NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60987

Première édition
First edition
1989-11

Calculateurs programmés importants pour la sûreté des centrales nucléaires

Programmed digital computers important to safety for nuclear power stations

Numéro de référence
Reference number
CEI/IEC 60987: 1989

Numéros des publications

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

Publications consolidées

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

Validité de la présente publication

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

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

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

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

Terminologie, symboles graphiques et littéraux

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

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

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

Numbering

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

Consolidated publications

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

Validity of this publication

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

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

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

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

Terminology, graphical and letter symbols

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

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

* See web site address on title page.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60987

Première édition
First edition
1989-11

Calculateurs programmés importants pour la sûreté des centrales nucléaires

Programmed digital computers important to safety for nuclear power stations

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

IEC Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE T

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CALCULATEURS PROGRAMMÉS IMPORTANTS POUR LA SÛRETÉ DES CENTRALES NUCLÉAIRES

AVANT-PROPOS

1) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparés par des Comités d'Etudes où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.

2) Ces décisions constituent des recommandations internationales et sont agréées comme telles par les Comités nationaux.

3) Dans le but d'encourager l'unification internationale, la CEI exprime le vœu que tous les Comités nationaux adoptent dans leurs règles nationales le texte de la recommandation de la CEI, dans la mesure où les conditions nationales le permettent. Toute divergence entre la recommandation de la CEI et la règle nationale correspondante doit, dans la mesure du possible, être indiquée en termes clairs dans cette dernière.

La présente norme a été établie par le Sous-Comité 45A: Instrumentation des réacteurs, du Comité d'Etudes n° 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

Règle des Six Mois	Rapport de vote
45A(BC)109	45A(BC)118

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

Les publications suivantes de la CEI sont citées dans la présente norme:

Publications n^{os} 50(191): Vocabulaire Electrotechnique International (VEI), Chapitre 191: Sûreté de fonctionnement et qualité de service (en cours d'impression).
557 (1982): Terminologie CEI sur les réacteurs nucléaires.
639 (1979): Réacteurs nucléaires. Utilisation du système de protection à d'autres fins que la sûreté.
780 (1984): Qualification des constituants électriques du système de sûreté des centrales électronucléaires.
801-1 (1984): Compatibilité électromagnétique pour les matériels de mesure et de commande dans les processus industriels, Première partie: Introduction générale.
801-2 (1984): Deuxième partie: Prescriptions relatives aux décharges électrostatiques.
801-3 (1984) Troisième partie: Prescriptions relatives aux champs de rayonnements électromagnétiques.
801-4 (1988): Quatrième partie: Prescriptions relatives aux transitoires électriques rapides en salves.
812 (1985): Techniques d'analyse de la fiabilité des systèmes - Procédure d'analyse des modes de défaillance et de leurs effets (AMDE).
880 (1986): Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires.
1025: Analyse par arbre des défaillances (en cours d'impression).

Autres publications citées:

ISO 2382-1 (1984): Traitement des données - Vocabulaire - Partie 01: Termes fondamentaux.
Guides de sûreté de l'AIEA 50-SG-D3, 50-SG-D7 et 50-SG-D8.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROGRAMMED DIGITAL COMPUTERS IMPORTANT TO SAFETY FOR NUCLEAR POWER STATIONS

FOREWORD

1) The formal decisions or agreements of the IEC on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.

3) In order to promote international unification, the IEC expresses the wish that all National Committees should adopt the text of the IEC recommendation for their national rules in so far as national conditions will permit. Any divergence between the IEC recommendation and the corresponding national rules should, as far as possible, be clearly indicated in the latter.

This standard has been prepared by Sub-Committee 45A: Reactor Instrumentation, of IEC Technical Committee No. 45: Nuclear Instrumentation.

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

Six Months' Rule	Report on the Voting
45A(CO)109	45A(CO)118

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

The following IEC publications are quoted in this standard:

Publications Nos. 50 (191): International Electrotechnical Vocabulary (IEV), Chapter 191: Dependability and quality of service (being printed).
557 (1982): IEC terminology in the nuclear reactor field.
639 (1979): Nuclear reactors. Use of the protection system for non-safety purposes.
780 (1984): Qualification of electrical items of the safety system for nuclear power generating stations.
801-1 (1984): Electromagnetic compatibility for industrial-process measurement and control equipment, Part 1: General introduction.
801-2 (1984): Part 2: Electrostatic discharge requirements.
801-3 (1984): Part 3: Radiated electromagnetic field requirements.
801-4 (1988): Part 4: Electrical fast transient/burst requirements.
812 (1985): Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).
880 (1986): Software for computers in the safety systems of nuclear power stations.
1025: Fault-tree analysis - FTA (being printed).

Other publications quoted:

ISO 2382/1 (1984): Data processing - Vocabulary - Part 01: Fundamental terms.
Safety Guides of IAEA 50-SG-D3, 50-SG-D7 and 50-SG-D8.

CALCULATEURS PROGRAMMÉS IMPORTANTS POUR LA SÛRETÉ DES CENTRALES NUCLÉAIRES

INTRODUCTION

Les principes de base pour la conception des systèmes importants pour la sûreté des centrales nucléaires ont fait l'objet de définitions dans les normes existantes telles les Guides de sûreté 50-SG-D3 et D8 de l'AIEA se référant aux systèmes câblés.

La présente norme interprète ces principes lors de l'utilisation de systèmes programmés dans les systèmes importants pour la sûreté. Elle comprend les systèmes multiprocesseurs distribués et les gros processeurs centraux construits à partir de constituants déjà disponibles ou de matériels nouvellement développés.

Cette norme introduit des prescriptions particulières aux matériels des systèmes programmés. La CEI 880 est applicable pour les prescriptions spécifiques des logiciels pour les calculateurs et les zones communes au matériel et au logiciel.

Cette norme fournit des prescriptions en matière de redondance, d'indépendance et de structure distribuée.

Les prescriptions figurant dans la CEI 780 pour la qualification en général, et en 4.2, en particulier, sont applicables aux calculateurs programmés importants pour la sûreté des centrales nucléaires.

Pour les modules utilisés dans la conception d'une application d'un système spécifique de sûreté, une expérience de fonctionnement appropriée et contrôlable à partir d'applications nucléaires ou autres, telles qu'elles sont décrites dans la CEI 780 en liaison avec des programmes d'assurance qualité de haute fiabilité, peut être une méthode acceptable de qualification.

1 Domaine d'application

La présente norme est applicable aux systèmes programmés importants pour la sûreté utilisés dans les centrales nucléaires. Elle est par conséquent applicable aux systèmes de sûreté et, en général, aux systèmes associés à la sûreté (voir le Guide de sûreté 50-SG-D8 de l'AIEA, figure 1). Certaines prescriptions peuvent ne pas s'appliquer aux systèmes associés à la sûreté.

Cette norme constitue un complément pour les prescriptions sur les classes de sûreté.

Les prescriptions spécifiées sont applicables, mais non limitées aux constituants suivants, jusqu'au niveau des composants de ces systèmes:

a) alimentation électrique extérieure du système programmé;
b) architecture interne;
c) équipements d'entrée/sortie et interfaces;
d) moyens de transmission de données;
e) mémoires;
f) dispositifs d'essai destinés à faire la preuve d'un fonctionnement correct continu pour autant qu'une défaillance de ces dispositifs ne conduise à une défaillance du système informatique.

2 Termes et définitions

Pour les besoins de la présente norme, les définitions suivantes sont applicables. Pour les termes définis ailleurs, la source est donnée entre parenthèses.

2.1 *Disponibilité (VEI 191-02-05)*

Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires est assurée.

PROGRAMMED DIGITAL COMPUTERS IMPORTANT TO SAFETY FOR NUCLEAR POWER STATIONS

INTRODUCTION

The basic principles for the design of systems important to the safety of nuclear power stations have been defined in existing standards such as the Safety Guides 50-SG-D3 and D8 of the IAEA with a view to hardwired systems.

This standard interprets these principles for the utilization of digital systems hardware for systems important to safety. This includes multiprocessor distributed systems and large scale central processor systems constructed from off-the-shelf items or from newly developed hardware.

It lays down requirements specific to the hardware of digital systems. For specific requirements for computer software and common areas of hardware and software, IEC 880 is applicable.

Requirements for redundancy, independence and structural distribution are given.

The requirements of IEC 780 for qualification in general, and especially 4.2, are applicable to programmed digital computers important to safety in nuclear power stations.

For modules used in the design of a specific safety system application, relevant and auditable operating experience from nuclear or other applications as described in IEC 780 in combination with quality assurance programs of high reliability may be an acceptable method of qualification.

1 Scope

This standard is applicable to computer systems hardware for systems important to safety used in nuclear power stations. It is therefore applicable to safety systems and in general to safety-related systems (see Safety Guide 50-SG-D8 of the IAEA, figure 1). Some requirements may not apply to safety-related systems.

This standard constitutes a supplement to the safety classes requirements.

The requirements specified are applicable but not restricted to the following items of such systems, down to the component level:

a) external power supplies to the computer system;
b) internal architecture;
c) input/output equipment and interfaces;
d) data transmission means;
e) storage devices;
f) test devices to prove continued correct operation as far as any failure of these devices leads to failure of the computer system.

2 Terms and definitions

For the purpose of this standard, the following definitions are applicable. For terms defined elsewhere, the source is given in parentheses.

2.1 *Availability (IEV 191-02-05)*

The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

2.2 *Ordinateur ou calculateur (ISO 2382/1)*

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

NOTE - Un ordinateur peut se composer d'une seule ou de plusieurs unités interconnectées.

2.3 *Système programmé (CEI 880, 2.5)*

Ensemble fonctionnel constitué d'une ou de plusieurs unités fonctionnelles et du logiciel associé qui utilise des éléments de stockage communs pour tout ou partie d'un programme ainsi que pour tout ou partie des données nécessaires à l'exécution du programme.

2.4 *Composant*

Matériel: Eléments composant le système (par exemple circuits intégrés, résistances, condensateurs, câbles, connecteurs, transistors, interrupteurs, commutateurs, etc.)

Logiciel: Partie de base d'un système ou programme. Voir aussi 2.17.

2.5 *Conception*

La conception constitue le travail théorique qui conduit à un système capable de satisfaire aux spécifications du système.

2.6 *Développement*

Le développement constitue le travail expérimental d'essais et de démonstration, dont le but est de prouver le fonctionnement satisfaisant de chaque partie du système dont les performances ne peuvent être garanties par le seul travail théorique.

2.7 *Diversité (CEI 880, 2.8)*

Existence de différents moyens de réaliser une fonction requise (par exemple autres principes physiques, autres manières de résoudre la même tâche).

2.8 *Alimentation électrique garantie*

Alimentation du calculateur conçue pour être capable de fournir de manière satisfaisante des sources électriques pendant le fonctionnement normal, pendant la perte de l'alimentation de la centrale et pendant la perte de la connexion de la centrale au réseau de distribution.

2.9 *Tests d'intégration (CEI 880, 2.12)*

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

2.10 *Maintenabilité (VEI 191-02-07 modifié)*

Probabilité de mener, dans des conditions données d'utilisation, une action active de maintenance donnée pendant une période établie, sur un constituant, si cette maintenance est effectuée dans des conditions fixées et en suivant des procédures et des ressources établies.

2.11 *Maintenance (VEI 191-07-01)*

Combinaison de toutes les actions techniques et administratives, y compris les actions de surveillance, destinées à maintenir ou à remettre une entité dans un état lui permettant d'accomplir une fonction requise.

2.2 *Computer (ISO 2382/1)*

A 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.

NOTE - A computer may be a stand-alone unit or may consist of several interconnected units.

2.3 *Computer system (IEC 880, 2.5)*

A functional unit, consisting of one or more computers and associated software, that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program.

2.4 *Component*

Hardware: Items from which the system is assembled (e.g. integrated circuits, resistors, capacitors, wires, connectors, transistors, switches, etc.)

Software: A basic part of a program. See also 2.17.

2.5 *Design*

The theoretical work which leads towards a system able to meet the system requirements specification.

2.6 *Development*

The experimental, test and demonstration work which is intended to prove the success of any parts of the design whose performance cannot be ensured by theoretical work alone.

2.7 *Diversity (IEC 880, 2.8)*

The existence of different means of performing a required function (e.g. other physical principles, other ways of solving the same task).

2.8 *Guaranteed power supply*

A power supply for the computer system which is designed to be able to provide satisfactory electrical supplies normally, during loss of electrical generator on the station, and during loss of connection of the station to the electrical distribution network or grid which it serves.

2.9 *Integration tests (IEC 880, 2.12)*

Tests performed during the hardware/software integration process prior to computer system validation to verify compatibility of the software and the computer system hardware.

2.10 *Maintainability (IEV 191-02-07 modified)*

The probability that a given active maintenance action to an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.

2.11 *Maintenance (IEV 191-07-01)*

The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform a required function.

2.12 *Module*

Tout assemblage de composants interconnectés constituant un dispositif, instrument ou élément de matériel identifiables. Un module peut être retiré en tant qu'unité indépendante et remplacé par une pièce de rechange. Il est doté de caractéristiques de fonctionnement définissables qui permettent de le tester comme unité. Un module peut être une carte, un disjoncteur à éléments amovibles ou tout autre sous-ensemble faisant partie d'un dispositif plus important, à condition de satisfaire aux prescriptions de cette définition.

2.13 *Durée de vie qualifiée (CEI 780, 3.16)*

Période de temps pendant laquelle il peut être vérifié que les caractéristiques restent satisfaisantes dans un ensemble spécifié de conditions d'utilisation.

2.14 *Redondance (AIEA 50-SG-D8)*

Existence d'éléments supplémentaires (identiques ou différents), de sorte que l'un d'entre eux puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou des défaillances de l'un d'entre eux.

2.15 *Fiabilité*

Probabilité de non-occurrence pendant une période d'exposition spécifiée d'une défaillance susceptible de modifier la sortie requise au-delà de tolérances spécifiées dans un environnement donné.

2.16 *Critère de défaillance unique (CEI 557, 2.26)*

Critère appliqué à un système tel que celui-ci soit capable de remplir sa propre tâche de sûreté lorsqu'il est soumis à un seul défaut.

2.17 *Logiciel (CEI 880, 2.16)*

Programmes, procédures, règles et tout document associé, liés à la mise en œuvre du système programmé.

2.18 *Sous-système*

Partie d'un système, elle-même dotée des caractéristiques d'un système.

2.19 *Système*

Ensemble d'éléments interconnectés constitués dans le but d'atteindre un objectif donné en accomplissant une fonction spécifiée.

2.20 *Validation (CEI 880, 2.20)*

Test et évaluation du système de traitement intégré (matériel et logiciel) pour s'assurer de sa conformité aux spécifications fonctionnelles, ainsi qu'aux prescriptions de performances et d'interfaces.

2.21 *Vérification (CEI 880, 2.21)*

Processus consistant à déterminer lors de chaque phase du développement du système de traitement programmé si le produit élaboré répond aux prescriptions issues de la phase précédente.

2.12 *Module*

Any assembly of interconnected components which constitutes an identifiable device, instrument or piece of equipment. A module can be removed as a unit and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card, a drawout circuit breaker or any other sub-assembly of a larger device, provided it meets the requirements of this definition.

2.13 *Qualified life (IEC 780, 3.16)*

The period of time for which satisfactory performance can be verified for a specified set of operating conditions.

2.14 *Redundancy (IAEA 50-SG-D8)*

The provision of alternative (identical or diverse) elements so that any one can perform the required function regardless of the state of operation or failure of any other.

2.15 *Reliability*

The probability that a failure which causes deviation from the required output by more than specified tolerances, in a specific environment, does not occur during a specified exposure period.

2.16 *Single failure criterion (IEC 557, 2.26)*

A criterion applied to a system such that it is capable of performing its safety task in the presence of any single failure.

2.17 *Software (IEC 880, 2.16)*

Programs, procedures, rules and any associated documentation pertaining to the operation of a computer system.

2.18 *Sub-system*

A division of a system that in itself has the characteristics of a system.

2.19 *System*

A set of interconnected elements constituted to achieve a given objective by performing a specified function.

2.20 *Validation (IEC 880, 2.20)*

The test and evaluation of the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements.

2.21 *Verification (IEC 880, 2.21)*

The process of determining whether or not the product of each phase of the digital computer system development process fulfils all the requirements imposed by the previous phase.

3 Structure du projet

En règle générale, un projet sera découpé en phases. Chaque phase constitue en quelque sorte une entité mais sera dépendante des autres phases, qui elles-mêmes en dépendent. Ces phases sont identifiables de manière informelle par les activités spécifiques qui s'y rapportent.

Pour les applications importantes pour la sûreté, ces phases doivent être formalisées, et aucune des phases identifiées ne doit être omise.

Certaines phases logiciel et matériel peuvent être effectuées simultanément. Les procédures formalisées doivent être définies dans le but de réguler la rétroaction entre une phase et celle qui la précède ou qui se déroule simultanément.

Une documentation sur la gestion du projet doit être fournie pour en définir les subdivisions et permettre de l'exécuter de façon contrôlée, en enregistrant et surveillant son évolution. Un plan d'assurance qualité doit être appliqué.

3.1 *Subdivision du projet*

Les facteurs généraux suivants déterminent les activités dans l'exécution d'un projet:

a) L'ensemble du cycle de vie du logiciel doit être considéré (annexe A).

b) Chaque phase du cycle de vie du système doit être divisée en tâches élémentaires dont l'activité doit être bien définie.

c) Les produits "matériel" qui doivent être introduits dans une phase doivent être contrôlés, vérifiés et essayés avant incorporation.

d) Des moyens (pièces de rechange, dispositifs d'essai ou de maintenance) et des locaux (laboratoires, ateliers, espaces, etc.) appropriés doivent être prévus pour la réalisation de chaque phase.

e) Chaque phase doit inclure l'élaboration des documents appropriés.

f) Chaque phase doit se terminer par une vérification (voir article 6).

g) Chaque vérification doit donner lieu à un rapport sur les analyses réalisées, les conclusions obtenues et les modifications éventuelles nécessaires décidées. Ce rapport doit être inclus dans la documentation.

h) Le planning du projet doit être établi dans le but de:

- faciliter une rétroaction entre les phases matériel et logiciel;
- donner le temps nécessaire aux essais, à la documentation, la vérification, la maintenance et l'assurance qualité;
- donner un moyen d'identifier les difficultés survenant inopinément.

3.2 *Assurance qualité*

Un plan d'assurance qualité pour le matériel doit exister en tant que partie du plan d'assurance qualité pour le système programmé. Il doit en principe comprendre les prescriptions pour le matériel déjà soumis à une procédure d'assurance qualité ainsi que des prescriptions pour le nouveau matériel. Le plan d'assurance qualité pour le matériel est étroitement lié aux procédures d'autorisation liées à la sûreté et doit comprendre toutes les activités menées pendant la vie du système programmé par l'opérateur, le propriétaire, les fournisseurs et les sous-traitants.

3 Project structure

Any project will normally be divided up 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.

For applications important to safety, these phases shall be formalized and none of the identified phases shall be omitted.

Some hardware and software phases may be performed simultaneously. Formalized procedures shall be defined to regulate the feedback between phases.

Project management documentation shall be provided to define the project subdivision so that the project can be run in a controlled manner with evolutions recorded and monitored. A quality assurance plan shall be applied.

3.1 *Project subdivision*

The following general factors determine the activities in implementing a project:

a) The whole system life cycle (annex A) shall be considered.

b) Each phase of the system life cycle shall be divided into elementary tasks with a well defined activity for each of them.

c) Hardware products to be introduced into a phase shall be checked, verified and tested as appropriate before incorporation.

d) Adequate means (spare parts, devices for test or maintenance) and accommodation (laboratories, workshops, space, etc.) shall be provided to carry out the tasks of each phase.

e) Each phase shall include generation of the appropriate documents.

f) Each phase shall be terminated by verification (see clause 6).

g) Every verification step shall result in a report on the analysis performed, the conclusions reached and any necessary changes decided. This report shall be included in the documentation.

h) The time schedule of the project shall be laid down with regard to:

- facilitating feedback between hardware and software phases;
- providing sufficient time for documentation, testing, verification, maintenance and quality assurance;
- giving a means for the recognition of difficulties which arise unexpectedly.

3.2 *Quality assurance*

A hardware quality assurance plan shall exist as a part of the quality assurance plan for the computer system. It should include requirements for hardware which already has undergone a quality assurance procedure as well as for new hardware. The hardware quality assurance plan is closely connected to the licensing procedures. All activities during the computer lifetime executed by the plant operator, owner, contractors and subcontractors shall be included.

Il comprend les phases suivantes:

- conception et développement;
- approvisionnement;
- fabrication;
- installation et mise en service;
- exploitation et maintenance.

Le plan d'assurance qualité décrit à la fois l'organisation, la gestion et la réalisation des activités ayant trait à l'assurance qualité, y compris:

- le contrôle des spécifications;
- le contrôle de la conception et des modifications éventuelles;
- le contrôle des approvisionnements;
- le contrôle des instructions, procédures, plans;
- le contrôle de la documentation;
- le contrôle de l'approvisionnement des matériels et des services;
- l'identification et le contrôle des matériaux;
- les inspections;
- le contrôle des matériels d'essais;
- le contrôle de la manutention, du stockage, du transport;
- l'état des inspections et des essais;
- la surveillance des non-conformités et des actions correctives;
- la production des enregistrements de l'assurance qualité;
- les audits.

4 Prescriptions du matériel

Les prescriptions du matériel sont issues des prescriptions des systèmes importants pour la sûreté et font partie des spécifications du système programmé. Ces spécifications présentent une description à la fois du matériel et du logiciel et définissent les objectifs et les fonctions du système programmé.

Les prescriptions du matériel doivent être décrites dans la spécification des prescriptions du matériel.

La spécification des prescriptions du matériel fait partie de la documentation du matériel (voir 13.2).

Les prescriptions du matériel doivent être présentées selon un modèle dont le formalisme ne doit pas nuire à la compréhension.

Les prescriptions doivent être non ambiguës, testables, vérifiables et réalisables.

La spécification des prescriptions du matériel doit être structurée de manière à donner comme introduction, une vue d'ensemble des prescriptions, avec mention des documents de référence et de l'édition à utiliser, et permettre d'identifier les fonctions du matériel importantes pour la sûreté.

Les prescriptions du matériel sont constituées des prescriptions fonctionnelles et de performances, des prescriptions de fiabilité, d'environnement et de documentation.

Les principes du Guide de sûreté 50-SG-D3 de l'AIEA, et spécialement ceux figurant en 7.12 et 7.32, sont applicables en ce qui concerne l'interface homme/machine et les procédures de fonctionnement et de maintenance.

Les moyens matériels destinés au chargement et au contrôle des programmes et des données et à la vérification pendant la mise en route et le fonctionnement normal ne font pas partie du système programmé requis pour le fonctionnement continu. Les prescriptions de fiabilité figurant en 4.2 peuvent être, pour ces moyens, différentes de celles relatives au système programmé.

Les prescriptions relatives au matériel des systèmes programmés comprennent à la fois des prescriptions applicables au matériel en général et d'autres prescriptions applicables uniquement au matériel du système programmé.

This includes the following phases:

- design and development;
- procurement;
- manufacturing;
- construction and commissioning;
- operation and maintenance.

The quality assurance plan shall describe the organization, management and execution of quality assurance orientated activities including:

- specifications control;
- design and design changes control;
- procurement control;
- control of instructions, procedures, drawings;
- document control;
- control of purchase material and services;
- identification and control of material;
- inspection;
- control of test equipment;
- control of handling/storage/shipping;
- inspection and testing status;
- monitoring of non-conformance and corrective actions;
- production of quality assurance records;
- audits.

4 Hardware requirements

The hardware requirements shall be derived from the requirements of the systems important to safety and form part of the computer system specification. The computer system specification is a description of the combined hardware/software system and states the objectives and functions assigned to the computer system.

The hardware requirements shall be described in the hardware requirements specification.

The hardware requirements specification is part of the hardware documentation (see 13.2).

Hardware requirements shall be presented according to a standard whose formality shall not preclude readability.

The requirements shall be unambiguous, testable, verifiable and achievable.

The hardware requirements specification shall be structured to give as an introduction, an overview of hardware requirements with a list of reference documents and the edition to be used and to identify the hardware functions important to safety.

The hardware functional and performance requirements, the reliability, the environmental and documentation requirements form the hardware requirements.

For man/machine interface, operating procedures and maintenance, the principles of Safety Guide 50-SG-D3 of the IAEA in general, and with particular considerations given to 7.12 and 7.32, are applicable.

The hardware facilities for program and data loading and checking as well as verification during start up and normal operation do not form an intrinsic part of the computer system required for continuous operation. The reliability requirements of 4.2 for these facilities may be different from those of the computer system.

The hardware requirements for computer systems include requirements which are applicable to hardware in general and requirements which are applicable to computer system hardware only.

Les prescriptions relatives au matériel décrivent le produit et non le projet. Il convient de définir les fonctions à accomplir, plutôt que les moyens de les exécuter. Les prescriptions relatives au matériel doivent décrire ce qui doit être fait et non la manière de le faire.

4.1 *Prescriptions fonctionnelles et de performances du matériel*

Les prescriptions fonctionnelles et de performances du matériel sont issues des prescriptions des systèmes importants pour la sûreté.

Elles doivent résulter d'une première phase de conception au niveau du système permettant:

- la définition de l'architecture globale du système programmé et sa division en sous-systèmes remplissant les fonctions requises;
- la définition de la structure distribuée des sous-systèmes;
- l'affectation des prescriptions de performances du matériel à ces sous-systèmes.

Les prescriptions fonctionnelles et de performances du matériel en combinaison avec les prescriptions du logiciel doivent être vérifiées par rapport aux prescriptions du système important pour la sûreté.

Toutes les parties du système comprenant des programmes intégrés et cela jusqu'au niveau des composants doivent être identifiées, leurs fonctions et leurs programmes doivent être spécifiés et conçus de façon appropriée en accord avec l'article 6 de la CEI 880.

a) Les prescriptions fonctionnelles du matériel doivent comprendre, sans toutefois s'y limiter, la définition:

- des tâches du matériel du système programmé et des sous-systèmes;
- de la structure du matériel du système programmé;
- du nombre et du type des capteurs et actionneurs qu'il faut connecter au système;
- du nombre et du type des dispositifs pour l'interface homme/machine, tels que les visualisations, les imprimantes et les claviers.

b) Les prescriptions fonctionnelles du matériel doivent définir clairement le niveau auquel il convient d'intégrer un sous-système au système. Pour les sous-systèmes, la définition doit comprendre l'identification des armoires, unités de traitement, circuits imprimés et circuits intégrés.Les prescriptions de conception seront choisies en fonction de ces niveaux (voir article 5).

Chaque composant ou sous-système livré par un fournisseur pour être intégré au système doit être accompagné d'une spécification détaillée.

c) Les prescriptions de performances du matériel doivent comprendre, sans toutefois s'y limiter, la définition:

- du taux de saisie des données;
- de la capacité de traitement des données;
- de la vitesse de calcul et de transmission de données;
- de la précision de calcul et de conversion;
- de la réjection de bruit;
- du temps de réponse.

Pour la conception des sous-systèmes, les prescriptions de performances doivent être choisies en fonction des niveaux mentionnés en 4.1b).

d) Les prescriptions fonctionnelles et de performances du matériel ainsi que les contraintes réciproques entre matériel et logiciel (voir la CEI 880, annexe A: A2.6) doivent être vérifiées en termes de faisabilité et de ressources en réserves installées à un stade précoce du projet pour éviter d'avoir à faire des modifications ultérieures.

The hardware requirements describe the product, not the project. The hardware requirements shall describe what has to be done and not how it has to be done. That is, the functions to be performed are described, rather than the means of implementation

4.1 *Functional and performance requirements*

The hardware functional and performance requirements are derived from the functional and performance requirements of the systems important to safety.

They shall be the result of a first design phase at system level allowing:

- definition of the overall architecture of the computer system and its division into sub-systems which fulfil the necessary functions;
- definition of the structural distribution of the sub-systems;
- assignment of hardware performance requirements to these sub-systems.

The hardware functional and performance requirements, combined with the software requirements, shall be checked for compliance with the requirements for the systems important to safety.

All parts of the system, down to the component level, which contain built-in programs shall be identified and the functions and programs of those parts shall be appropriately specified in accordance with clause 6 of IEC 880.

a) The hardware functional requirements shall include, but are not restricted to, the definition of:

- the purpose of the computer system hardware and each sub-system;
- the structure of the computer system hardware;
- the number and type of sensors and actuators to be connected to the computer system;
- the number and type of devices for the man/machine interface such as displays, printers and keyboards.

b) The hardware functional requirements shall clearly define the level at which a sub-system is to be integrated into the system. This definition shall identify for the sub-system, the relevant cabinet, frame, printed circuit board and integrated circuits. The design requirements will be selected on the basis of these levels (see clause 5).

Each component or sub-system delivered by a supplier and which is to be integrated into the system shall be accompanied by a complete specification.

c) The hardware performance requirements shall include but are not restricted to the definition of:

- data acquisition rate;
- data handling capability;
- computation and data transmission speed;
- computation and conversion accuracy;
- noise rejection;
- response time.

The performance requirements for the design of sub-systems shall be selected on the basis of the levels mentioned in 4.1b).

d) The hardware functional and performance requirements and mutual constraints between hardware and software (see IEC 880, annex A: A2.6) shall be checked for feasibility, and for the allowance of installed spare capacity, at an early phase of the project, to avoid the need for later changes.

4.2 *Prescriptions de fiabilité*

Les prescriptions de fiabilité du matériel constituent une extension des prescriptions de fiabilité du système important pour la sûreté. Elles doivent comprendre la description des types de défaillance tolérables sans engendrer de perte des fonctions ou entraînant seulement une perte de fonction définie et limitée.

Dans ce contexte, le terme de fiabilité s'applique à la sûreté de la centrale et à sa disponibilité d'exploitation.

a) Aucune défaillance aléatoire unique ne doit pouvoir nuire directement ou indirectement aux actions de sûreté des systèmes de sûreté (voir la CEI 557, 2.19).

Les sous-systèmes redondants doivent suivre les principes de la CEI 639 et prendre en considération les conséquences maximales d'une défaillance ou d'un risque unique, de manière à permettre dans ce cas l'accomplissement des fonctions de sûreté requises.

b) Lors de la conception, une analyse des défaillances venant en complément de l'analyse de sûreté du niveau système doit être réalisée. Une étude appropriée des possibilités de défaillances de mode commun et de défaillances multiples doit figurer dans cette analyse.

L'évaluation de la fiabilité et de la sûreté doit débuter avec la conception.

Les méthodes qui peuvent être utilisées à cet effet sont les suivantes:

- L'analyse par arbre des défaillances qui identifie et analyse les conditions et les facteurs produisant ou contribuant à produire des événements indésirables définis (voir la CEI 1025 [en cours d'impression]).

- L'analyse des modes de défaillances et de leurs effets qui identifie les défaillances dont les conséquences affectent notablement les performances du système, par exemple la fiabilité, la sûreté, la disponibilité (voir la CEI 812).

Il faut noter qu'il est possible de faire une analyse de sûreté du niveau système (matériel et logiciel) au moyen d'une extension de l'analyse par arbre des défaillances.

Il faut apporter une attention toute particulière aux effets:

- des diaphonies dans les mémoires;
- des pannes d'alimentation, des redémarrages qui s'ensuivent et des procédures d'adaptation;
- des pannes des sous-systèmes qui partagent un bus ou d'autres ressources avec d'autres sous-systèmes;
- des interférences électromagnétiques;
- du rayonnement nucléaire.

Toute modification qui s'avérerait nécessaire à la sûreté nucléaire doit être réalisée.

c) Il faut définir les stratégies et les mesures propres à assurer la fiabilité sur toute la durée de vie du système programmé.

Ces mesures doivent être établies en tant que prescriptions de maintenance, qui sont une partie des prescriptions de fiabilité.

Elles doivent comprendre des prescriptions pour:

- le fonctionnement pendant la maintenance;
- le remplacement des sous-systèmes, modules et composants;
- la revalidation;
- faciliter les modifications rétroactives.

4.2 *Reliability requirements*

The hardware reliability requirements represent an expansion of the reliability requirements of the systems important to safety. They shall include a description of the types of failure which have to be tolerated without loss or with a defined and limited loss of function.

In this context, the term reliability is applied to the safety of the plant and its operational availability.

a) No single random hardware failure shall prevent directly or indirectly the safety actions of the safety systems (see IEC 557, 2.19).

Redundant sub-systems shall follow the principles of IEC 639, taking account of the maximum consequences of a single fault or hazard, such that the required safety functions can still be performed.

b) To support the system level safety analysis, an analysis of failures shall be made during design. Proper consideration for the potential for common-mode or common cause failures shall be included in this analysis.

Reliability and safety assessment shall begin as soon as the design starts.

The methods which can be used for this purpose are:

- Fault-tree analysis, which is concerned with the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event (see IEC 1025 [being printed]).

- Failure mode effects analysis, which identifies failures which have significant consequences affecting the system performance, e.g. reliability, safety, availability (see IEC 812).

It is noted that a safety analysis at the system level (hardware and software) can be done through an extension of the fault-tree analysis method.

Special consideration shall be given to the effects of:

- cross-talk in memories;
- power failure and subsequent restart and adaptation procedure;
- failures of sub-systems which share a bus or other resources with other sub-systems;
- electromagnetic interference;
- nuclear radiation.

Any changes shown to be necessary for nuclear safety shall be implemented.

c) Strategies and provisions to assure reliability over the whole lifetime of the computer system shall be defined.

These measures shall be laid down as maintenance requirements, which form part of the reliability requirements.

They shall include requirements for:

- operation during maintenance;
- replacement of sub-systems, modules and components;
- revalidation;
- facilitating backfitting.

d) Pour satisfaire aux prescriptions du matériel en matière de fiabilité, le système programmé doit s'autocontrôler par le logiciel. Pour l'autocontrôle, la CEI 880, 4.8 est applicable.

Les défaillances non autosignalées par ces essais doivent être identifiées et il faut établir les méthodes servant à détecter les défaillances.

Les caractéristiques du matériel, nécessaires pour améliorer la conception et la réalisation d'autotests, sont par exemple:

- les dispositifs de détection et de correction d'erreurs pour les mémoires;
- les dispositifs de détection d'erreurs pour les bus;
- la répétition des instructions sur détection d'erreurs;
- la supervision du temps d'exécution;
- la gestion des mémoires avec protection de parties de la mémoire;
- la redondance au niveau des composants, associée à une logique de vote.

e) La fiabilité requise pour le système et les sous-systèmes doit être classée en fonction de son importance pour la sûreté (voir les Guides de sûreté de l'AIEA 50-SG-D3 et D8; pour les dispositifs de support, voir également le Guide de sûreté 50-SG-D7).

f) Le système doit être conçu de manière à permettre la réalisation aisée des activités de maintenance. Les prescriptions du matériel doivent en principe fournir les valeurs des principaux paramètres de maintenance (tels que le temps moyen de réparation, la maintenabilité et le temps moyen de revalidation) et spécifier les prescriptions concernant les méthodes et les moyens nécessaires à l'accomplissement des activités et des objectifs de maintenance.

Ces méthodes comprennent, par exemple, l'accessibilité en service, la modularité, le suivi des défaillances des unités amovibles, les indicateurs des défaillances, l'enregistrement et l'évaluation de l'historique du fonctionnement et des défaillances.

Les prescriptions en matière de maintenabilité du matériel doivent être définies en se basant sur les prescriptions de fiabilité de la centrale nucléaire.

4.3 *Prescriptions relatives à l'environnement*

Les prescriptions en matière d'environnement du matériel doivent comprendre les conditions d'emplacement, les conditions climatiques, sismiques, chimiques, électriques et les conditions de rayonnement de l'endroit où est appelé à fonctionner le système programmé. Il faut accorder une attention particulière à l'environnement avant et pendant l'installation et la mise en service.

L'environnement électrique du système peut être affecté par une grande variété de sources de perturbations, comme par exemple les disjoncteurs, contacteurs, relais, walkies-talkies, décharges électrostatiques, coups de foudre et défauts de mise à la terre.

Le degré d'immunité aux perturbations magnétiques, électriques et électromagnétiques doit être spécifié et testé conformément à la CEI 801.

Les niveaux de sévérité des essais pour les sous-systèmes doivent être choisis pour les conditions d'installation et d'environnement les plus réalistes.

Les prescriptions du matériel doivent inclure toutes les conditions d'environnement imposées pour le choix des types de constituants, de matériels spéciaux utilisés ou de types particuliers de processus de production et de stratégies d'essais.

4.4 *Prescriptions relatives à la documentation*

Les prescriptions ayant trait à la documentation du matériel font partie des prescriptions sur les systèmes programmés. Elles doivent définir la documentation à livrer avec le produit et comprendre les procédures agréées:

d) In order to meet the reliability requirements, the computer system shall supervise itself by software means. For self-supervision, IEC 880, 4.8 is applicable.

Failures which cannot be made self-annunciating by these tests shall be identified and methods specified by which the failures will be detected.

Hardware features necessary to support the design and performance of self check may include:

- error detection/correction devices for memories;
- error detection devices for busses;
- instruction repetition on error detection;
- runtime supervision;
- memory management with protection of parts of the memory;
- redundancy on the component level in connection with voting logic.

e) The required reliability of the system and the sub-systems shall be classified according to its importance to safety (see IAEA Safety Guides 50-SG-D3 and D8; for support features, see also Safety Guide 50-SG-D7).

f) The system shall be designed to allow maintenance activities to be carried out simply. The hardware requirements should give figures for the major maintenance parameters (such as mean time to repair, maintainability, and mean time to revalidate) and specify the requirements for methods or provisions by which the appropriate maintenance activities and targets are achieved.

These methods may include in-service accessibility, modularity, fault traceability to replaceable units, fault indicators, logging and evaluation of operation and fault history.

The hardware maintainability requirements shall be defined using as a background the reliability requirements of the nuclear power station.

4.3 *Environmental requirements*

The hardware environmental requirements shall include location, climatic, seismic, chemical, electrical and radiation conditions where the computer system is operated. Special consideration shall be given to the environment before and during installation and start-up.

The electrical environment in which the computer is located may be affected by a wide variety of electrical interference sources, e.g. switchgear, contactors, relays, walkie-talkies, electrostatic discharges, lightning, earth faults.

The degree of immunity to magnetic, electrical and electromagnetic interference shall be specified and tested according to IEC 801.

The test severity levels for sub-systems shall be selected in accordance with the most realistic installation and environmental conditions.

The hardware requirements shall include any environmental conditions imposed on the choice of part types, special materials to be used or particular types of production processes and testing strategies.

4.4 *Documentation requirements*

The hardware documentation requirements are part of the documentation requirements of the computer systems. They shall define the documentation to be produced with the product and shall include agreed procedures:

- pour l'identification des différentes parties de la documentation et la garantie de leur mise à jour;
- pour l'identification des signaux et composants du système;
- pour la description des fonctions importantes pour la sûreté;
- pour la description des fonctions figurant dans les manuels des opérateurs et les manuels de maintenance;
- pour la description du contenu et des limites des unités fonctionnelles (modules);
- pour la modification de la documentation.

a) Il faut décrire la configuration du système programmé en se basant à la fois sur les prescriptions de fiabilité du système et sur celles de l'environnement, en raison des relations étroites qui existent entre les propriétés de fiabilité et la configuration du système.

b) Il faut identifier et documenter l'interface entre le système programmé et tout autre système situé dans la centrale ou à l'extérieur de celle-ci, dans le cas d'une connexion directe existante ou prévue; il faut donc indiquer les interfaces spécifiques et les prescriptions associées pour le matériel (voir la CEI 639).

c) Il faut décrire les contraintes que s'imposent mutuellement le matériel et le logiciel.

d) Il faut décrire les contraintes imposées au matériel pour les conditions particulières de fonctionnement (voir la CEI 880: 4.7 et annexe A: A2.7).

5 Conception et développement

Cet article est applicable aux systèmes, sous-systèmes et modules selon le niveau approprié. La conception et le développement sont interactifs et doivent être conformes à la spécification des prescriptions du matériel.

La conception et le développement commencent avec la spécification des prescriptions du matériel, se poursuivent au cours d'étapes de divers niveaux de détail et s'achèvent par la définition d'un produit dont on a prouvé la conformité aux prescriptions du matériel. A chaque étape, les activités suivent le même cadre (voir l'annexe A).

Le niveau plus général de l'activité de conception est l'étude de l'avant-projet qui est l'analyse des différentes possibilités de conception, visant à définir l'architecture matérielle du système en termes de sous-systèmes et de modules.

La conception de l'avant-projet est suivie d'un ou de plusieurs niveaux d'étude de projet détaillé. Les études des projets détaillés enrichissent l'avant-projet pour apporter une description plus détaillée au niveau des sous-systèmes, modules et composants jusqu'à ce que la description du projet soit suffisamment complète pour permettre la réalisation.

On construit généralement un ensemble de matériels prototypes, d'une part pour démontrer l'interaction satisfaisante entre modules et, d'autre part, pour permettre le fonctionnement simultané matériel/logiciel, de façon à prouver leur compatibilité.

Dans certains cas, on dispose de matériel du commerce pour le développement et la conception du système ou de certaines parties de celui-ci (par exemple matériel doté de logiciel intégré et d'outils de mise en service). Il faut alors établir la preuve de la qualification de ce matériel (voir l'annexe B, la CEI 780: 3.15, 4.2, 5.4, 7.4, etc., et la CEI 880: 5.1.2e)) et de la conformité de son domaine d'application aux prescriptions de conception. Pour les programmes d'application, la CEI 880 est applicable.

NOTE - Dans ce contexte, les programmes résidents sont les programmes informatiques qui constituent une partie inhérente du calculateur pour son fonctionnement ou pour des fonctions d'applications génériques, alors que les programmes d'application sont des programmes de calculateur qui sont uniques pour une application spécifique. Les programmes résidents, associés aux programmes d'application, constituent la totalité des programmes du calculateur .

- to identify parts of the documentation itself and ensure that the documentation is kept up to date;
- to identify signals and components of the system;
- for the description of functions important to safety;
- for the description of functions in the operators' manuals and in the maintenance manuals;
- to describe contents and boundaries of functional units (modules);
- to modify documentation.

a) The computer system configuration shall be described using as a background, the reliability requirements of the system and the environment, since reliability properties and system configuration are closely connected.

b) The interface between the computer system and any other systems either within or outside the nuclear plant, wherever a direct connection exists or is planned, shall be identified and documented, indicating the specific interfaces and related hardware requirements (see IEC 639).

c) The constraints which the hardware and software impose on each other shall be described.

d) The constraints on the hardware of any special operating conditions shall be described (see IEC 880: 4.7 and annex A: A2.7).

5 Design and development

This clause is applicable to system, sub-system and module levels as appropriate. Design and development are interactive with one another and shall conform to the hardware requirements specification.

Design and development starts from the hardware requirements specification, goes through stages of different levels of detail and ends with a definition of a product which has been shown to meet the hardware requirements specification. During each stage, the activities follow the same framework (see annex A).

The more general level of design activity is the preliminary design, which consists of the analysis of different design alternatives in order to define the hardware system architecture in terms of sub-systems and modules.

Preliminary design is followed by one or more detailed design levels. The detailed design activity expands the preliminary design to contain more detailed descriptions on the sub-system, module and component levels to the extent that the design description is sufficiently complete to be implemented.

It is usual to build a set of prototype hardware, not only to demonstrate successful interaction between modules, but also to enable both hardware and software to be operated together in order to demonstrate their compatibility.

In some cases, off-the-shelf available equipment (e.g. hardware with built-in programs and implementation tools) may exist for the development and design of the system or parts of it. In this case, evidence shall be provided that this equipment is qualified (see annex B, IEC 780: 3.15, 4.2, 5.4, 7.4, etc., and IEC 880: 5.1.2e)) and that its scope conforms to the design requirements. For application programs, IEC 880 is applicable.

NOTE - In this context, built-in programs are the computer programs that are an inherent part of the computer equipment for the operation of the computer or for generic application functions, while application programs are computer programs that are unique to the specific application. Built-in programs, together with application programs, form the whole set of computer programs.

5.1 *Activités de conception*

a) Toutes les caractéristiques de performances du système, définies dans les prescriptions du matériel, doivent être analysées et indiquées dans la documentation; il faut d'autre part, prouver que la conception répond *a minima* aux caractéristiques de fonctionnement prévues. Ces caractéristiques comprennent la précision, le temps de réponse, le temps de cycle, les conditions d'environnement et les prescriptions d'alimentation électrique.

b) L'attention des responsables des prescriptions du matériel doit être attirée sur tout obstacle éventuel au respect de celles-ci.

c) Les concepteurs doivent réaliser et enregistrer les essais prouvant les performances requises. La CEI 880, 7.5, est applicable pour des essais supplémentaires du système intégré.

d) Les concepteurs doivent spécifier les activités de maintenance nécessaires pour répondre aux prescriptions de performances et de fiabilité. Ces activités couvrent les essais opérationnels, l'étalonnage, les dépannages, la périodicité des remplacements et les procédures.

e) La preuve de la réalisation de la vie qualifiée spécifiée doit être fournie.

5.2 *Critères de fiabilité*

Il faut effectuer des estimations de la fiabilité des sous-systèmes, modules et composants susceptibles d'affecter la sûreté nucléaire et ils doivent être comparés aux prescriptions de fiabilité du matériel correspondant pour en identifier et corriger les défauts.

a) Il convient d'utiliser la redondance et la diversité pour satisfaire à la fiabilité requise. On doit choisir de préférence des éléments tolérants aux fautes au niveau le plus bas possible.

b) En cas d'utilisation de la redondance ou de la diversité, la conception doit prévoir une indépendance satisfaisante des systèmes et sous-systèmes. Il y a lieu que les alimentations électriques proviennent, par exemple, de sources différentes et qu'une séparation physique les protège contre les effets de l'incendie. Il est possible d'adopter une politique visant à obtenir des composants chez plusieurs fournisseurs.

c) La conception doit prévoir des dispositions facilitant la maintenance. Il convient par exemple de prévoir des dispositifs de signalisation des anomalies et de diagnostic de défauts, des possibilités de remplacement simple d'éléments et d'essais sur le terrain.

5.3 *Interfaces*

Pour les interfaces entre le système de traitement et d'autres systèmes, les principes de la CEI 639 sont applicables.

a) Les systèmes de moindre importance pour la sûreté ne doivent pas risquer d'influencer les performances des systèmes de sûreté de plus haute importance. Il faut, en particulier, démontrer que les défaillances du matériel ou du logiciel du système de moindre importance pour la sûreté ne risquent pas, par exemple, de détruire des données ou augmenter le temps de cycle du système de sûreté de plus haute importance.

b) Il convient de prévoir le projet de manière à être compatible avec celui d'autres systèmes utilisés dans la même centrale. Le système doit également être protégé contre l'endommagement ou les défaillances résultant d'une panne dans les systèmes ou les éléments du système reliés à ce dernier par une interface. Cela s'applique également à l'interface utilisateur.

5.4 *Modification*

Il doit être possible de modifier le projet pour répondre aux modifications des prescriptions fonctionnelles, conformément aux réglementations nationales ou à la pratique des compagnies, ou faire face aux défauts de conception (voir l'article 11).

5.1 *Design activities*

a) All the characteristics of the performance of the system which are defined in the hardware requirements shall be analyzed and stated in the design documentation, and evidence shall be made available to show that the design has at least the performance characteristics listed. Such characteristics include accuracy, time response, cycle time, environmental conditions and electrical supply requirements.

b) Anything affecting the compliance with the hardware requirements shall be brought to the attention of those responsible for the hardware requirements.

c) The designers shall carry out and record such tests as are necessary to show that the required performance has been achieved. For further testing of the integrated system, IEC 880, 7.5 is applicable.

d) The designers shall specify the maintenance activities needed to meet the performance and reliability requirements. This may cover operational tests, calibration, repair, replacement periodicity and procedures.

e) Evidence shall be made available to show that the specified qualified life will be achieved.

5.2 *Reliability criteria*

Estimates shall be made of the reliability of sub-systems, modules and components which may affect nuclear safety and shall be compared with the corresponding hardware reliability requirements to identify and correct deficiencies.

a) Redundancy and diversity should be used to meet the required reliability. Fault tolerant units at the lowest level possible should be preferred.

b) When redundancy or diversity is used, the design shall provide adequate independence of systems and sub-systems. For example, power supplies should be from different sources and physical separation should guard against the effects of fire. A policy of obtaining components from more than one supplier may be applied.

c) The design shall provide facilities which make maintenance easy as far as is compatible with reliability goals. For example, fault annunciation, fault diagnostic features, simple module replacement and in-the-field testing capabilities should be provided.

5.3 *Interfaces*

For interfaces of the computer system with other systems, the principles of IEC 639 are applicable.

a) No systems of lower safety relevance shall be allowed to influence the performance of a system of higher safety relevance. It shall be demonstrated in particular that no hardware and no software failure of the system of lower safety relevance can, for example, destroy data or increase cycle times of the system of higher safety relevance.

b) The design should be made to be compatible with other systems used on the same plant. The system shall also be protected against damage or malfunction as a result of failure in the systems or features of the systems with which it shares an interface. This applies also to the user interface.

5.4 *Modification*

The design shall be capable of being modified to meet changed functional requirements within the spare capacity specified, according to national regulations or company practice, or to overcome design faults (see clause 11).

5.5 *Coupures*

Le système programmé doit être aussi peu sensible que possible aux conséquences de coupures de courte durée de la source d'alimentation garantie. Les opérateurs et le personnel de maintenance doivent disposer des moyens nécessaires pour être avertis de ces coupures d'alimentation. On utilisera de préférence des mémoires non volatiles, non effaçables ou du type ROM, ainsi que le rechargement automatique des programmes, lorsque cela est approprié.

5.6 *Choix de composants*

Les caractéristiques des composants utilisés dans la conception et importants pour la fonction doivent être spécifiées. Les composants doivent répondre à une norme de qualité appropriée. Ils doivent être en principe sélectionnés à partir d'une liste préférentielle. Il faut étudier et vérifier avec précision la qualité des nouveaux composants et des nouvelles techniques d'assemblage à utiliser.

5.7 *Documentation de conception*

La documentation de conception du matériel décrit le matériel du système ainsi que la méthode nécessaire à une mise en œuvre conformes aux prescriptions du matériel. La description du matériel, y compris les descriptions préliminaire et finale, doit être produite par les concepteurs. On utilisera de préférence des formes normalisées de documentation et des outils de conception automatisés.

La documentation de chaque niveau comprend le projet détaillé d'exécution des composants définie au niveau en question, ainsi que les prescriptions du matériel, pour les composants du niveau inférieur. A la fin du projet détaillé d'exécution, les documents ayant trait à la fabrication, l'installation, la mise à disposition, la maintenance et le fonctionnement doivent être disponibles. Il n'est pas indispensable d'y inclure la totalité des instructions sur la fabrication, par contre toutes les informations sur la fabrication, la maintenance et le fonctionnement, importantes pour le respect de la spécification des prescriptions du matériel, doivent y figurer.

5.7.1 *Description préliminaire*

La description préliminaire définit l'architecture du matériel, à savoir la structure et les relations entre les parties du système. Elle comprend le schéma général d'implantation du matériel et les schémas fonctionnels des sous-systèmes et modules de niveau inférieur. Elle comprend également les prescriptions du matériel pour l'étude d'exécution détaillée comme par exemple:

- le nombre et les types d'unités de l'ordinateur central et des autres ordinateurs;
- le nombre, le type et les dimensions des mémoires;
- le nombre et les types d'interfaces;
- le nombre et les types de liaisons de données et de bus.

5.7.2 *Description finale*

Lors de l'achèvement de la conception et de la réalisation du système pour le matériel, une description finale doit être disponible. Celle-ci détaille l'étude d'exécution jusqu'au niveau inférieur et les prescriptions, la philosophie de la conception, les performances, les limitations et autres caractéristiques du matériel.

Les documents correspondants doivent comprendre:

a) Une vue d'ensemble définissant de façon détaillée les limites du matériel.

b) Les références croisées à la conception du système et aux descriptions du logiciel.

c) La subdivision du système en sous-systèmes physiques. Chaque sous-système est décrit en termes de modules et composants principaux.

d) La structure des sous-systèmes et des modules (schémas fonctionnels, schémas des circuits au niveau des portes).

5.5 *Power failure*

The computer system shall be made as insensitive as possible to the consequences of short-term power failures of the guaranteed power supply. Means shall be provided for operators and maintenance staff to be made aware of such power failures. Non-volatile, non-erasable or read-only memories are preferred, as is automatic program reloading where appropriate.

5.6 *Component selection*

The characteristics of the components used in the design which are important to its function shall be specified. The components shall be available to an appropriate quality standard. Components should be chosen from a list of preferred components. The quality of new components or new assembly techniques to be used shall be investigated and proven.

5.7 *Design documentation*

The hardware design documentation describes the hardware system and the method by which the implementation will meet the hardware requirements specification. The hardware description, including preliminary and final description shall be produced by the designers. Standardized forms of documentation and automated design tools should be preferred.

The detailed design documentation of each level includes the detailed design of the components defined at that level and the hardware requirements for components of lower level. Documents for manufacturing, installation, commissioning, maintenance and operation shall be available at the end of detailed design. They need not include all manufacturing instructions but they shall include all manufacturing, maintenance, and operating information which is important to meeting the hardware requirements specification.

5.7.1 *Preliminary description*

The preliminary description defines the hardware architecture, i.e. the structure and relationship between the parts of the system. It includes the general layout of hardware with block diagrams of sub-systems and modules of lower level. It includes also hardware requirements for the detailed design such as:

- the number and types of central processor units and other processors;
- the number, types and capacities of memories;
- the number and types of interfaces;
- the number and types of data links and busses.

5.7.2 *Final description*

At the conclusion of the design and development of the hardware system, a final description shall be available that conveys both the design details down to the lower level and the requirements, design principles, capabilities, limitations and other characteristics of the hardware.

The corresponding documents shall include:

a) An overview defining the boundaries of the hardware to be described in detail.

b) Cross-references to the system design and software descriptions.

c) The subdivision of the system in terms of physical sub-systems. Each sub-system is described in terms of its major modules and components.

d) The sub-system and module structure (block diagrams, circuit diagrams at gate level).

e) Les interfaces du sous-système. Les interfaces sont décrites en termes logiques, physiques, électriques ou autres.

f) Les interfaces du système programmé. Il faut identifier les interfaces avec tout autre système, qu'il soit situé à l'intérieur ou à l'extérieur de la centrale nucléaire, chaque fois qu'une liaison directe existe ou est prévue, en indiquant les interfaces spécifiques et les prescriptions correspondantes du matériel (voir la CEI 639).

g) L'implantation physique. La description de l'implantation physique du matériel, accompagnée de schémas, doit en principe être fournie.

h) Les données de qualification (voir l'article 7).

i) L'approche fiabilité et sûreté. Elle doit en principe décrire comment le matériel satisfait aux prescriptions relatives à la fiabilité du système et aux pannes sûres.

6 Vérification et validation

Le processus de conception et de développement doit comprendre des vérifications formalisées de la conformité du matériel à chaque phase de conception et de développement, aux prescriptions imposées par la phase précédente. Afin d'être plus efficaces, les vérifications doivent être effectuées à partir du début du programme de développement du matériel et non se limiter à la phase d'essais.

Le nombre de vérifications réalisées dépendra de l'importance du système par rapport à la sûreté de la centrale et des effets des défaillances du système. Par exemple, il convient de soumettre le matériel utilisé dans les systèmes de sûreté à un programme de vérifications plus rigoureux que celui utilisé dans les systèmes liés à la sûreté.

La phase de vérification du matériel commence par la vérification des prescriptions de conception du matériel par rapport aux performances du matériel et s'achève lorsque le logiciel d'application est intégré au matériel. Les prescriptions de vérification concernant la phase d'intégration matériel/logiciel du développement du système (7.5 de la CEI 880) sont applicables.

6.1 *Plan de vérification*

Un plan de vérification formalisé doit être établi par le personnel chargé de la vérification afin d'expliciter la méthode utilisée pour vérifier la conception du matériel et contrôler le processus de vérification. Le plan de vérification doit être préparé avant le début des actions de vérification. Il doit en principe expliciter la structure de l'organisation de vérification, les méthodes à utiliser, le niveau de vérification à atteindre, les programmes et autres activités importantes de projet liées à la vérification.

a) Il y a lieu que la vérification soit effectuée parallèlement au processus de conception, afin de pouvoir détecter les erreurs et les corriger le plus rapidement possible.

b) Les actions de vérification formelles ne doivent pas être menées avant la mise à disposition pour vérification du projet ou d'une partie de celui-ci par le personnel chargé de la conception. Après leur mise à disposition pour vérification, le projet et la documentation correspondante doivent être maintenus sous contrôle formel de modification. La compatibilité avec les articles 7 et 8 de la CEI 880 doit être respectée.

c) Après mise à disposition pour vérification, toute modification du projet doit être soumise au personnel de vérification pour examen. Le personnel chargé de la vérification doit déterminer la nécessité de vérifications supplémentaires.

6.2 *Indépendance de la vérification*

Les individus ou les groupes chargés des vérifications de conception doivent être indépendants de ceux qui sont chargés des activités de conception. Les vérificateurs peuvent appartenir au même organisme que les concepteurs:

e) The sub-system interfaces. Interfaces are described as appropriate in logical, physical, electrical or other terms.

f) The computer system interfaces. Interfaces with any other systems either within or outside the nuclear plant, wherever a direct connection exists or is planned, shall be identified showing the specific interfaces and related hardware requirements (see IEC 639).

g) The physical layout. A description with diagrams of the physical layout of the equipment should be provided.

h) Qualification data (see clause 7).

i) The approach to reliability and safety. This should describe how the requirements for system reliability and fail-safe properties are fulfilled by the hardware.

6 Verification and validation

The design and development process shall include formal checks that the hardware at each phase of design and development meets the requirements imposed by the previous phase. In order to ensure maximum efficiency, verification shall be applied from the beginning of the hardware development programme and not during the testing phase alone.

The amount of verification performed will depend upon the importance of the system to plant safety and the effects of system failure. For example, hardware used in safety systems should have a more stringent verification program than that used in safety-related systems.

The hardware verification phase starts with verification of the hardware design requirements against the system performance requirements and ends when the application software is integrated with the hardware. The verification requirements for the hardware/software integration phase of system development of IEC 880, 7.5 are applicable.

6.1 *Verification plan*

A formal verification plan shall be prepared by the verification personnel to document the approach used to verify the hardware design and to control the verification process. The plan shall be prepared prior to initiating verification actions. The plan should document the verification organization structure, verification methods to be used, level of verification to be performed, schedules and other significant project activities related to verification.

a) Verification should be performed in parallel with the design process in order that errors may be detected and corrected as soon as possible.

b) Formal verification actions shall not take place until the design or part of it is released for verification by the design personnel. Once released for verification, the design and related documentation shall be maintained under formal change control. This should be compatible with IEC 880, clauses 7 and 8.

c) After release for verification, all changes to the design shall be submitted to the verification personnel for review. The verification personnel shall determine the need for additional verification.

6.2 *Independence of verification*

Individuals or groups who perform the design verification shall be independent from those who are involved in the design activity. Persons involved with verification may be from the same organization as the individuals responsible for the design:

a) Les qualifications des vérificateurs doivent être similaires à celles des concepteurs.

b) La communication entre concepteurs et vérificateurs doit être documentée de manière formelle afin de permettre le suivi du déroulement des activités de vérification.

c) Les personnes responsables de la vérification doivent déterminer et documenter le niveau de vérification à atteindre.

6.3 *Méthodes*

La vérification de la conception peut s'effectuer par des revues critiques, audits, analyses, essais ou une combinaison de ces différentes méthodes. Les méthodes de vérification utilisées doivent être déterminées par le personnel de vérification. Les éléments de base pour le choix de ces méthodes doivent être documentés de manière assez détaillée pour permettre le contrôle par un personnel n'ayant pas directement participé à la conception ou à la vérification.

a) Le choix de la méthode de vérification doit tenir compte:

- de la classification liée à la sûreté du système (système de sûreté ou système lié à la sûreté);
- des examens et essais effectués dans le cadre des processus normaux de conception et de contrôle de la qualité avec une documentation disponible accompagnant la vérification;
- des précédentes activités de vérification effectuées sur un matériel ou sur des systèmes similaires;
- de la dimension, du degré de maturité et de la complexité du système;
- des données qui peuvent être obtenues à partir d'autres sources telles que les procédures d'assurance qualité ou de qualification d'environnement.

b) Le personnel chargé de la vérification doit choisir les outils ou les instruments d'essais à utiliser pour le programme de vérification. Les outils et méthodes appropriés doivent être fournis pour les essais de sous-systèmes et de composants électroniques pour en garantir l'exhaustivité du test. Il convient d'utiliser des outils automatiques pour assurer la reproductibilité et la documentation des résultats des essais et réduire la probabilité d'erreurs humaines pendant les essais.

c) Les instruments et outils de test utilisés pour les processus de vérification ou d'essais doivent être étalonnés et validés de façon appropriée. Un compte rendu doit être établi pour montrer que les étalonnages valides sont opérationnels au moment où on les utilise.

6.4 *Documentation*

Toutes les activités de vérification doivent donner lieu à un document formel suffisamment détaillé pour permettre la vérification par des personnes qui ne sont pas directement impliquées dans le programme de développement et de vérification. Ce document comprend la documentation du plan des programmes de vérification, les prescriptions, les procédures d'essais, les résultats d'essais, les résultats d'une étude des modifications de la conception et de toutes divergences susceptibles d'être identifiées pendant le processus de vérification du matériel.

a) Il est recommandé de rédiger clairement les procédures d'essais. Elles doivent fournir des instructions par étapes pour la vérification du matériel et contenir des informations détaillées sur l'installation d'essai.

b) Les procédures d'essais doivent contenir des critères satisfaisants/non satisfaisants, non ambigus.

c) Les procédures d'essais mises en œuvre du logiciel doivent être documentées et intégrées dans la documentation d'essais.

6.5 *Divergences*

Les divergences identifiées au cours du processus de vérification doivent être documentées de manière formelle et transmises au personnel de conception pour résolution. La réponse des concepteurs doit être formellement documentée pour fournir une trace identifiable et garantir que toutes les divergences ont été résolues et tous les défauts corrigés.

a) The skills of verification personnel shall be similar to the skills of the people who carried out the design.

b) Communications between the design and verification personnel shall be formally documented to allow traceability of the verification activities.

c) The persons responsible for verification shall determine and document the level of verification to be performed.

6.3 *Methods*

Critical reviews, audits, analysis, tests or a combination of these methods may be used to provide design verification. The verification methods used shall be determined by the verification personnel. The basis for the choice of verification method to be used shall be documented with enough detail to allow auditing by personnel who are not directly involved in the design or verification activities.

a) The choice of verification method should consider the following:

- the safety-related classification of the system (safety system or safety-related system);
- reviews and tests performed as part of the normal design and quality control processes with documentation available to support verification;
- previous verification activities performed on similar hardware or systems;
- system size, maturity and complexity;
- data which may be available from other sources such as quality assurance or environmental qualification processes.

b) Verification personnel shall choose the test tools and instruments to be used in the verification programme. Appropriate tools and methods shall be provided for the testing of sub-systems and electronic components to ensure that they can be thoroughly tested. Automatic test tools should be used to provide for reproducibility and documentation of test results, and to reduce the probability of human errors during the test.

c) Test instruments or test tools used in the verification or testing process shall be calibrated and appropriately validated. A record shall be made to show that valid calibrations are in effect at the same time as the device is used.

6.4 *Documentation*

All verification activities shall be formally documented with sufficient detail to allow auditing by persons not directly involved in the development and verification programme. This includes documentation of the verification programme plan, requirements, test procedures, test results, results of a review of design changes and any discrepancies which are discovered during the hardware verification process.

a) Test procedures should be clearly written, provide step-by-step instructions for hardware verification and should contain detailed information of the test set-up.

b) Test procedures shall contain unambiguous pass/fail criteria.

c) Test procedures implemented by software shall be documented and integrated in the test documentation.

6.5 *Discrepancies*

Discrepancies found during the verification process shall be formally documented and transmitted to the design personnel for resolution. The response of the design personnel shall be formally documented to provide a traceable path to assure that all discrepancies are responded to and all deficiencies are corrected.

6.6 *Changements et modifications*

Après avoir été effectuée avec succès, la vérification ne nécessite pas de répétition tant que les prescriptions du système programmé ne subissent pas de modification. En cas de modification apportée à la conception vérifiée, 6.1c) est applicable.

Les parties modifiées doivent être en principe identifiées conformément aux procédures de contrôle qualité spécifiées.

6.7 *Vérification de l'installation*

La vérification de l'installation correcte du système doit être conforme à l'article 9.

6.8 *Validation*

Des essais doivent être réalisés pour valider le matériel et le logiciel en tant que système conforme aux prescriptions des systèmes importants pour la sûreté, prescriptions devant devant être remplies par le système programmé. Pour cette validation, l'article 8 de la CEI 880 est applicable.

7 Qualification

Le matériel du système programmé doit être qualifié conformément à la CEI 780. La qualification peut être accordée lors d'un certain nombre de phases pendant le développement.

8 Fabrication

Les sous-systèmes, modules et composants à utiliser dans le système programmé comprennent des produits du commerce et des produits matériel spécifiques construits conformément aux documents finaux. La CEI 880, 3.2, est applicable à l'assurance qualité pour les deux classes.

9 Installation et mise en service

9.1 L'emballage, la manutention, le transport, le stockage et le déballage doivent être effectués de manière à éviter d'endommager le système.

9.2 Avant le déballage et l'installation du système, la conformité de son environnement aux prescriptions d'environnement du matériel doit être vérifiée conformément à 4.3.

9.3 Des procédures et informations appropriées doivent être disponibles pour permettre l'installation, le câblage et le raccordement du système conformément aux prescriptions du projet, en particulier pour les prescriptions de mise à la terre. L'identification des parties de l'équipement doit faire partie de cette information. Un plan de qualité doit être appliqué à cet effet. Le système doit être installé, câblé, essayé et mis en fonctionnement conformément à des procédures définies.

9.4 Le bon fonctionnement du système sur le site doit être vérifié par des essais de mise à disposition, planifiés et spécifiés. Un plan d'essai de mise à disposition, qui traite des critères d'acceptation, des cas d'essais et des environnements d'essais, doit être établi.

Chaque sous-système doit être soumis à des essais pour vérifier son bon fonctionnement.

a) Toute défaillance due à des erreurs de conception et toute modification destinée à améliorer les performances du système doivent être consignées dans un compte rendu. Une procédure formelle conforme à l'article 11 doit être utilisée pour contrôler les modifications nécessaires.

b) Toute défaillance due à des erreurs de fabrication doit faire l'objet d'un compte rendu. Les parties défectueuses doivent être remplacées uniquement par des parties neuves ayant satisfait à des essais en usine. Le processus de fabrication et les essais en usine doivent être vérifiés et modifiés le cas échéant afin d'éviter de nouvelles livraisons de parties défectueuses.

c) Tout défaut dû à des erreurs d'installation, de câblage ou de filerie doit être corrigé et noté.

6.6 *Changes and modifications*

Once successfully completed, verification is not required to be repeated as long as the computer system requirements are not changed. For changes to the verified design, 6.1c) is applicable.

Modified parts should be identified in accordance with the specified quality control procedures.

6.7 *Installation verification*

Verification of correct system installation shall be in accordance with clause 9.

6.8 *Validation*

Testing shall be performed to validate the software and hardware as a system which complies with the requirements of the systems important to safety to be satisfied by the computer system. For this validation, clause 8 of IEC 880 is applicable.

7 Qualification

The computer system hardware shall be qualified according to IEC 780. Qualification may be achieved at a number of phases during development.

8 Manufacture

The sub-systems, modules and components to be used in the computer system include off-the-shelf products and dedicated hardware products built in accordance with the final documents. IEC 880, 3.2, is applicable to quality assurance for both classes.

9 Installation and commissioning

9.1 Packing, handling, transport, storage and unpacking shall be such as to prevent any damage to the system.

9.2 Before the system is unpacked and installed, the environment in which the system is to be installed shall be verified to conform to the hardware environmental requirements of 4.3.

9.3 Adequate procedures and information shall be available to enable the system to be installed, cabled and wired in accordance with the design requirements, in particular with regard to the earthing requirements. Identification of items of equipment shall form part of this information. For this purpose, a quality plan shall be applied. The system shall be installed, cabled, tested and set to work in accordance with defined procedures.

9.4 The proper working of the system at site shall be checked by planned and specified commissioning tests. A commissioning test plan, consisting of acceptance criteria, test cases and test environments, shall be established.

For each sub-system, tests shall be carried out to demonstrate its correct function.

a) Any defect due to design errors or any change to improve the system performance shall be recorded. A formal procedure according to clause 11 shall be used to control the necessary changes.

b) Any defect due to manufacturing errors shall be recorded. Defective parts shall be replaced only by new parts which have undergone factory testing. The manufacturing process and the factory testing shall be investigated and changed if necessary to avoid further delivery of defective parts.

c) Any defect due to errors in installation, cabling or wiring shall be corrected and recorded.

9.5 L'immunité aux perturbations électriques du système programmé doit faire l'objet d'essais dans les conditions finales installées.

Les essais doivent être réalisés conformément aux CEI 801-1, 2, 3 et 4. Voir aussi 4.3.

Le niveau de sévérité des essais de perturbations électromagnétiques doit être déterminé dans les conditions d'installation et d'environnement les plus défavorables auxquelles le système peut être soumis.

9.6 Après achèvement de l'installation et mise à disposition, il convient de mener une procédure d'acceptation avant de transférer le système à l'utilisateur.

10 Maintenance

La maintenance du matériel comprend:

- des essais, vérifications et étalonnages réalisés périodiquement à des intervalles maximaux spécifiés ou après remplacements, échanges, révisions et réparations (revalidation);

- une maintenance destinée à conserver le matériel de l'ordinateur en bon état de fonctionnement, telle que le remplacement des matériels courants, les échanges préventifs et la révision du matériel des sous-unités, parties et composants;

- des réparations, telles que la restauration de l'opérabilité des matériels défectueux, des sous-unités et parties.

10.1 *Activités de maintenance*

a) Une procédure formelle doit être spécifiée et appliquée dans le but de contrôler l'exécution et la documentation de la maintenance (voir l'annexe C).

Elle doit prendre en considération:

- les préparations de structures, si les activités de maintenance affectent le fonctionnement de la centrale;

- les préparations de fonctionnement des systèmes importants pour la sûreté et celles des composants de la centrale.

b) Le travail accompli pour mener les tâches décrites en 10.1a) doit être exclusivement confié à un personnel qualifié et autorisé. Il doit être noté suivant une procédure spécifiée. Cette procédure doit stipuler la certification, assurée par une personne autorisée, que chaque tâche a été accomplie de façon satisfaisante.

D'autres informations appropriées comme l'heure, la date, la mention des pièces remplacées, etc., doivent être également notées. Il convient de suivre l'usage national ou pratiqué par le client pour l'autorisation de la documentation.

c) Les travaux de maintenance doivent être soumis à des vérifications.

d) Le fonctionnement satisfaisant en service dépend de l'application de contrôles destinés à vérifier que le remplacement des pièces s'effectue après une période n'excédant pas la durée de vie qualifiée (voir la CEI 780) et que les pièces de rechange sont d'une qualité appropriée à leur tâche. Il faut s'assurer que les fournisseurs de composants, modules, sous-systèmes et de systèmes dans leur ensemble ont bien l'intention d'assurer la fourniture de ces pièces de rechange.

Les pièces de rechange doivent être entreposées dans un local où s'exercent des contrôles de température, d'humidité, de teneur en gaz et particules de l'atmosphère. L'entrepôt doit être conçu de manière à limiter les effets du feu sur les pièces de rechange. Leur durée de conservation doit faire l'objet de contrôles à intervalles spécifiés, conformément aux instructions de maintenance.

9.5 The immunity of the computer system to electromagnetic interference shall be tested in the final installed conditions.

The tests shall be performed in accordance with IEC 801-1, 2, 3 and 4. See also 4.3.

The severity level of electromagnetic interference shall be chosen such that it conforms to the worst conditions to which the system may be subjected.

9.6 On the completion of installation and commissioning, it is necessary to carry out the process of acceptance before the system is transferred to the user.

10 Maintenance

Hardware maintenance comprises:

- tests, checks and calibration which may be either periodic within specified maximum intervals or after replacement, exchange, overhaul and repair (revalidation);

- maintenance such as is required to maintain the computer hardware in good working order, replacement of expendables and the preventative exchange and overhaul of equipment, subunits, parts and components;

- repairs, the restoration of the operability of failed equipment, sub-units and parts.

10.1 *Maintenance requirements*

a) A formal procedure shall be specified and applied to control the execution and the documentation of maintenance (see annex C).

This shall take into account:

- organizational preparations if the maintenance activities affect plant operation;

- operational preparations of the systems important to safety and of plant components.

b) Maintenance shall be undertaken by qualified and authorized personnel only. It shall be recorded according to a specified procedure. The procedure shall make provision for personal certification by an authorized person that each task has been completed satisfactorily.

Other relevant information, such as time and date, replacements fitted, etc., shall also be recorded. National or customer authorization documentation practice should be followed.

c) Maintenance work shall be subject to audits.

d) Satisfactory operation in service depends upon the application of controls to ensure that parts are replaced after a period of time not longer than the qualified life (see IEC 780) and that the replacement parts are of a quality appropriate to their duty. The suppliers of components, modules, sub-systems and the systems in total shall be shown to intend to continue to provide such replacement.

Spare parts shall be kept in a store whose atmosphere is controlled with regard to temperature, humidity, gases and particles. The store shall be constructed in such a way that the effects of fire on the spare parts are minimized. The shelf life of spare parts shall be controlled within specified intervals according to maintenance instructions.

e) Seules les pièces de rechange qualifiées conformément à l'article 7 doivent être utilisées.

f) Les pièces de rechange dans leur ensemble et les pièces de rechanges modifiées doivent être identifiables au-dessus du niveau des composants.

10.2 *Données de défaillance*

Il faut envisager d'établir des statistiques du taux de défaillance à partir des comptes rendus de réparation.

L'acquisition de données de défaillance pendant le fonctionnement du matériel constitue une source majeure d'informations que l'on peut utiliser pour améliorer:

- les connaissances sur les données de fiabilité des composants, en prenant en considération les conditions réelles de fonctionnement de l'environnement;

- les évaluations sur la fiabilité du matériel afin de déterminer le taux effectif de défaillances sur le site et la disponibilité observée en fonctionnement;

- la politique de maintenance grâce à une optimisation des pièces détachées, à des programmes de maintenance préventifs et à des prescriptions sur le personnel de maintenance.

Il convient que les données de défaillances sur le site soient consignées dans une banque de données de défaillances, à partir des informations issues des comptes rendus de maintenance.

Les comptes rendus de maintenance doivent mentionner:

- l'identification du matériel;
- la description de défauts;
- la référence à un compte rendu éventuel du problème;
- la date de l'intervention;
- la durée de l'intervention;
- l'identification des composants défaillants avec éventuellement l'identification de l'équipement primaire défaillant (origine d'une cascade de défaillances);
- l'âge des composants;
- la localisation des composants;
- les circonstances des défaillances et leurs effets.

NOTE - La CEI 812 peut fournir une méthodologie pour les mesures de fiabilité.

10.3 *Documentation de maintenance*

Les instructions pour la maintenance doivent être fournies par écrit sous la forme de manuels, guides, etc.

Les documents de maintenance doivent décrire une politique de maintenance pour le type des composants du matériel et du logiciel qui sont vérifiés, revérifiés ou substitués (voir 10.1e)).

Les documents de maintenance doivent décrire comment sont mises en évidence et diagnostiquées les défaillances dans chaque partie spécifique du système.

Les documents de maintenance doivent décrire une politique de réparation, à savoir:

- les méthodes de réparation ou substitution des différents sous-systèmes, modules et composants;
- les restrictions auxquelles est soumis le système pendant les réparations (par exemple le système ou les parties du système qu'il faut mettre hors tension);
- la nécessité de revalider un système après une réparation.

Outre les procédures de maintenance périodique programmée, il faut prévoir des procédures à utiliser dans le cas où un comportement anormal du système laisserait supposer une défaillance ou une erreur de conception.

e) Only spares qualified according to clause 7 shall be used.

f) Replacement parts in general as well as modified replacement parts shall be identifiable above component level.

10.2 *Failure data*

Consideration shall be given to the derivation of failure data statistics from the equipment repair records.

Failure data acquisition during equipment operation constitutes a major source of information which can be used to improve:

- component reliability data knowledge by taking into account real operating environment conditions;

- equipment reliability evaluations by determining actual field failure data and by observing availability in operating conditions;

- maintenance policy through better spare parts optimization, preventative maintenance schedules and maintenance personnel requirements.

Accordingly field failure data should be logged in a failure data bank using information available from maintenance reports.

The maintenance reports shall contain:

- equipment identification;
- description of fault;
- reference to eventual problem report;
- date of intervention;
- intervention duration;
- failure component identification with eventual primary failed component (origin of a cascade of component failures);
- component age;
- component localization;
- failure circumstances and failure effects.

NOTE - IEC 812 may be used to provide a methodology for reliability measurements.

10.3 *Maintenance documentation*

Instructions for maintenance shall be provided in written form by means of procedures, manuals, handbooks, etc.

Maintenance documents shall describe maintenance policy for the type of hardware components which are checked and when they are rechecked or substituted (see 10.1e)).

Maintenance documents shall describe the way in which failure of each specific module of the system is made apparent and diagnosed.

Maintenance documents shall describe repair policy, i.e.:

- the methods of repair or substitution of different sub-systems, modules and components;
- the restrictions to which the system is subjected during repair time (e.g. the system or parts of the system which shall be switched off);
- the extent to which the system shall be revalidated after a repair.

In addition to the procedures for scheduled periodic maintenance, procedures shall be provided to be used for cases where anomalous system behavior leads to suspicion of failure or design error.

11 Modifications

Pour corriger un fonctionnement défectueux ou prendre en compte des prescriptions de fonctionnement nouvelles ou révisées, on peut être amené à exiger des modifications du matériel.

Toute modification nécessaire pour répondre à des prescriptions supplémentaires ou modifiées doit être signalée afin d'attirer l'attention des responsables des prescriptions du matériel.

11.1 Les modifications du matériel apportées pendant la conception doivent être contrôlées par une procédure formelle. Il convient que cette procédure soit compatible avec les procédures utilisées pour le contrôle des modifications du logiciel et qu'elle garantisse l'identification des parties modifiées, conformément à la procédure de contrôle qualité spécifiée.

11.2 Une procédure formelle doit être utilisée pour contrôler les modifications de la conception et du matériel par rapport à la conception d'origine approuvée ou aux objectifs d'essais; il convient que la procédure soit compatible avec la CEI 880, articles 7 et 9, et avec la procédure de contrôle des modifications de conception du logiciel.

11.3 Les conséquences de ces modifications sur le logiciel doivent être examinées conformément à 9.3.3 de la CEI 880.

11.4 On doit établir que le matériel ayant subi des modifications répond à la spécification des prescriptions d'intégration matériel/logiciel figurant à l'article 7 de la CEI 880.

11.5 On doit établir que le matériel modifié satisfait aux spécifications des prescriptions du matériel de l'article 4.

11.6 Pour la vérification du matériel modifié, 6.1c) et 6.4 sont applicables. Dans les cas où les vérificateurs de la conception d'origine ne seraient pas disponibles, les prescriptions de 6.2 sur le personnel chargé de la vérification doivent être satisfaites en conséquence.

11.7 Les modifications après mise à disposition et acceptation doivent suivre une procédure formelle. Selon le type de modification, il peut s'avérer nécessaire de revenir à la phase de projet de détail ou bien même au niveau du système.

12 Exploitation

Outre les prescriptions de l'article 10 de la CEI 880, les prescriptions suivantes s'appliquent pour le fonctionnement du système programmé. Une méthode permettant de contrôler l'agrément des manuels et procédures et l'habilitation du personnel d'exploitation doit être appliquée conformément à la réglementation et aux pratiques nationales.

12.1 Il faut prévoir des procédures de fonctionnement devant être considérées comme des instructions obligatoires et non comme des guides.

12.2 Les procédures doivent inclure la marche à suivre dans les cas non envisagés pour signaler ces situations à une personne ou à un groupe de personnes habilitées afin de décider ce qu'il faut faire.

12.3 La décision de s'écarter d'une procédure autorisée ne peut être prise que par une personne ou un groupe de personnes habilitées et doit être documentée de façon détaillée.

12.4 Les prescriptions de 10.3 doivent s'appliquer aux procédures de fonctionnement.

12.5 Toutes les personnes dites "habilitées" doivent préalablement suivre une formation appropriée et on doit appliquer un système formel de certification. On peut prévoir un système de réentraînement périodique et de recertification dans le cas où la certification d'origine serait remise en question, comme par exemple à la suite d'une affectation temporaire à un type de travail différent ou d'une modification importante du matériel installé. Le terme de "personnes habilitées" recouvre dans ce cas toutes les personnes spécifiquement habilitées à mener des tâches particulières dans le cadre de la centrale. Il comprend le personnel d'exploitation, de maintenance et de dépannage.

11 Modification

Hardware modification may be required to correct defective performance or to cater to new or revised performance requirements.

Any change necessary to fulfil additional or changed requirements shall be brought to the attention of those responsible for the hardware requirements.

11.1 Hardware changes made during design shall be controlled by a formal procedure. The procedure should be compatible with the procedure used to control software changes and should ensure that the modified parts are identified in accordance with the specified quality control procedure.

11.2 A formal procedure shall be used to control design and hardware changes to the original approved design or test intent. The procedure should be compatible with IEC 880, clauses 7 and 9, and with the procedure used to control software design changes.

11.3 The effect of the modification on the software shall be examined according to 9.3.3 of IEC 880.

11.4 The changed hardware shall be shown to meet the hardware/software integration requirements specification of clause 7 of IEC 880.

11.5 The changed hardware shall be shown to meet the hardware requirements specifications of clause 4.

11.6. For the verification of changed hardware, 6.1c) and 6.4 are applicable. In cases where the verification personnel for the original design are not available, the requirements of 6.2 with regard to the verification personnel shall be met accordingly.

11.7 Modifications after commissioning and acceptance shall follow a formal procedure. Depending on the kind of modification, it may be necessary to return to the detail design phase or even to the system level.

12 Operation

In addition to the requirements of IEC 880, clause 10, the following requirements are applicable to the operation of the computer system. A method of controlling the authorization of manuals, procedures and personnel shall be applied in accordance with national regulations and practice.

12.1 Operating procedures shall be provided and they shall be treated as mandatory instructions, not as guides.

12.2 The procedures shall include activities to be followed in circumstances not explicitly provided for in order to bring these situations to the attention of an authorized person or group of persons to determine what is to be done.

12.3 Any decision to deviate from an authorized procedure shall be made only by an authorized person or group of persons, and shall be comprehensively documented.

12.4 The requirements of 10.3 shall apply to the operating procedures.

12.5 All persons classed as authorized persons shall be properly trained before authorization and a formal certification system applied. A system of periodic retraining and recertification may be provided if it is possible for the original certification to be in doubt, for example following a temporary assignment to a different kind of work or major changes to the installed equipment. The term "authorized persons" is used in this connection to describe all who are specifically authorized to carry out particular duties in relation to the plant. It includes operating staff, maintenance and repair personnel.