IEC 62646

Edition 1.0 2012-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Control rooms – Computer based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées

IEC 62646:2012

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62646

Edition 1.0 2012-09

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

PRICE CODE
CODE PRIX

ICS 27.120.20

ISBN 978-2-83220-388-0

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
back-up system
alternative equipment for plant monitoring and control designed to be used in case of failure of the normally used HMI system