IEC 62646

Edition 1.0 2012-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Control rooms – Computer based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX **W**

ICS 27.120.20

ISBN 978-2-83220-388-0

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – CONTROL ROOMS – COMPUTER BASED PROCEDURES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62646 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/886/FDIS	45A/888/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

This IEC standard focuses on computerisation of procedures used by the operating staff. Procedures have always contributed to a large extent to NPP safety and availability and, now, the use of computer technology to provide enhanced guidance to the plant operators is increasing and becoming current practice. This standard also provides guidance for the decision on the extent the procedures should be computerised.

It is intended that the Standard be used by nuclear power plant designers, utilities operating staff, systems evaluators and by regulatory engineers.

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

IEC 62646 is the third level IEC SC 45A document tackling the generic issue of computerised procedures.

IEC 62646 is to be read in association with IEC 60964 and with IEC 61839. IEC 60964 is the appropriate IEC SC 45A document providing guidance on operator controls, verification and validation of design, application of visual display units in the control room, whereas IEC 61839 establishes functional analysis and assignment guidance for allocating functions between operators and systems.

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

c) Recommendations and limitations regarding the application of the Standard

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

This standard deals with technical requirements and Human Factor Engineering related to Computer Based Procedures (CBP). However it does not provide detailed guidance on ergonomic design of control centres as it is treated in the ISO 11064 series of standards, nor on task allocation between human and systems dealt with in IEC 61839 and on cyber security, which is developed in IEC 62645. It also excludes the organisation for maintenance of procedures.

Aspects for which requirements and recommendations have been provided in this Standard are:

– the establishment of a policy for computerisation of procedures, especially which types of procedure should be computerised and to what extent. The different families of CBP (Computer Based Procedures) to be aimed at, with their associated features, are then defined. Finally, the safety aspects of CBP are considered;

– the use of CBP inside and outside of the MCR (Main Control Room), in possible conjunction with paper based procedures, as well as the assistance provided to operator activities, including user coordination;

– safety and non safety design requirements for the digital system processing CBP, and considerations about what to do in case of failure of this system;

– detailed requirements and recommendations related to the functional features of CBP, from the basic ones to the most sophisticated ones, i.e. information, navigation, guidance and plant control;

– the CBP life cycle, from the set-up of the project to the CBP maintenance and the operator training via design and implementation.

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

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

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

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

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

A fourth level extending the IEC SC 45A standard series, corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements NS-R-1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NOTE It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied, that are based on the requirements of a standard such as IEC 61508.

NUCLEAR POWER PLANTS – CONTROL ROOMS – COMPUTER BASED PROCEDURES

1 Scope

1.1 Object

This International Standard establishes requirements for the whole life cycle of operating procedures that the designer wishes to computerise. It also provides guidance for making decisions about which types of procedures are to be computerised and to what extent. Once computerised, procedures are designated as "Computer Based Procedures" (CBP).

Enhancing safety, easing operation and increasing NPP availability have always been greatly valued aims which, during NPP operation, rely to a large extent on the operating staff and on operating procedures. Digital technology is currently contributing by providing efficient help to do this at the automation level.

In addition, the use of computer technology to provide formats of operating procedures to the plant operators[1], on-line and in real time, is increasing and becoming current practice. This can be done both for normal operating situations and also as advisory formats for use in abnormal situations. When properly implemented and kept up-to-date, such operating procedures can provide enhanced support for greater safety and operator effectiveness compared to paper based procedures. Their preparation demands great care and close interaction with operators and plant designers, and will also need close co-operation with I&C designers.

CBP have many common points with paper based procedures. This standard focuses only on what is specific to CBP.

1.2 CBP overview

Procedures provide the operators with two types of high level elements:

- information, i.e. explanations or data displayed in order to enable the operator to control the process, assess the plant situation, understand operating strategies and make appropriate decisions,
- guidance, i.e. a set of ordered steps for prompting and helping the operator to operate the process and the plant equipment.

Information and guidance are combined to minimise operators errors and to optimise efficiency of plant operation.

These elements can be of a varying level of detail depending on the procedure policy, which aims to benefit from operator experience and predefined guidelines.

Computerisation of procedures can provide, according to the specified design policy:

- enhanced process and plant equipment information,
- enhanced operator guidance,

[1] Operators may be male or female, so that in this standard, “he” is a shortcut for “he / she” and “his” is a shortcut for “his / her”.

- optional automatic plant control.

However, introducing such procedures requires attention to the following issues:

- defining a clear policy on the scope of procedures, level of guidance and possible direct process control for example, taking into account experience from plant operation and human capabilities as well as organisational and technological issues,
- designing a safe and reliable CBP system, and also providing an appropriate back-up including operating procedures covering the assumed failure of the CBP system,
- validating a combination of plant operation strategies, formats presentation and human capabilities, as well as digital issues,
- maintaining the operator in the loop, i.e. ensuring adequate priority of human action versus computerised actions and preventing the loss of knowledge.

1.3 Exclusions from this standard

In order to design CBP efficiently and properly, some important inputs should have already been decided and are therefore outside the scope of this standard:

- functional analysis and assignment

  IEC 61839 specifies functional analysis and assignment procedures and gives rules for developing criteria for the assignment of functions either to operators or to systems,
- human factors design guidelines.

  ISO 11064 series of standards provides guidance on human-centered design activities throughout the life cycle of a computer-based interactive system.

In addition, IEC 60964 and IEC 60965, which provide requirements and recommendations for the main control room and supplementary control point arrangements, apply to the implementation of CBP in new nuclear power plants. Complementary advice for implementing CBP in case of main control room retrofitting is given in 6.2.3 of this standard.

This standard also excludes:

- computer security, which is necessary to protect the whole life cycle of CBP, but is not restricted to computerisation of procedures. Nevertheless, this topic is to be considered when computerising operating means. IEC 62645 deals with cyber-security,
- requirements on the implementation for CBP functions of software and hardware of computer systems for CBP has to be implemented in line with its safety class in compliance with IEC 61513,
- the organisation for maintenance of procedures.

1.4 Organisation of this standard

Clause 2 lists the reference documents.

Clause 3 gives definitions relevant to this standard.

Clause 4 lists the abbreviations used in this standard.

Clause 5 provides an overview of CBP. It presents recommendations for the development of a policy for computerisation of procedures, based on the type of procedure to be implemented. Three generic types (termed “families”) are proposed, for which general and specific guidance is provided. Guidance related to the safety requirements of CBP systems is also provided.

Clause 6 gives requirements for use in different environments, inside and outside of the MCR (Main Control Room) and possibly in conjunction with paper based procedures. It then considers assistance to and coordination of operator activities.

Clause 7 deals with the digital system which processes CBP. It first considers safety and non-safety requirements, then gives requirements for handling failures of this system.

Clause 8 focuses on the detailed requirements and recommendations related to the functional features of CBP, from the basic ones to the most sophisticated ones, i.e. information, navigation, guidance and plant control. Miscellaneous options that could ease CBP use are also given.

Clause 9 considers the CBP life cycle, from the set-up of the project to the CBP maintenance and the operator training via design and implementation.

2 Normative references

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

IEC 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60964:2009, *Nuclear power plants – Control rooms – Design*

IEC 60965:2009, *Nuclear power plants – Control rooms – Supplementary control points for reactor shutdown without access to the main control room*

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

IEC 61772, *Nuclear power plants – Control rooms – Application of visual display units (VDUs)*

IEC 61839, *Nuclear power plants – Design of control rooms – Functional analysis and assignment*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62241:2004, *Nuclear power plants – Main control room – Alarm functions and presentation*

ISO 11064 (all parts), *Ergonomic design of control centres*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – PROCÉDURES INFORMATISÉES

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.

2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.

3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.

4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.

5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.

6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.

7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.

8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62646 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/886/FDIS	45A/888/RVD

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

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

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

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

a) Contexte technique, questions importantes et structure de la présente norme

La présente norme CEI s'intéresse à l'informatisation des procédures de conduite utilisées par le personnel d'exploitation. Les procédures ont toujours largement contribué à la sûreté des centrales nucléaires de puissance et à leur disponibilité. Aujourd'hui la technologie informatique est de plus en plus utilisée pour fournir à l'opérateur de centrales des recommandations détaillées et devient la pratique courante. Cette norme établit aussi des recommandations pour prendre une décision sur le niveau d'informatisation qu'il convient de retenir.

L'objectif de la présente norme est d'être utilisée par les concepteurs de centrales nucléaires, le personnel de conduite, les évaluateurs de système et par les régulateurs.

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

La CEI 62646 est le document du SC 45A de la CEI de troisième niveau qui traite du problème particulier des procédures informatisées.

La CEI 62646 doit être lue avec la CEI 60964 et avec la CEI 61839. La CEI 60964 est le document du SC 45A de la CEI qui fournit des recommandations applicables pour les commandes opérateur, la vérification et la validation de la conception ainsi que l'utilisation des unités de visualisation, alors que la CEI 61839 établit des recommandations au niveau analyse fonctionnelle et affectation pour répartir les fonctions entre les opérateurs et les systèmes numériques.

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

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

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

La présente norme couvre les exigences techniques et les aspects ergonomiques liés aux Procédures Informatisées (PI). Cependant elle ne fournit pas de recommandations détaillées concernant la conception ergonomique des salles de commande car ce sujet est couvert par les normes de la série ISO 11064; elle ne couvre pas non plus la répartition des tâches entre l'humain et les systèmes qui est traitée dans la CEI 61839; pas plus qu'elle ne traite de cyber-sécurité, sujet couvert par la CEI 62645. L'organisation des procédures de maintenance est aussi exclue de la présente norme.

La présente norme établit des exigences et des recommandations pour les aspects suivants:

– mise en place d'une politique d'informatisation des procédures, en particulier quels types de procédures il convient d'informatiser et quel est le niveau d'informatisation. Les différentes familles de PI auxquelles on doit s'intéresser, ainsi que leurs caractéristiques associées qui sont à définir. Enfin, les aspects sûreté des PI qui sont à prendre en compte;

– utilisation des PI, à l'intérieur comme à l'extérieur de la SdC (Salle de Commande principale), en parallèle des procédures papier, ainsi que le support fournit pour les activités opérateur, y compris la coordination utilisateur;

– le système numérique support des PI, avec les exigences de conception de sûreté et celles non associées à la sûreté, et la prise en compte de ce qu'on doit faire en cas de défaillance de ce système;

– les exigences détaillées et les recommandations associées aux caractéristiques fonctionnelles des PI, en partant des plus simples jusqu'aux plus sophistiquées, c'est-à-dire information, navigation, orientation et conduite de la centrale;

– le cycle de vie des PI, de la mise en place du projet, à la maintenance des PI, en passant par la formation des opérateurs.

Afin d'assurer la pertinence de la présente norme pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

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

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

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

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

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

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales des CEI 61508-1, CEI 61508-2 et CEI 61508-4 pour le secteur nucléaire, pour ce qui concerne le domaine de la sûreté nucléaire. Dans ce domaine, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire. La CEI 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales, dont les exigences sont comparables à des normes telle que la CEI 61508.

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – PROCÉDURES INFORMATISÉES

1 Domaine d'application

1.1 Objet

La présente Norme internationale établit des exigences pour l'ensemble du cycle de vie des procédures de conduite que le concepteur souhaite informatiser. Elle fournit aussi des recommandations pour prendre les décisions concernant le choix des procédures à informatiser et le niveau d'informatisation de celles-ci. Une fois informatisées, ces procédures sont nommées «procédures informatisées» (PI).

L'amélioration de la sûreté, l'aide à l'exploitation et l'amélioration de la disponibilité des centrales nucléaires de puissance ont toujours été des objectifs majeurs dont l'atteinte, en exploitation, repose en grande partie sur le personnel de conduite et sur les procédures suivies. Aujourd'hui la technologie numérique contribue à l'atteinte de ces objectifs en assurant un support efficace au niveau de l'automatisation.

De plus, l'utilisation de la technologie numérique fournissant des images de procédure de conduite aux opérateurs[1], en ligne et en temps réel, se développe et devient la pratique courante. Ceci peut être fait pour les situations d'exploitation normale, comme pour fournir des images présentant des recommandations utilisables pour des situations anormales. Lorsqu'elles sont correctement mises en œuvre et maintenues, de telles procédures de conduite peuvent fournir une aide avancée permettant d'atteindre un niveau supérieur de sûreté et aussi d'efficacité des opérateurs, par rapport au niveau atteint avec les procédures papier. Leur préparation exige beaucoup d'attention et une interaction étroite entre les opérateurs et les concepteurs de la centrale. Enfin, une collaboration étroite avec les concepteurs d'I&C (Instrumentation et Contrôle-commande) sera aussi nécessaire.

Les PI ont de nombreux de points en commun avec les procédures papier. La présente norme s'intéresse donc aux aspects particuliers des PI.

1.2 Vue d'ensemble des PI

Les procédures fournissent à l'opérateur deux types d'élément de haut niveau:

- de l'information, c'est-à-dire des explications ou des données affichées pour permettre à l'opérateur de conduire le procédé, pour comprendre les stratégies de conduite et pour prendre des décisions adaptées,
- des recommandations, c'est-à-dire un ensemble ordonné d'étapes pour attirer l'attention de l'opérateur et l'aider dans la conduite du procédé et des matériels de la centrale.

Les informations et les recommandations sont combinées pour minimiser les sources d'erreur pour l'opérateur et pour optimiser la conduite de la centrale.

Ces éléments dont le niveau de détail peut varier suivant la politique associée aux procédures qui a été adoptée, et qui est là pour tirer profit de l'expérience des opérateurs et des orientations prédéfinies.

---

[1] Les opérateurs peuvent être des hommes ou des femmes, ainsi dans cette norme, lorsqu'on on fait référence à l'opérateur par « il », ceci est un raccourci pour « il/elle » et « son » est un raccourci pour « son/sa ».

L'informatisation des procédures peut fournir, suivant la politique spécifiée par les concepteurs:

- de l'information avancée sur les matériels de la centrale et le procédé,
- des recommandations avancées utilisateur,
- une possibilité optionnelle de commande automatique de la centrale.

Cependant, l'introduction de telles procédures s'accompagne de nouveaux problèmes:

- définition d'une politique claire portant sur le domaine des procédures, du niveau de recommandations et de la possibilité de conduite directe du procédé, par exemple en prenant en compte le retour d'expérience lié à l'exploitation de l'installation et les capacités humaines, ainsi que les questions technologiques et organisationnelles,
- conception d'un système de PI sûr et fiable, mais aussi fourniture du système secours adapté comprenant des procédures de conduite couvrant la défaillance hypothétique du système de PI,
- validation de la combinaison des différentes stratégies de conduite de la centrale, de la présentation des images et des capacités humaines, et de l'utilisation des technologies numériques,
- maintien de l'opérateur dans la boucle de conduite, par exemple en garantissant un niveau de priorité adapté aux actions humaines par rapport aux actions informatisées et en luttant contre la perte des connaissances au niveau du personnel de conduite.

1.3 Aspects hors du domaine d'application de la présente norme

Pour concevoir les PI de façon efficace, il convient d'avoir déjà défini certaines données d'entrée importantes qui de fait se situent donc hors domaine de la présente norme:

- analyse fonctionnelle et répartition

  la norme CEI 61839 spécifie les procédures d'affection et d'analyse fonctionnelles et donne des règles pour développer des critères pour affecter les fonctions aux opérateurs ou aux systèmes,
- recommandations de nature ergonomique pour la conception

  la série de normes ISO 11064 fournit des recommandations applicables aux aspects ergonomiques dans le cadre des activités de conception d'un système interactif numérique et ceci pour l'ensemble de son cycle de vie.

De plus, les CEI 60964 et CEI 60965 qui fournissent des exigences et des recommandations portant sur la mise en œuvre des salles de commandes principales (SdC) et des points de commande supplémentaires, sont applicables pour la mise en œuvre des PI dans les nouvelles centrales nucléaires. Des recommandations complémentaires pour la mise en œuvre des PI dans le cadre des rénovations de SdC sont fournies en 6.2.3.

Les points suivants sont aussi hors du domaine d'application de la présente norme:

- la sécurité informatique, nécessaire à la protection des PI durant l'ensemble de leur cycle de vie qui n'est pas particulier à l'informatisation des procédures. Néanmoins, ce sujet doit être pris en compte lorsqu'on informatise les moyens de conduite. Pour cela la CEI 62645 couvre les aspects cyber-sécurité,
- les exigences relatives à la mise en œuvre des fonctions PI relatives au logiciel et au matériel liés aux systèmes PI doivent être mises en œuvre en fonction de la classe de sûreté associée aux systèmes et conformément aux recommandations de la CEI 61513 suivant la catégorie de sûreté associée aux fonctions,
- l'organisation à mettre en place pour la maintenance des procédures.

1.4 Structure de la présente norme

L'Article 2 fournit la liste des documents de référence.

L'Article 3 fournit les définitions pertinentes applicables dans le cadre de la présente norme.

L'Article 4 contient la liste des abréviations utilisées dans la présente norme.

L'Article 5 fournit une vue d'ensemble des PI. Il présente les recommandations applicables au développement d'une politique d'informatisation des procédures, basée sur le type de procédures à mettre en œuvre. Trois types génériques (appelés «famille») sont proposés, pour lesquels des recommandations générales et particulières sont fournies. Des recommandations liées aux exigences de sûreté applicables aux systèmes PI sont aussi données.

L'Article 6 fournit des exigences permettant une utilisation dans différents environnements, à l'intérieur et à l'extérieur de la SdC et une possible coexistence avec les procédures papier. Il couvre les aspects relatifs au support des activités et de la coordination des opérateurs.

L'Article 7 traite du système numérique support des PI. Il considère d'abord les exigences de sûreté puis les autres, enfin il fournit des exigences à prendre en compte pour faire face à la défaillance de ce système.

L'Article 8 s'intéresse plus particulièrement aux exigences et aux recommandations détaillées relatives aux caractéristiques fonctionnelles des PI, en partant des plus simples jusqu'aux plus sophistiquées, c'est-à-dire l'information, la navigation, l'orientation et la conduite de la centrale. Différentes options qui peuvent rendre service au niveau des PI sont données.

L'Article 9 couvre le cycle de vie des PI, de la mise en place du projet, jusqu'à la maintenance des PI et la formation des opérateurs, en passant par la conception et la mise en œuvre.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60964:2009, *Centrales nucléaires de puissance – Salles de commande – Conception*

CEI 60965:2009, *Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

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

CEI 61772, *Centrales nucléaires de puissance – Salles de commande – Utilisation des unités de visualisation*

CEI 61839, *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions*

CEI 62138, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

CEI 62241:2004, *Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes*

ISO 11064 (toutes les parties), *Conception ergonomique des centres de commande*