

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Nuclear power plants – Control rooms – Computer-based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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 l'IEC

La Commission Electrotechnique Internationale (IEC) 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 IEC

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

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

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

La recherche avancée permet de trouver des publications IEC 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.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. 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 de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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.

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

ICS 27.120.20

ISBN 978-2-8322-3650-5

**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

FOREWORD.....	5
INTRODUCTION.....	8
1 Scope.....	11
1.1 Object of this standard	11
1.2 Context leading to development and use of CPB.....	11
1.3 CBP overview	11
1.4 Use of this standard with related standards.....	12
1.5 Organisation of this standard.....	12
2 Normative references.....	13
3 Terms and definitions	14
4 Abbreviated terms	16
5 CBP policy and conceptual requirements.....	16
5.1 General.....	16
5.2 Computerisation policy	17
5.2.1 General	17
5.2.2 Rationale underlying the implementation of CBP.....	17
5.2.3 The scope of CBP	18
5.3 Families of CBP	19
5.4 Overview of computerisation features	20
5.4.1 General	20
5.4.2 Global requirements for computerisation.....	20
5.4.3 Provision of guidance to operator	21
5.4.4 Provision of procedure based automation	22
5.5 Output documentation	22
5.6 Design extension conditions	23
6 Contexts of use of CBP.....	23
6.1 General.....	23
6.2 Application environments of CBP use	23
6.2.1 General	23
6.2.2 Use of CBP in computerised control rooms	23
6.2.3 Use of CBP in a conventional or hybrid main control room	24
6.2.4 Use of CBP in conjunction with paper-based procedures.....	24
6.2.5 Use of CBP outside the main control room.....	25
6.3 Forms of CBP assistance to operator activities	25
6.3.1 General	25
6.3.2 Assistance to primary activities of the operator	25
6.3.3 Assistance to secondary activities of the operator.....	25
6.4 Assistance with operator coordination.....	26
6.5 Output documentation	26
7 CBP system and functional requirements	27
7.1 General.....	27
7.2 Safety requirements	27
7.3 HMI considerations	28
7.4 Integration of the CBP system into the DPDS.....	28
7.5 CBP system implemented externally to the DPDS	28

7.5.1	General	28
7.5.2	Sizing and dependability requirements.....	29
7.5.3	Connections between the CBP system and the DPDS	29
7.5.4	Coherent maintenance of both systems	29
7.6	CBP system failure.....	29
7.7	Output documentation	30
8	Detailed design requirements.....	31
8.1	General.....	31
8.2	Basic CBP features	31
8.2.1	General	31
8.2.2	Basic features necessary for CBP	31
8.2.3	Presentation rules	31
8.2.4	CBP display format layout	32
8.2.5	Requirements for presentation of individual display elements.....	32
8.3	Information presented by the CBP	33
8.3.1	General	33
8.3.2	Information for Family 1 CBP.....	33
8.3.3	Information for Family 2 CBP.....	33
8.3.4	Information for Family 3 CBP.....	34
8.4	Navigation.....	34
8.4.1	General	34
8.4.2	Navigation for Family 1 CBP.....	34
8.4.3	Navigation for Family 2 and Family 3 CBP	34
8.5	CBP guidance	35
8.5.1	General	35
8.5.2	CBP selection, accessibility and execution	35
8.5.3	Diagnosis assistance	35
8.5.4	Decision assistance	35
8.5.5	Computerisation of CBP guidance	36
8.6	Procedure-based automation.....	36
8.6.1	General	36
8.6.2	Interactions between operators and procedure based automation.....	37
8.6.3	Design of CBP to control the plant.....	37
8.7	Other CBP facilities	38
8.8	Output documentation	38
9	CBP life cycle.....	38
9.1	General.....	38
9.2	Project organisation	39
9.3	Project team	39
9.4	CBP detailed design and implementation quality assurance (QA)	39
9.5	Verification and validation programme	40
9.6	Verification and validation of CBP.....	40
9.6.1	General	40
9.6.2	Technical verification of CBP.....	41
9.6.3	Functional and ergonomic validation.....	41
9.6.4	Output documentation	42
9.7	Implementation of CBP in NPP	42
9.8	Output documentation	43
9.9	Training of the operating staff.....	44

9.10	CBP and CBP system maintenance	44
9.11	Feedback of experience	44
	Bibliography	45
	Table 1 – CBP families	19

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 operators¹, 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".