puisse détecter autant que possible:

- les défaillances aléatoires des composants matériels,
- les erreurs de comportement du logiciel (par exemple, écarts de conditions de fonctionnement de l'installation, écarts de traitements logiciels spécifiés ou corruption de données),
- la transmission de données erronées entre différentes unités de traitement.

6.2.4 Si une défaillance est détectée par le logiciel pendant l'exploitation de l'installation, le logiciel doit donner les réponses appropriées en temps voulu. Celles-ci doivent être réalisées en accord avec les réactions du système exigées par la spécification et les règles de conception du système énoncées dans la CEI 61513.

Cela peut impliquer l'étude de dispositions évitant des déclenchements intempestifs.

6.2.5 L'auto-surveillance ne doit pas dégrader les fonctions que le système doit remplir.

6.2.6 Il convient que la collecte automatique des informations utiles au diagnostic, obtenues durant l'auto-surveillance, soit possible.

6.3 Test périodique

6.3.1 Pour les systèmes de sûreté programmés, il convient que les principes généraux de la CEI 60671 soient utilisés pour les composants qui ne sont pas testés de façon adéquate par l'auto-surveillance.