

**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**

© IEC 1989 Droits de reproduction réservés — Copyright - all rights reserved

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

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

International Electrotechnical Commission
Telefax: +41 22 919 0300

3, rue de Varembé Geneva, Switzerland
e-mail: inmail@iec.ch IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

T

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

SOMMAIRE

	Pages
AVANT-PROPOS	4
INTRODUCTION	6
Articles	
1 Domaine d'application	6
2 Termes et définitions	6
3 Structure du projet	12
4 Prescriptions du matériel	14
5 Conception et développement	22
6 Vérification et validation	28
7 Qualification	32
8 Fabrication	32
9 Installation et mise en service	32
10 Maintenance	34
11 Modifications	38
12 Exploitation	38
13 Documentation	40
Annexes :	
A - Aperçu général sur le cycle de vie du système	42
B - Grandes lignes du processus de qualification	44
C - Exemple de procédure de maintenance	46

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	7
Clause	
1 Scope	7
2 Terms and definitions	7
3 Project structure	13
4 Hardware requirements	15
5 Design and development	23
6 Verification and validation	29
7 Qualification	33
8 Manufacture	33
9 Installation and commissioning	33
10 Maintenance	35
11 Modification	39
12 Operation	39
13 Documentation	41
Annexes :	
A - Overview of system life cycle	43
B - Outline of qualification	45
C - Example of maintenance procedure	47

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):	Reacteurs 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.