IEC 62646

Edition 2.0 2016-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Control rooms – Computer-based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-3650-5

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, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 2012. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) clarification of the way in which the standard is to be used in conjunction with related standards (in 1.4);
b) replacement, when necessary, of HMI system by DPDS (abbreviation added in Clause 4);
c) new titles for 5.2.2 and 5.2.3 to more closely represent their content;
d) text improvement in 5.2.2, to present the CBP system as a part of the I&C architecture rather than a stand alone system;
e) text improvement in 5.2.3 and 7.2 to clarify links between safety and CBP;

f) new definition of CPB families in 5.3;
g) addition of generic recommendations for computerization in 5.4.2;
h) addition of generic recommendations for CBP guidance in 5.4.3;
i) improvements regarding use of CBP in 5.4.4;
j) addition of 5.6, named “Design extension conditions”;
k) addition of reference standards in 6.2.1;
l) addition of a criterion related to detail compatibility between CBP and operating formats in 6.2.2;
m) addition of references related to HMI in 6.2.3;
n) addition of 7.3 to deal with HMI aspects;
o) text improvement regarding integration of the CBP system into the DPDS in 7.3;
p) text improvement regarding implementation of the CBP into a system independent of the DPDS in 7.4;
q) text improvement regarding the CBP system failure in 7.6;
r) note added to detail the different types of feedbacks in 8.5.4;
s) text improvement to detail interactions between operators and procedure based automation in 8.6.2;
t) text improvement regarding design of CBP to control the plant in 8.6.3;
u) clarification of the content of the V&V programme for CBP in 9.5;
v) clarification regarding CBP programming in 9.4;
w) inversion of subclauses 9.4 and 9.5;
x) clarification of the content and requirements of the V&V in 9.6;
y) change of title of 9.7.

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

FDIS	Report on voting
45A/1098/FDIS	45A/1110/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.

IEC 62646 is to be read in conjunction with IEC 60964:2009 and IEC 61839:2000.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website 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 nuclear power plant (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 of the extent to which 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 inspectors.

In June 2013 during the IEC SC 45A meeting held in Moscow, the decision was made to revise IEC 62646 with the lessons learned from the Tokyo Electric Power Company (TEPCO) Fukushima Daiichi accident and the late comments from the national committee of Canada. The resulting improvements are listed in the Foreword of the Standard.

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.

As indicated in the Foreword, IEC 62646 is to be read with IEC 60964 and IEC 61839. IEC 60964 – supported by IEC 61227, IEC 61771 and IEC 61772 – 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 humans 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 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 documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPP. IEC 63046 provides general requirements for electrical power systems of NPP; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPP), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPP, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPP, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPP and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level

2, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPP 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.

NOTE 2 IEC SC 45A's domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirement for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 will be published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – CONTROL ROOMS – COMPUTER-BASED PROCEDURES

1 Scope

1.1 Object of this standard

This 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 should be computerised and to what extent. Once computerised, procedures are designated as "computer-based procedures" (CBP).

1.2 Context leading to development and use of CPB

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 contributes not only by providing efficient ways of automating key functions but also enhances instrumentation, control and the plant's HMI.

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.

1.3 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 that prompt and help the operator to monitor and control the plant processes, systems and equipment.

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

Information and guidance can be of a varying level of detail depending on the procedure policy, which aims to benefit from operator experience and existing 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".

– additional functions to initiate and control automation sequences.

This standard provides guidance on and an overview of policy, philosophy and conceptual requirements for CBP implementation, including design objectives, assumptions, approaches, inputs, scope, CBP family types, key CBP features, and output documentation.

1.4 Use of this standard with related standards

This standard intends to deal with aspects that are:

- specific to computer-based procedures, i.e. that are not common with paper-based procedures. For example, establishing functional scenarios to validate procedures is not specific to CBP,
- not already dealt with in existing standards, i.e. HFE, life cycle of safety classified systems, allocation of tasks to human or machines.

In order to design CBP efficiently and properly, some important considerations at the conceptual design stage of CBPs are addressed in the following related standards:

a) 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,

b) human factors design guidelines

   IEC 61772:2009, especially Clauses 4 and 5, provides guidance on physical implementation of VDUs (see 4.1), display formats (see 4.4), and implementation into the MCR (see Clause 5). The 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 room arrangements, and IEC 61772, providing requirements and recommendations for implementing VDUs in control rooms, 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.

This standard assumes the simultaneous consideration of the requirements for:

1) computer security, which is necessary to protect the whole life cycle of CBP, but is not restricted to computerisation of procedures. Nevertheless, this topic should be considered when computerising operating means (IEC 62645 deals with cyber-security),
2) requirements on the implementation for CBP functions of software and hardware of computer systems for CBP which should be implemented in line with their safety class in compliance with IEC 60880, IEC 61226, IEC 62138 and IEC 61513,
3) the design of plant scenarios (including anticipated operating occurrences such as plant transients, plant upset conditions and/or initiating events) for validating CBPs,
4) the organisation for functional maintenance of procedures.

1.5 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 described, 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 contexts, including main control room (MCR) upgrading, and different environments, inside and outside of the MCR 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 are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE The output documentation requested by these normative standards that is related to CBP is not addressed in this standard.

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 60965:2016, *Nuclear power plants – Control rooms – Supplementary control room 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 61772:2009, *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*

ISO 11064-1, *Ergonomic design of control centres – Part 1:Principles for the design of control centres*

ISO 11064-3, *Ergonomic design of control centres – Part 3: Control room layout*

ISO 11064-4, *Ergonomic design of control centres – Part 4: Layout and dimensions of workstations*

ISO 11064-5, *Ergonomic design of control centres – Part 5: Displays and controls*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – PROCÉDURES INFORMATISÉES

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC 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 IEC 62646 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et électriques des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition publiée en 2012. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) clarification concernant la façon d'utiliser la présente norme avec les autres normes connexes (1.4);
b) remplacement lorsque nécessaire, de l'expression «système d'IHM» par «SANC» (système d'affichage numérique de conduite) (abréviation ajoutée à l'Article 4);
c) nouveau titres pour 5.2.2 et 5.2.3 représentant plus fidèlement leurs contenus;

d) amélioration du texte de 5.2.2 présentant les systèmes PI comme faisant partie de l'architecture d'I&C plutôt que comme un système indépendant;

e) amélioration du texte de 5.2.3 et 7.2 pour clarifier les liens entre sûreté et les PI;

f) nouvelles définitions pour les familles de PI en 5.3;

g) rajout de recommandations génériques portant sur l'informatisation en 5.4.2;

h) rajout de recommandations génériques concernant les recommandations portant sur les PI en 5.4.3;

i) améliorations portant sur l'utilisation des PI en 5.4.4;

j) rajout de 5.6 pour couvrir les conditions hors dimensionnement;

k) rajout de références aux normes en 6.2.1;

l) rajout d'un critère relatif à la compatibilité des détails entre les PI et les images de conduite en 6.2.2;

m) rajout de références portant sur l'IHM en 6.2.3,

n) rajout de 7.3 pour couvrir les aspects IHM;

o) amélioration du texte pour ce qui concerne l'intégration du système PI dans le SANC en 7.3;

p) amélioration du texte pour ce qui concerne la mise en œuvre des PI dans un système indépendant du SANC en 7.4;

q) amélioration du texte pour ce qui concerne la défaillance du système PI en 7.6;

r) rajout d'une note fournissant des détails concernant les différents types d'acquittement en 8.5.4;

s) amélioration du texte détaillant les interactions des opérateurs avec les procédures automatisées en 8.6.2;

t) amélioration du texte concernant la conception des PI pour conduire l'installation en 8.6.3;

u) clarification du contenu du programme de V&V des PI en 9.5;

v) clarification concernant la programmation des PI en 9.4;

w) inversion de 9.4 et 9.5;

x) clarification du contenu et des exigences de V&V en 9.6;

y) changement du titre de 9.7.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/1098/FDIS	45A/1110/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/IEC, Partie 2.

L'IEC 62646 doit être lue conjointement avec l'IEC 60964:2009 et l'IEC 61839:2000.

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 l'IEC 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 IEC 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.

En juin 2013, durant la réunion de l'IEC SC 45A qui s'est tenue à Moscou, la décision a été prise de réviser l'IEC 62646 pour prendre en compte les leçons tirées de l'accident survenu à la centrale de TEPCO (Tokyo Electric Power Company) à Fukushima Daïchi ainsi que les commentaires tardifs formulés par le comité national Canadien sur la première version. La liste des améliorations apportées à la présente norme est fournie dans son avant-propos.

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

L'IEC 62646 est le document du SC 45A de l'IEC de troisième niveau qui traite du problème particulier des procédures informatisées.

Comme indiqué dans l'avant-propos, l'IEC 62646 est lue avec l'IEC 60964 et avec l'IEC 61839. L'IEC 60964, complétée par l'IEC 61227, l'IEC 61771 et L'IEC 61772, est le document pertinent du SC 45A de l'IEC 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 l'IEC 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 structure de la série de normes du SC 45A de l'IEC, 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 l'IEC 61839; pas plus qu'elle ne traite de cyber-sécurité, sujet couvert par l'IEC 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 l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme IEC 61513 traite des exigences générales 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. La norme IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. les normes IEC 61513 et IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet, cohérent et consistant établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes programmés numériques, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par les normes IEC 61513 ou IEC 63046, 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 l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires , avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en

œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, l'IEC 61508-2 et l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, la norme IEC 62645 est le document chapeau des normes du SC 45A de l'IEC portant sur la cybersécurité. Elle est élaborée sur principes pertinents de haut niveau des normes ISO/IEC 27001 et 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la norme IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 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.

NOTE 2 Le domaine de l'IEC SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein de l'IEC SC 45A pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts de l'IEC SC 45A ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée la présente NOTE 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – PROCÉDURES INFORMATISÉES

1 Domaine d'application

1.1 Objet de la présente norme

La présente norme 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 qu'il convient d'informatiser et le niveau d'informatisation de celles-ci. Une fois informatisées, ces procédures sont nommées «procédures informatisées» (PI).

1.2 Contexte à l'origine de l'utilisation et du développement des 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. La technologie numérique non seulement fournit des moyens efficaces pour l'automatisation des fonctions clef, mais aussi elle permet d'améliorer l'instrumentation, le contrôle-commande et l'IHM de conduite.

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 demande 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.

1.3 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 qui attire l'attention de l'opérateur et l'aide à surveiller et à contrôler le procédé opérationnel, les systèmes et les 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.

---

[1] Les opérateurs peuvent être masculins ou féminins, 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 ».

Les informations et les recommandations peuvent être d'un niveau de détail variable suivant la politique associée aux procédures qui a été adoptée, et qui est là pour tirer profit de l'expérience des opérateurs et des directives existantes.

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,
– un meilleur niveau de recommandations pour l'opérateur,
– des fonctions supplémentaires pour lancer et contrôler des séquences d'automatisation.

La présente norme fournit des recommandations et une vue d'ensemble sur la politique, la philosophie et les exigences conceptuelles liées à la mise en œuvre des PI, y compris pour ce qui concerne les objectifs de conception, les hypothèses, les approches, les données d'entrée, le domaine, les types de famille de PI, les caractéristiques clef des PI et la documentation produite.

1.4 Utilisation de la présente norme avec les normes associées

La présente norme a pour objectif de traiter des aspects qui:

- sont propres aux procédures informatisées, c'est-à-dire qui ne sont pas partagées avec les procédures papier. Par exemple, l'établissement de scénarii fonctionnels pour valider les procédures n'est pas propre aux PI;
- ne sont pas déjà couverts par des normes existantes, c'est-à-dire ergonomie, cycle de vie de sûreté des systèmes classés, allocations des tâches humain/machine.

Pour concevoir les PI de façon efficace, certains aspects à prendre en compte au niveau de la phase de conception conceptuelle sont couverts par les normes associées suivantes:

a) analyse fonctionnelle et répartition

   la norme IEC 61839 spécifie les procédures d'affectation et d'analyse fonctionnelles et donne des règles pour développer des critères pour affecter les fonctions ou aux opérateurs ou aux systèmes,

b) recommandations de nature ergonomique pour la conception

   L'IEC 61772:2009, en particulier les Articles 4 et 5, fournit des recommandations sur la mise en œuvre physique des unités de visualisation (voir 4.1) et des images (voir 4.4), de même que sur la mise en œuvre au niveau des SdC (voir Article 5). 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, l'IEC 60964 et l'IEC 60965 qui fournissent des exigences et des recommandations portant sur la mise en œuvre des salles de commandes principales (SdC) et des salles de commande supplémentaires et l'IEC 61772 qui établit des exigences et des recommandations pour la mise en œuvre des unités de visualisation en salle de commande, 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.

La présente norme fait l'hypothèse que soient prises en compte de façon simultanée les exigences relatives aux points suivants:

1) 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, il convient que ce sujet soit pris en compte lorsqu'on informatise les moyens de conduite. Pour cela l'IEC 62645 couvre les aspects cyber-sécurité,
2) les exigences relatives à la mise en œuvre des fonctions PI relatives au logiciel et au matériel liés aux systèmes PI qu'il convient de mettre en œuvre en fonction de la classe

de sûreté associée aux systèmes et conformément aux recommandations des IEC 60880, IEC 61226, IEC 62138 et IEC 61513 suivant la catégorie de sûreté associée aux fonctions,

3) la conception des scénarii opérationnels (y compris les incidents de fonctionnement prévus tels que les transitoires d'exploitation, les conditions opérationnelles de départ et/ou les événements initiateurs) pour valider les PI,
4) l'organisation à mettre en place pour la maintenance fonctionnelle des procédures.

1.5 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 décrits, 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 contextes, y compris celui de mise à niveau des salles de commande (SdC) et 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).

NOTE La documentation produite requise par les normes précédentes et qui est relative aux PI n'est pas couverte par la présente norme.

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

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

IEC 60965:2016*, Centrales nucléaires de puissance – Salles de commande – Salles de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale*

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

IEC 61772:2009, *Centrales nucléaires de puissance – Salles de commande – Utilisation des unités de visualisation*

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

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

IEC 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*

ISO 11064-1*, Conception ergonomique des centres de commande – Partie 1: Principes pour la conception des centres de commande*

ISO 11064-3, *Conception ergonomique des centres de commande – Partie 3: Agencement de la salle de commande*

ISO 11064-4, *Conception ergonomique des centres de commande – Partie 4: Agencement et dimensionnement du poste de travail*

ISO 11064-5, *Conception ergonomique des centres de commande – Partie 5: Dispositifs d'affichage et commandes*