NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
880

Première édition
First edition
1986

Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires

Software for computers in the safety systems of nuclear power stations

Bureau central de la Commission Electrotechnique Internationale 3, rue de Varembé Genève Suisse

IEC

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE
XB

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

LOGICIEL POUR LES CALCULATEURS UTILISÉS DANS LES SYSTÈMES DE SÛRETÉ DES CENTRALES NUCLÉAIRES

PRÉAMBULE

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.

PRÉFACE

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)88-I/II/III	45A(BC)90

Pour de plus amples renseignements, consulter le rapport de vote mentionné dans le tableau ci-dessus.

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

Publications nos 557 (1982): Terminologie CEI sur les réacteurs nucléaires.

639 (1979): Réacteurs nucléaires. Utilisation du système de protection à d'autres fins que la sécurité.

643 (1979): Application des calculateurs numériques à l'instrumentation et à la conduite des réacteurs nucléaires.

671 (1980): Essais périodiques et surveillance du système de protection des réacteurs nucléaires.

Autres publications citées:

Norme ISO 2382/1 (1984): Traitement des données — Vocabulaire — Partie 01: Termes fondamentaux.

Guide de l'AIEA 50-SG-D3 (1980): Guide de sûreté.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SOFTWARE FOR COMPUTERS IN THE SAFETY SYSTEMS OF 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.

PREFACE

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

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

Six Months' Rule	Report on Voting
45A(CO)88-I/II/III	45A(CO)90

Further information can be found in the Report on Voting indicated in the table above.

The following IEC publications are quoted in this standard:

Publications Nos. 557 (1982): IEC Terminology in the Nuclear Reactor Field.
639 (1979): Nuclear Reactor. Use of the Protection System for Non-safety Purposes.
643 (1979): Application of Digital Computers to Nuclear Reactor Instrumentation and Control.
671 (1980): Periodic Tests and Monitoring of the Protection System of Nuclear Reactors.

Other publications quoted:

ISO standard 2382/1 (1984): Data processing — Vocabulary — Part 01: Fundamental terms.
IAEA Guide 50-SG-D3 (1980): Safety guide.

LOGICIEL POUR LES CALCULATEURS UTILISÉS DANS LES SYSTÈMES DE SÛRETÉ DES CENTRALES NUCLÉAIRES

INTRODUCTION

Les principes de base pour la conception de l'instrumentation nucléaire appliqués en particulier aux systèmes de sûreté des centrales nucléaires ont été traités dans les normes existantes, se référant aux systèmes câblés tel le «Guide de sûreté 50-SG-D3» de l'AIEA.

La présente norme a été développée pour interpréter ces principes lors de l'utilisation de systèmes programmés — systèmes multiprocesseurs distribués aussi bien que gros processeurs centraux — dans les systèmes de sûreté des centrales nucléaires. Elle traite des principes et prescriptions relatives au logiciel du système et il convient qu'elle soit employée en association avec les normes appropriées traitant du matériel et de l'intégration du système.

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

Les aspects qui ont été spécialement envisagés, vu le caractère particulier des systèmes programmés et de leur logiciel, sont:

a) les critères auxquels doit répondre le matériel pour autant qu'ils affectent le logiciel, en tenant compte du haut degré d'interdépendance entre le matériel et le logiciel;

b) une approche générale du développement du logiciel pour assurer la production d'un logiciel de grande fiabilité;

c) une approche générale de la vérification du logiciel et de la validation du système programmé;

d) les procédures relatives à la maintenance du logiciel, la modification, la gestion de la configuration.

1. Domaine d'application et objet

Cette norme est applicable au logiciel de haute fiabilité exigé pour les équipements programmés devant être utilisés dans les systèmes de sûreté des centrales nucléaires pour les fonctions liées à la sûreté — fonctions de classe 1, selon la Publication 643 de la CEI: Application des calculateurs numériques à l'instrumentation et à la conduite des réacteurs nucléaires. Cela inclut le système de commande, les systèmes auxiliaires des systèmes de sauvegarde et les systèmes de protection.

Pour les fonctions qui ne sont pas de sûreté, les principes de la Publication 639 de la CEI: Réacteurs nucléaires — Utilisation du système de protection à d'autres fins que la sûreté, sont applicables dans le cas d'utilisation de systèmes programmés.

Cette norme fournit un ensemble de prescriptions pour chaque étape de l'élaboration du logiciel, comprenant la conception, le développement, la qualification et la mise en œuvre, ainsi que la documentation accompagnant chaque étape de l'élaboration du logiciel dans le but d'obtenir un logiciel de haute fiabilité.

Les principes appliqués dans la mise en œuvre de ces prescriptions sont les suivants:

— méthodes les plus avancées;
— conception descendante;
— modularité;
— vérification de chaque phase;
— documentation claire;
— documents pouvant être soumis à audit;
— contrôle de validation.

SOFTWARE FOR COMPUTERS IN THE SAFETY SYSTEMS OF NUCLEAR POWER STATIONS

INTRODUCTION

The basic principles for the design of nuclear instrumentation as specifically applied to the safety systems of nuclear power plants have been interpreted in existing standards with reference to hard-wired systems as the "Safety Guide 50-SG-D3" of the IAEA.

This standard has been developed to interpret these principles for the utilization of digital systems — multiprocessor distributed systems as well as larger scale central processor systems — in the safety systems of nuclear power plants. It discusses the software system principles and requirements and should be read in association with appropriate standards on computer hardware and system integration.

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

Aspects for which special recommendations have been produced, due to the unique nature of computer systems and their software are:

a) established hardware criteria as far as they affect the software, taking careful account of the high degree of interdependency between hardware and software;

b) a general approach to software development to assure the production of the highly reliable software required;

c) a general approach to software verification and computer system validation;

d) procedures for software maintenance, modification and configuration control.

1. Scope and object

This standard is applicable to highly reliable software required for computers to be used in the safety systems of nuclear power plants for safety functions — Class 1 functions according to IEC Publication 643: Application of Digital Computers to Nuclear Reactor Instrumentation and Control. This includes the safety actuation systems, the safety system support features and the protection systems.

For the utilization of computer systems for non-safety functions the principles of IEC Publication 639: Nuclear Reactors — Use of the Protection System for Non-safety Purposes, are applicable.

This standard provides requirements for each stage of software generation, including design, development, qualification and operation as well as the documentation for each stage of the software generation for the purpose of achieving highly reliable software.

The principles applied in developing these requirements include:

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

Des directives et informations complémentaires sur la manière de satisfaire aux prescriptions de la partie principale de cette norme sont données dans les annexes A à F. Les références à ces annexes sont données entre parenthèses.

Si des pratiques différentes de celles figurant dans les annexes sont utilisées, elles doivent être documentées et pouvoir être vérifiées par rapport aux exigences de la partie principale de cette norme.

Additional guidance and information on how to comply with the requirements of the main part of this standard is given in Appendices A to F. References to those appendices are given in brackets.

If practices differing from those of the appendices are used, they shall be documented and auditable according to the requirements of the main part of this standard.