

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Nuclear power plants – Control rooms – Computer-based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées

IECNORM.COM : Click to view the full PDF of IEC 62646:2016



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

IECNORM.COM : Click to view the full PDF of IEC 62646:2016

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.

IECNORM.COM : Click to view the full PDF of IEC 62646:2016

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.

IECNORM.COM : Click to view the full PDF of IEC 62646:2016

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".

- 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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>.

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

Note 1 to entry: The back-up system may become unavailable if a beyond design basis accident occurs.

3.2

CBP

computer-based procedures

interactive computer application used to present procedural guidance to plant operators and which may additionally contain dynamic process information including access to operator controls

Note 1 to entry: Unlike paper-based procedures which are static documents, CBP offer dynamic reading options. These options allow the operator to "navigate" from one step to others in different enhanced ways, to place bookmarks, and to use parallel displays.

3.3

CBP system

digital system implementing the CBP

Note 1 to entry: The CBP may be implemented in the HMI system, together with other plant control functions, or may be implemented in a standalone CBP computer.

3.4

DPDS

digital plant display system

digital system computing formats (display formats) dedicated to plant monitoring and control, for example flow diagrams, in order to have them displayed on VDUs

3.5

format (display format)

pictorial display of information on a visual display unit (VDU) such as message text, digital presentation, symbols, mimics, bar-charts, trend graphs, pointers, multi-angular presentation

[SOURCE: IEC 60964:2009, 3.7]

3.6

high-level mental processing

human act to process and/or interpret information to obtain reduced abstract information

[SOURCE: IEC 60964:2009, 3.12]

3.7

HMI

human machine interface

interface between operating staff and I&C system and computer systems linked with plant. The interface includes displays, controls, and the operator support system interface

[SOURCE: IEC 60964:2009, 3.13]

3.8

navigation

function, which supports the operators in locating the position of desired information in a VDU-based information system, and also in guiding the selection of displays

[SOURCE: IEC 62241:2004, 3.29]

3.9

OP

operating procedures

set of documents specifying operational tasks it is necessary to perform to achieve functional goals

[SOURCE: IEC 60964:2009, 3.19]

3.10

operating strategy

formalized approach defining high level ways, for example depressurization or cooling of the primary loop, to keep the unit in or to bring it back in a safe state and which aims at guiding the elaboration of operating procedures

3.11

paper-based procedures

OP (see 3.9) that are printed on paper sheets

3.12

PIE

postulated initiating event

event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[SOURCE: IAEA Safety Glossary, 2007]

3.13

sequence

procedure sequence

set of elementary steps in a procedure that is to be completely executed in order to reach a functional objective

Note 1 to entry: A partial execution of a sequence could either lead to malfunction or failure of circuits or equipment or jeopardise the execution of a function.

Note 2 to entry: Generally, a procedure encompasses several sequences to achieve its global functional objective.

Note 3 to entry: A sequence may consist of a single step.

3.14

step

single check of parameters, single action on an item of plant, or simple decision or oral message between operators to be made that is put forward by a procedure

3.15

SCR

supplementary control room

location from which limited plant control and/or monitoring can be carried out to accomplish the safety functions identified by the safety analysis as required in the event of a loss of ability to perform those functions from the main control room

Note 1 to entry: For existing plants, the supplementary control room may be a special control room, but in many cases comprises a sets of control panels and displays in switchgear rooms or similar areas. In the latter case, the term 'supplementary control point' is used.

[SOURCE: IEC 60965:2016, 3.6]

3.16

VDU

visual display unit

type of display incorporating a screen for presenting computer-driven images

Note 1 to entry: This note applies to the French language only.

[SOURCE: IEC 60964:2009, 3.31]

4 Abbreviated terms

CBP	computer-based procedures
DPDS	digital plant display system
HFE	human factors engineering
HMI	human machine interface
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
MCR	main control room
NPP	nuclear power plant
OP	operating procedures
PIE	postulated initiating event
SCR	supplementary control room
VDU	visual display unit
V&V	verification and validation

5 CBP policy and conceptual requirements

5.1 General

Clause 5 provides guidance on 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,
- CBP family types,

- key CBP features,
- the output documentation.

5.2 Computerisation policy

5.2.1 General

Elaboration of a policy shall be part of specifying the control room concept, the overall I&C architecture, the definition of human factors policy and the utility operating principles (see IEC 60964:2009, Clause 5).

It should be supported by feedback of experience analysis, conceptual studies, possibly some prototyping, performed either as an input to the design or as an early step of the design.

The designer shall decide the types of procedures subject to computerisation and the extent of this computerisation.

The reasons for computerisation of procedures shall be stated in the governing project plan, as they will strongly influence which procedures will be computerised and to what extent. Implementing CBP will not necessarily resolve operating strategy or staffing problems, but a design study for a CBP may help to clarify the nature of those problems and help to identify ways for problem resolution at an early stage of the design process.

NOTE Possible consequences on operating staff organisation, main control room layout, operating strategies, procedure scope, automation design and development, etc., are out of the scope of this standard.

The types of procedures that may be computerised include:

- procedures guiding normal plant operation in normal conditions, for example plant start-up, or procedures guiding elementary tasks, pipework warm-through, or load reduction and return to power,
- accident procedures,
- alarm response procedures,
- fire handling procedures,
- loss of electrical power procedures, and any types of procedures dedicated to unusual conditions,
- periodic testing procedures designed according to IEC 60671, for example dedicated to flux calibration or to reactor trip, or any other periodic testing procedures.

Other documents may also be computerized:

- technical specifications,
- technical component sheets, offering easy access to specific device data on the screen-based DPDS.

5.2.2 Rationale underlying the implementation of CBP

In addition to the task analysis, functional analysis and assignment and human factors design guidance which are issues addressed by other IEC standards listed in Clause 2, the following technical aspects shall be considered in the project planning and from the early stages of design. These are:

- a) national regulatory issues,
- b) operating strategies:

this is a functional issue to be considered independently from computerisation, for example if a decision has to be made between state-based and event-based strategies in the event of an accident,

c) operating staff organisation:

when constructing a new plant or modernising an existing plant, CBP design may be made an integral part of the overall control room design or redesign, which makes it necessary to apply accepted human factors engineering methods,

d) operating staff experience feedback:

- 1) lessons learned from existing CBP or paper-based solution should be identified;
- 2) in addition, the designer may consider that only the operating strategy, or on the contrary, only the detailed part of the procedures, should be computerised,

e) operator training,

f) data issued from the plant instrumentation,

NOTE 1 The CBP guidance level depends on available instrumentation.

g) drawbacks and advantages of processing CBP and other functions in the same system should be carefully weighed with regard to HFE, digital system capacities and the MCR layout. In particular, the unavailability of both CBP and other operating functions occurring simultaneously is to be considered. According to IEC 61513, the whole architecture including the CBP system, as well as the CBP system itself, are to be considered.

NOTE 2 The CBP system can possibly interface with a lot of systems, so that possible failure modes and operator response considerations can be quite important.

A preliminary CBP policy and the types of procedures that could be computerised should be defined from these considerations.

5.2.3 The scope of CBP

IEC 61839 shall first be used to identify functions which are to be assigned to human operators.

To make a final decision on the types of procedures to be computerised and the degree or form of computerisation to be implemented (i.e. refer to CBP families in 5.3), IEC 61772:2009, Clauses 4 and 5, as well as the following issues should be considered in the conceptual design:

- identification of the types of procedures that could be processed simultaneously (i.e., by multiple operators) in normal operation, in case of fire, in case of a loss of electrical power supply, in case of a periodic test, in case of a PIE,
- the safety significance of guidance delivered by CBPs to the operator and operator response time limits assumed or required,
- assessment of the amount of display formats and VDUs necessary for these procedures,
- assessment of the maximum number of procedures that could be processed in parallel by a single operator or by the entire operating staff to operate in the case of an occurrence of the worst design basis combination of events,
- assessment of the maximum number of windows that could be displayed in parallel in the worst cases on a single workstation or on all room workstations,
- allocation of operating staff's tasks to CBP and paper-based procedures in a consistent way (e.g., for avoidance of operator errors).

The above assessment should be made considering the control room concept. Items to be considered are:

- a) the set of workstations and workplaces where CBP are intended to be used, in the main control room and at all other control points,
- b) the fact that a procedure could be temporarily abandoned without being terminated, for example in case of an alarm outbreak,
- c) the maximum amount of information to be displayed in a format,

- d) the performance of the CBP system, in particular regarding displays, memory capacities, navigation,
- e) adequate additional margins in order to facilitate future modifications.

In addition, the achievable system class (i.e. see IEC 61513) for the CBP system should be considered early in the design process when functional allocation decisions are being made. The achievable system class of the CBP system will often be determined by the feasibility of qualification of the various elements of the overall architecture within which the CBP system is being implemented. These elements typically include: the CBP system itself, the DPDS and control systems through which the CBP interfaces with the plant and underlying networks that support communications between these elements, and the CBP design itself.

These considerations may challenge aspects of the CBP implementation policy, the proposed CBP system design, its capability and operation or the associated cost-benefit case, as well as the shift organisation or the operating strategies.

The content and scope of human factors and organisation studies should be defined regarding both:

- 1) identification of the human resources necessary for the project, i.e. specialists to be integrated into the project team, specialists for verifying and validating, organisation of CBP maintenance,
- 2) the use of the final product, including maintenance facilities.

IEC 60964, IEC 61772, IEC 61839, IEC 62241, ISO 11064, especially ISO 11064-1, ISO 11064-3, ISO 11064-4 and ISO 11064-5 may be used to make a decision. IEC 60965 may be used if some CBP are to be implemented in a supplementary control room.

5.3 Families of CBP

Though procedures may be computerised in very different ways according to the design policy, the implementation should be treated as one of three generic families of CBP, as shown in Table 1. The three families are based on a consideration of:

- the intended level of operator guidance,
- the required process inputs and outputs.

Table 1 – CBP families

<i>Determining CBP family</i>		Level of operator assistance		
		No step tracking/manual progress	Automatic step tracking	Guidance capability
Type of CBP signal interfaces	No input of process information	1	<i>Not possible</i>	<i>Not possible</i>
	Manual input of process information	1	<i>Not possible</i>	2
	Automatic input of process information	2	2	2 or 3
	Action on process	3	3	3

The rows represent different levels of connectivity of the CBP system, from no process information to action on process. The columns represent different levels of computerisation and associated intelligence. In the most advanced level of operator assistance, the system is able to provide decision aids to the operator; this feature is called guidance capability (see 8.5). The intersections of rows and columns represent the possible options for CBP.

These three CBP families are characterised in the following way:

- Family 1: CBP which are essentially stand-alone replacements for paper-based procedures, presenting linked pages of static information and operating steps. The operator may have the possibility to input some data manually in order to ease the understanding of the procedure.
CBP of this family do not receive any process information automatically and possess no plant control capabilities.
- Family 2: CBP that may provide guidance to the operator based on information acquired by the CBP system. Every item of information may be integrated into the display formats presented. If advanced guidance is provided, for example in the form of decision assistance (see 8.5.4), then the CPB should belong to Family 3.
- Family 3: CBP presenting information and operating steps with full integration of on-line plant information, states and values, so that an actuator can be controlled by the operator from the CBP display, automatic control functions can be accessed from the CBP display, and automatic execution of sequences can be initiated by the operator from the CBP display.

The CPB family allocation and the associated argumentation shall be documented.

All families may include some facilities presented in 8.7.

NOTE 1 Manual input is meant to represent a limited amount of information, otherwise the task of inputting information would be too demanding for the operator.

A different CBP family may be selected for each type of procedure listed in 5.2.1 so far as a simple and clear engineering approach can be maintained.

The choice of CBP family type, the CBP design and the overall architecture within which the CBP is being implemented will affect how each CBP function is allocated (or partitioned) between the human operator, the other hardwired or computerized MCR HMIs, the CBP system, and the other various elements of the overall architecture. The functional allocation determines the reliance for safety (i.e. the dependency for safety, including necessary requirements for fail-safe or fail-detected behaviour) that will be placed on the CBP system and the various elements of the overall architecture that implement or contribute to each of the various CBP functions. Therefore the resulting required system class will be a direct result of the CBP design, including the CBP family type, and the functional allocation within the overall CBP architecture.

NOTE 2 Depending on the plant's I&C architecture, especially during a retrofit, it might not be possible to implement Family 2 and Family 3 CBP systems.

5.4 Overview of computerisation features

5.4.1 General

Computerisation is based on generic rules and requirements and on items related to operator guidance and plant control.

5.4.2 Global requirements for computerisation

For all families of procedures:

- CBP should provide features to display the global objective of a procedure and an overview of its sequences either permanently, or on operator request. On operator request, the CBP should display additional information for steps or sequences, such as preliminary actions, process and device considerations,
- the designer shall verify that the set of procedures and the related requirements on processing capacity are in line with the CBP system capabilities.

Regarding Family 1 CBP, the procedure computerisation should:

- a) be intuitive and as simple as possible,
- b) give a clear view of the functional objective,
- c) ensure that operators easily understand the operating strategy,
- d) ensure the context of CBP sequence is not lost to the operator,
- e) leave full responsibility to the operators,
- f) ease progression inside procedures and limit calls between procedures.

For Families 2 and 3 CBPs, the procedure computerisation should:

- 1) respect recommendations established for Family 1 CBP,
- 2) include the possibility for the operator to leave steps and sequences out, if they are not relevant to achieve the procedure high-level goal,
- 3) provide adequate checks (preferably automatic) and safety interlocks on plant or equipment states to ensure that requested sequences are permitted and safe at that time and inform the operator otherwise,
- 4) avoid implementation of safety overrides from within the CBP system (i.e. they should not be permitted),
- 5) support appropriate operator confirmations prior to execution of automatic sequences,
- 6) provide adequate and consistent information and display formats between members of the team who may be accessing independent CBP displays, and ensure any inconsistencies that may arise on independent CBP displays due to internal CBP system faults are detected and clearly indicated to the operator,
- 7) apply in the same way to all procedures of a given type, for example to all accident procedures or to all fire handling procedures,
- 8) be consistent for different types of procedures that could be processed in parallel.

5.4.3 Provision of guidance to operator

Guidance provided by CBP should remind operators of the functional objectives and of the detailed information on the proper sequence of steps of operational procedures as well as information and guidance on how to achieve each step and the overall objectives.

In addition to providing the operator with elementary process information, enhanced information on the process may be given through CBP access, diagnosis or decisions guidance.

Diagnosis or decision guidance may be:

- automated: a diagnosis/decision is suggested to the operator, who may then ask for detailed information about it,
- supported: CBP display flow charts which assist the operator to establish a diagnosis/decision. Information necessary to the operator to make elementary choices is made easy to find or is incorporated in flow charts so that the operator can validate successively each step.

To design CBP guidance, due consideration should be given to:

- a) plant states in which the CBP will be required to be used,
- b) frequency of events or situations. For example, enhanced guidance should be provided for rare events compared with that for daily operation,
- c) the operating policy. For example, the desire for high plant availability may lead to an increase in computerisation and automation,

- d) whether/when operator actions are required within a certain time limit (i.e. considering appropriate operator alarms or notifications that may be required, or conservative safe action(s) required in the event of failure of the operator to act),
- e) operating staff feedback and requirements.

The designer shall take account of the inherent CBP system capabilities, i.e. performance, look-and-feel, to define guidance.

Possibilities for the operator to ask for elementary information may be extended to calculations leading to high level summarised information.

CBP provide the operator with synthesised information and possibly some assistance as described in 8.7

5.4.4 Provision of procedure based automation

CBP may assist the operator in the control of the plant by:

- automatically prompting messages to the operator when predefined conditions are met,
- automatically executing sequences that have been initiated by an operator.

As for paper-based procedures, CBP should be defined considering:

- the allocation of functions between the operator and the CBP system, the plant automation system or the DPDS,
- that the procedure set for the back-up system is independent from the DPDS and from the CBP system,
- the ease of comprehension by the operator, especially in abnormal conditions.

Additional considerations to be taken into account are:

- a) except if designed as a back-up means, duplication of functions between the operator and the system should be avoided; and designs should be sought where the CBP system and the operator perform complementary functions,
- b) CBP display formats may include command possibilities or may forward operators actions to control display formats of the DPDS. Another option may be to authorise CBP commands by enabling them from the DPDS.

The operator's situation awareness shall be enhanced by:

- 1) displaying adequate information to keep the operator fully informed of the changing plant status:
important decisions should not be automated, the end of automated sequences should be signalled, any problems encountered during an automated sequence should be signalled, as well as process values reaching a predefined threshold,
- 2) providing the operator with the option to take control from the CBP at any moment,

NOTE Some situations could require the action of the CBP to be terminated, whereas others could lead the operator to take control for a limited number of steps,

- 3) taking operating team coordination into account:
sequences launched by two operators may have different execution times and should not lead to contradictory or competing actions.

5.5 Output documentation

The decision rationale and assumptions to implement CBP (as discussed in 5.1 to 5.4 above) shall be documented early in the project and include:

- the policy, conceptual requirements and philosophy for CBP implementation,

- the type of CBP, their objectives and scope,
- the CBP implementation approach and assumptions, including considerations of the DPDS,
- the CBP guidance options, including a description of the design inputs and other required information,
- the option(s) for procedure-based automation,
- the utility policy for operator training.

5.6 Design extension conditions

In case of an occurrence of a design extension condition, the CBP system shall not be assumed to be available (see NOTE). A set of paper-based procedures designed to cope with such an occurrence shall be available to operate the plant from the MCR, i.e. the CBP should not be designed to operate in these situations.

NOTE As it is not designed to cope with design extension conditions, it is assumed that the CBP system may become unavailable or unreliable at any time.

The update of the CBP and paper-based procedure sets shall be coordinated and aligned with backup procedures.

The operating teams shall be trained to use these procedure sets and exercises shall be performed periodically.

6 Contexts of use of CBP

6.1 General

Clause 6 gives requirements for the various contexts of use of CBP. It considers different use environments relative to the MCR and in possible conjunction with paper-based procedures. It then considers the requirements of the possible different forms of assistance to and coordination of operator's activities. It concludes with the expected documentation.

6.2 Application environments of CBP use

6.2.1 General

Subclause 6.2 considers the different environments where CBP can be used, either in new computerised control rooms, or for partial modernisation of conventional control rooms, in conjunction with paper-based procedures or local operation by the field operator.

The overall integration of CBP in the MCR and in other control points shall be done based on IEC 60964, IEC 60965 and IEC 61513. Application of VDU shall comply with IEC 61772. Alarm functions and presentation shall comply with IEC 62241. Software shall comply with IEC 60880 or IEC 62138 according to safety category.

6.2.2 Use of CBP in computerised control rooms

It shall be possible to separately control the display formats of the CBP system and other display formats of the DPDS.

Compatibility between CBP formats and operating formats of a DPDS should be ensured by:

- designing compatible HMI layouts and details for display formats, i.e. abbreviations, symbols, colours, etc.,
- avoiding discrepancies when operating formats and CBP formats refer to the same object, circuit or equipment,

- updating without significant time difference associated formats of the DPDS and CBP formats when displayed at the same time.

6.2.3 Use of CBP in a conventional or hybrid main control room

A “conventional control room” is one that has been designed without any digital equipment. A “hybrid control room” is one that encompasses digital devices to monitor and control part(s) of the plant, but not the whole plant. Conventional control rooms can be modernized to become hybrid control rooms. The extent of computerisation of a hybrid control room, excluding the whole plant control, may vary a lot according to the utility objectives.

To implement CBP in a conventional or hybrid control room, the constraints of the existing MCR, i.e. mainly free space, and the operator work areas shall be considered in addition to those of 5.2.3. Introducing devices to display CBP in a conventional MCR may require existing elements, indicators, push-buttons, etc., to be relocated in order to make room to install sets of VDUs and related equipment, such as keyboards, pads, tracker balls, etc.

NOTE Services such as HVAC (heating, ventilation, and air conditioning) capacities are also considered.

As a specific challenge of conventional and hybrid control rooms, the concurrent use of CBP with discrete equipment, such as indicators, recorders, push buttons, auto-manual control stations, etc., should be studied. In addition, concurrent use of CBP and paper-based procedures has to be expected and shall be analysed.

Taking into account that the plant control computerisation is limited, CBP should be designed to provide information and guidance, i.e. they should belong to Family 1 or Family 2, and should comply with the requirements associated with these families.

In addition, specific provisions should be made to:

- design CBP HMI so that, in case of VDUs displaying information, the operator does not confuse CBP with any other displayed formats, especially in accident conditions. If there are no other digital display formats, ISO 11064-1, ISO 11064-3, ISO 11064-4 and ISO 11064-5 and IEC 61772:2009, especially Clause 4, shall be used to define any displayed formats that are required,
- enable the operators to read CBP from their working areas, either in front of the VDU or at some distance from the VDU.

6.2.4 Use of CBP in conjunction with paper-based procedures

CBP may be used together with paper-based procedures, either due to design reasons or for temporary reasons depending on the options defined according to 5.2.3.

EXAMPLE 1 Detailed operation remains paper-based whereas operating strategy is computerised.

EXAMPLE 2 Specific sets of paper-based procedures being used for example during outages, being used because a mistake has been detected in a computerised procedure and a set of paper-based procedures is used until a correct new computerised version is prepared.

Such situations shall be designed so that:

- there is no gap between CBP and paper-based procedures,
- possible overlaps between CBP and paper-based procedures are functionally justified,
- references and naming of CBP and paper-based procedures are consistent and do not lead to human errors,
- transfer between CBP and paper-based procedures is clear,
- traceability of actions done with both CBP and paper-based procedures is ensured,
- the situation remains easy to explain during staff changeover.

6.2.5 Use of CBP outside the main control room

If some local control rooms, the SCR for example, are computerised and operated with CBP, these latter shall be adapted to the operator's tasks.

Operation from local control points, if computerised, or from any types of portable devices, shall respect the requirements given in 6.4.

6.3 Forms of CBP assistance to operator activities

6.3.1 General

CBP shall be designed to allow for operators' responses to the conditions by taking account of the real plant situation, by monitoring the process and detecting events.

Procedures are designed to assist the operator by suggesting operation strategies and preparing possible actions regarding the plant state. Nevertheless, unexpected situations could happen so that the operator has to be able to achieve the high level goal set by a procedure even if some parts of it have become irrelevant.

For the purposes of this standard, the functions provided by CBP are divided into primary functions (e.g. the provision of information to the operator) and secondary functions (e.g. the management of windows and the navigation within the required information).

6.3.2 Assistance to primary activities of the operator

The following concepts of the CBP shall be considered during the design phase with a documented justification of the design decisions against each concept:

- compatibility with the operator's representation
HMI aspects are compatible with the operator's mental processing, i.e. with the operator's understanding, experience and expectation about the plant state and evolution and the way in which the CBP function
- situation representation
information displayed is easy to identify and to understand, accuracy of displayed values is consistent with accuracy of the sensed values, so that it helps mental processing and the progression of the operator towards the functional goal of the procedure. Data validity should be displayed
- HMI structure
HMI aspects are based on logical and consistent rules. The main HMI aspects are information presentation, sequences hierarchy within a procedure, terminology, assistance phraseology, lists structure, etc.
- compatibility with the activity
information displayed is relevant to the plant situation
- operator capabilities
the amount of information displayed allows the operator to understand it and there is enough time given to the operator to make proper decisions

Contextual information may be displayed to reinforce the relevance of information and to assist the operator's understanding.

6.3.3 Assistance to secondary activities of the operator

In order to simplify the operator tasks and allow him to concentrate on the primary tasks, the following aspects shall be considered during the design. The main design decisions against each aspect should be documented, including a justification:

- the operator's mental workload
memorisation of items, such as lists of codes, command codes, information to memorise from one page to another, is minimized
- the operator's actions
it is easy to perform an action and any redundant action is avoided

Secondary activities on CBP should be easy to perform in a reliable manner, so that accomplishing the primary activities is not degraded.

6.4 Assistance with operator coordination

CBP should make explicit the communication with respect to the sequences assigned to the individual member of the operating team, i.e. the communication necessary due to the task-sharing between the operators and the supervisor. Such coordination may be implemented by hold points in procedures, requesting oral dialogues and computerised acknowledgments.

Note that for example, when the supervisor is the only CBP user and then coordinates the other operators, or both the supervisor and the primary and secondary operators are provided with CBP, the procedure has to say what communications between them are necessary.

If several operators can simultaneously access the same CBP, rules shall be stated controlling the concurrent access to a single procedure. The following topics shall be defined:

- who can access it, regarding the authorisation level;
- which kind of access is allowed: read only, or full use;
- how a CBP is accessed, with regards to CBP being currently processed;
- how to prevent an operator from repeating or stopping an action already launched by another operator, especially when CBP are designed to control the plant. This may be achieved by reservation of procedures, which ensures that only one operator at a time can use CBP to control the plant, whereas all other operators are provided with read only access.
Procedure reservation requires a policy to be defined regarding possible calls of another procedure or of a sub-procedure;
- what CBP signals are provided, i.e. signals warning that a CBP is currently being used or signals indicating that a CBP is reserved for a long time without being used.

All or only specific procedures may be assigned to specific workstations.

CBP shall provide coordination of operators for parallel use of CBP in the main control room and in local control points. Possible digital communication failures should not decrease reliability and availability of CBP in the MCR and in local control points. Significant difference in progress between operators applying the same set of CBP should be signalled in order to avoid uncoordinated control of the process.

6.5 Output documentation

All options defined according to 6.3 and 6.4 should be documented in appropriate documents:

- a summary giving options and rationales for the design, development, validation or licensing phases,
- a summary for operators. It should be a reminder and easy to use in abnormal plant situations,
- a detailed document as a guideline for CBP design and maintenance.

This documentation shall be updated together with further CBP modifications to ensure completeness.

7 CBP system and functional requirements

7.1 General

Clause 7 deals with the digital system processing CBP, whether integrated in the DPDS operating the plant or independent from it. Safety and non safety requirements are considered.

It then gives requirements for the handling of failures of the CBP system. It concludes with output documentation.

Whatever the solution, screensavers shall not be used.

7.2 Safety requirements

It is necessary to consider carefully the fundamental safety role of a CBP and if it has any role in safety at all, or if it is part of the defence in depth strategy of the plant as a whole. The CBP system shall not compromise the defence in depth of the I&C system of the plant.

Procedures, whether paper- or computer-based and whatever their level of guidance, are designed to be used by the operator and they shall not control the process without the operator's involvement (i.e. operator initiation and supervision). The operator is expected to act in an intelligent way, not to apply them automatically, and to remain solely responsible for their adequate use.

The safety classification of the CBP system may be class 1, 2 or 3 or even not safety classified according to IEC 61513. The class shall be attributed considering:

- a) the functional coverage of CBP,
- b) the CBP family type,

NOTE 1 The different family types of CBP are listed in 5.3.

- c) possible impacts on safety in case of:

- 1) loss of CBP,
- 2) erroneous guidance to operators or spurious control signals,

EXAMPLE The possible and acceptable failure modes of each CBP, the impacts on operator awareness and ability to respond to plant events, likelihood of operator error (e.g. due to time availability, complexity and safety significance of decision making etc.), and availability of back-up means to recover from the failure.

- d) availability of diverse information displayed to the operator, allowing confirmation of information displayed by the CBP. The operator should be trained to undertake such comparisons (see 9.9).

NOTE 2 Though IEC 61226:2009, 7.3.2.1, opens the possibility to perform manually category A functions by interfacing a CBP system with a class 1 system, the attention of the designer is drawn to the fact that this would necessitate significant analysis in support of the safety demonstration, especially from the HFE aspects.

CBP may be implemented in several sub-systems with different safety classifications.

The requirements and guidance given in IEC 61513, IEC 60880 and IEC 62138 shall be applied to the design and implementation of the overall I&C architecture including the CBP system, as well as for the CBP system itself. The level of redundancy of the CBP system shall be consistent with the safety class of the CBP system. The requirements given in IEC 61772:2009, 4.3, shall be applied.

NOTE 3 The achievable system class could limit the feasible options in terms of CBP design approach, including what CBP family types could be implemented. If the required system class cannot be achieved and qualified, an alternate approach will be considered. This could require changing the CBP family type, design approach and functional allocations. It could also require changing the CBP platform selection, changing the communications

mechanisms, or changing the overall architecture. Failure to consider such issues early in a CBP system implementation project can result in costly delays and the need for redesign.

In case no safety class is attributed to the CBP system, requirements commensurate to possible operating impacts should be defined based on the IEC standards listed in the preceding paragraph.

Adequate checking of sequences launched from the CBP shall be implemented in plant control systems. This shall include any interlocks needed to ensure safety.

Particular attention, during development and verification phases, shall be given to ensure that potential faults or failures of the CBP system cannot disable, inhibit or launch manual and automatic functions. Functional consequences of erroneous or desynchronized data received from other systems, in particular automation systems, should be investigated. Safety studies shall consider the overall I&C architecture including the CBP system as well as the CBP system itself.

7.3 HMI considerations

IEC 61772:2009, especially Clauses 4 and 5, and ISO 11064, especially ISO 11064-1, ISO 11064-3, ISO 11064-4 and ISO 11064-5, give guidance for HMI.

Regarding the HMI of CBP display formats, only three cases are possible:

- 1) a digital system, DPDS, is already used to operate the plant at the time the CBP and CBP system are being designed: the HMI of the two systems shall be compatible;
- 2) a digital system, DPDS, is being defined in parallel with the CBP and the CBP system: the HMI of the two systems shall be compatible. IEC 61772 and ISO 11064 should be used for designing the display formats of both systems;
- 3) there is no other digital system displaying information on screen to operate the plant. IEC 61772 and ISO 11064 shall be used to design the CBP display formats.

7.4 Integration of the CBP system into the DPDS

In order to integrate the CBP processing into the DPDS, it shall be verified that:

- the safety class of the DPDS is able to cope with the safety class of the CBP as defined according to considerations in 7.2,
- DPDS features comply with the requirements of 5.2.3,
- for “family 3” CBP implementing category B functions, both the plant display system and the communications links to and from it should meet IEC 61513 and IEC 62138 class 2 requirements,
- DPDS features comply with the requirements of Clause 8.

IEC 61772 requirements and recommendations shall be applied.

7.5 CBP system implemented externally to the DPDS

7.5.1 General

Subclause 7.5 complements the safety requirements stated in 7.2 and deals with connections between the CBP system and the DPDS.

For Family 2 and Family 3 CBP that interface with the plant through the DPDS, the CBP system and the DPDS should be attributed compatible safety classes and requirements unless a clear justification is provided otherwise.

For Family 3 CBP, the task allocation between the CBP system and plant control systems should be:

- the initiation of automatic sequences by the operator should be at the computer display level, as well as the hold point treatment,
- automatic sequences, possibly using plant inputs and actuators' feedbacks, launched from the CBP should be processed by plant control systems.

7.5.2 Sizing and dependability requirements

In addition to safety requirements, there are additional fields to be considered:

- the CBP system shall comply with the requirements of 5.2.3,
- reliability and availability requirements shall be compatible for the CBP system and the DPDS,
- self-tests shall be specified,
- spare capacity should be specified for possible extensions considering items such as memories, processor capacity, storage capacities, network capacities, number of connected workstations.

7.5.3 Connections between the CBP system and the DPDS

The architecture and system aspects shall be compliant with IEC 61513.

Provisions in order to avoid discrepancies between commands sent by both the CBP system and the DPDS shall be implemented or, at least, such discrepancies shall be signalled to the operator.

Considering that some variables issued from the process or equipment can be used both by the CBP system and the DPDS to process different functions and possibly be displayed in different formats, then:

- both systems should be analyzed together regarding failure modes as well as the back-up process in case of failure and periodic testing,
- the CBP system should not be jeopardized by possible failures of the DPDS, and vice versa,
- failure of the CBP system should be signalled by the DPDS and partial or total failures of the DPDS should be signalled by an independent alarm,
- failure of the interface between the two systems should be signalled at least by one of the two systems,
- the sending of orders from both systems to the same actuator, either simultaneously or within a few minutes, shall be signalled. Contradictory orders shall be signalled in a specific way,
- provisions should be taken to minimize time differences in updating dynamic parts of displays for the same object. A value in the range of 2 s may be considered acceptable, greater differences should be signalled.

7.5.4 Coherent maintenance of both systems

Maintenance from the hardware, software, configuration and application points of view shall be considered for both systems, including the requalification process.

7.6 CBP system failure

Generic considerations regarding failures in VDU displays are given in IEC 61772:2009, 4.3 and 4.4.

Operators shall be trained to have a questioning attitude regarding the CBP performance. To support them, self-monitoring and self-test provisions for detecting and signalling malfunction shall be implemented in the CBP system. Considering the possible consequences of

operators' misguidance, the coverage of the self-monitoring should be as high as possible. For Family 3 CBP, adequate fail-safe mechanisms should be provided where possible. To enforce detection of CBP malfunction, a part of the operating team may use paper-based procedures.

NOTE 1 The main ways to detect malfunctions are currently self-monitoring, implemented according to IEC 60671, independent monitoring mechanisms, and periodic surveillance performed by the staff.

If an operator suspects a malfunction of the CBP which has not been detected or annunciated by the system, for example unexpected parameter deviations, the CBP system, parts thereof, or underlying I&C subsystems may be considered unavailable.

In the event of failure of CBP important to safety or failure of a CBP system implementing safety-related (i.e. category B or C) functions, a diverse back-up means and an adapted procedure set shall be used. This back-up procedure set shall be compatible with the DPDS, if this latter is still available and used to operate the plant.

NOTE 2 The extent of the back-up means and the associated procedures will be typically restricted to the set of functions necessary to put and maintain the plant in a safe state, and to minimize impact on plant operation until the CBP system or DPDS is restored.

A diverse set of procedures designed to back-up the CBP system (e.g. such as paper-based manual procedures) shall take into account that this situation is rare and stressful, and shall aim to avoid operators' mistakes or misunderstandings by:

- being independent from the CBP system, both from technical and functional points of view, i.e. there is no reference to information existing only in the CBP system,
- relying on operating strategies similar to those of CBP,
- being designed for the same operating staff,
- using as far as possible the same vocabulary and graphic elements, and procedure presentation consistent with that of the CBP.

The back-up procedure set, and any associated back-up system, shall be easily accessible.

The back-up system, and the back-up procedure set, if computerised, shall have been designed, developed and validated according to their safety class and shall comply with Clause 9 requirements.

NOTE 3 Choosing a second set of CBP as a back-up is a great challenge for it implies a diverse CBP system featured with malfunction detection, more complex maintenance and operator training. For this reason paper-based procedures are usually preferred. To make such a decision, economical aspects are also considered.

If the CBP is implemented as a system separate from the DPDS, the following apply:

- the DPDS should monitor the CBP system and signal the detected faults to the control room staff,
- the DPDS should not be blocked in case of failure of the CBP system.

7.7 Output documentation

The system and functional requirements and related design rationale (options and decisions) for the overall architecture and CBP system approach shall be documented consistently with IEC 61513 requirements (and appropriate sub-tier standards such as IEC 62138) and in a manner consistent with the safety class of the system.

8 Detailed design requirements

8.1 General

Clause 8 provides guidance and describes requirements for a detailed design of CBP features, from the basic ones to the most sophisticated ones, i.e. information, navigation, guidance and plant control. Various options that could ease CBP use are also given.

8.2 Basic CBP features

8.2.1 General

To coordinate development, to avoid misinterpretation when using CBP, and to ease their maintenance, basic CBP features shall be defined at the very beginning of the project and shall be used throughout the CBP life cycle. They shall be used to design, develop and maintain the CBP set.

NOTE People who update CBP may be different from people who first developed them.

This activity should be performed by the integrated team introduced in 9.3. It should take into account feedback of experience, based on use of paper-based procedures and on known other cases of use of CBP.

Any further change to the features defined according to Clause 8 should be justified and formally accepted and documented.

8.2.2 Basic features necessary for CBP

The following basic CBP features should be defined in an accurate and unambiguous way:

- all technical terms, symbols and graphic elements,
 - a glossary giving the meaning and use of every format element,
 - symbols or drawings representing elementary CBP steps, as well as links between them,
 - rules for processing the content of CBP steps,
 - rules for allocating names to calculated or internal variables,
- NOTE Variable names help the operator to understand the type and the use of a calculated variable.
- navigation rules between elementary steps, pages or sequences of a CBP and between CBP.

Elements such as “steps”, “indicators”, “decision boxes”, as well as combinations thereof, which are designed to be generically used, should be defined as re-useable elements, with a set of parameters to be specified.

For procedures that have been interrupted and re-entered, there should be some confirmation that the conditions and assumptions are still valid to continue the execution.

8.2.3 Presentation rules

In order to minimise the operator’s mental workload, and to be consistent with the generic requirements of 5.4.2, CBP presentation should be designed so that:

- local actions are clearly identified,
- an overview of the procedures currently executed and of currently interrupted procedures is provided to the operator,
- procedure presentation is consistent throughout the CBP and consistent with the presentation paradigms of the DPDS,

- the possibility of operator errors using both CBP and a DPDS to operate the plant are minimised,
- information needed to perform the procedure is readable from the working position of the operator,
- the most recently approved and issued version of a procedure is always presented.

Exceptions to these requirements shall be justified.

To minimise human errors, the format contents should:

- a) display the identification of the current procedure and of the current sequence within that procedure,
- b) identify clearly the achieved steps, active steps, and possible next steps,
- c) minimise the number of discrete actions to access a required format display,
- d) ease dialogue between operator and procedure.

8.2.4 CBP display format layout

The CBP display format layout should be designed so that:

- the identification of the procedure, i.e. title and functional coding, as well as the functional procedure objectives, are permanently visible as part of the procedure format and have a permanent location in the format;
- allocation of information follows the same method throughout all procedures;
- division of a procedure into sequences is done according to consistent rules;
- the importance of steps is displayed in a salient manner;
- warnings, cautions, and other information associated with a single step are visible whenever this step is displayed.

Any such warnings, cautions and information are presented in such a way that they have to be read, for example by using pop-up menus which have to be confirmed by the operator, before the operator is able to start performing this step. If used, pop-up windows should appear in predefined parts of formats, should not hide too much of a format and should be easy to move from one place to another or to iconize, close or memorize depending on the context. They shall not disturb the use of CBP, for example by skipping or masking or duplicating steps or sequences or by blocking formats on screens.

8.2.5 Requirements for presentation of individual display elements

Rules for presenting individual elements are as follows:

- information and action steps should look different,
- presentation of decision gates with their associated choices (e.g., "yes" or "no") should be uniform whatever the procedure,
- if an operator's response is required, the automation should not proceed without operator response.

Whenever procedure formats contain repetitive information elements, such as a set of plant components, a set of similar actions, etc., the presentation of these information elements should be in terms of lists. The design should ensure that:

- a) the list stands out from other parts of the procedure,
- b) the priority of items is clearly marked,
- c) all lists have a heading,
- d) the operator attention is attracted to the list.

8.3 Information presented by the CBP

8.3.1 General

Information about the CBP system should be available to the operator, for example designation, version, release date, page number. Such items should either be systematically displayed or should be displayed upon the operator's request.

All CBP families shall feature this kind of information,

- so that the operator is able to use the CBP guidance correctly,
- in order to keep the operator fully informed of the changing plant status.

Alarms and messages generated by a process or an installation incident shall be adapted to the operating phase where they can be displayed and shall not mislead the operator or create doubt in his mind.

Alarms generated by CBP shall be displayed in the same way as those generated by process or equipment events. IEC 62241 should be used as a design reference.

8.3.2 Information for Family 1 CBP

Family 1 CBP are similar to paper-based procedures in that they indicate process and equipment values to be monitored but do not display any dynamic information from the plant.

8.3.3 Information for Family 2 CBP

In order to provide an adequate understanding of the operation, CBP information for Family 2 CBP shall include all indications and inputs from the process and equipment that are:

- necessary to understand and perform the operating strategies,
- necessary to understand the context, plant state and displayed messages, relevant to the procedure.

The quality of CBP information should be ensured by:

- a) an update frequency of parameters adapted to the needs of the procedure,
- b) prompt presentation of possible conflict between inputs typed by an operator and acquired or computed values.

Cross-referenced information should be easily accessed by the operator. Paper-based procedure steps involved in the cross-checking of data should be carried over to the CBP solution.

Information availability should be indicated to the user. More generally, information status should be accessible, for example: available, inhibited for test, inhibited for maintenance, unavailable, inconsistent with other inputs.

Applying the design policy should lead to decisions on displaying:

- 1) summarised information,
- 2) information related to the plant state,
- 3) information chosen by the operator.

NOTE These options may require that additional values are calculated by the CBP system based on inputs or other internal values. It may also lead to a requirement to complement raw inputs by an indication of their reliability, resulting for example from cross-checking of different values.

Additional computed values should:

- be accessible by the operator as for any other acquired field signals,
- be easily identified when displayed on VDU, for example by specific encoding or by a specific colour.

Information features may differ depending on the types of procedures listed in 5.2, provided that the HMI formats remain consistent.

The guidance policy may require that possible discrepancies between operators' actions and the suggested decision are signalled.

8.3.4 Information for Family 3 CBP

In order to automatically control the plant and/or to provide adequate guidance capability, all the types of Family 2 CBP information, mandatory and optional, shall be provided to Family 3 CBP.

8.4 Navigation

8.4.1 General

Navigation possibilities should be implemented in line with the HMI of the DPDS and CBP policies.

8.4.2 Navigation for Family 1 CBP

Navigation for Family 1 CBP should include options to go directly to pages, skim through pages and to retrieve terms in pages.

Enhanced options may be implemented for:

- retrieving pages or sequences, such as bookmarks, indexes, table of contents;
- displaying contextual information such as pop-up windows or thumbnails;
- standardizing subroutines, such as pipework warm-through or rod withdrawal processes.

Links to related procedures, for example to technical specifications or alarm response procedures, may be provided. They should not be confused with individual steps.

If several procedures are simultaneously active, it should be possible to move from one to another, even if it is not currently displayed.

8.4.3 Navigation for Family 2 and Family 3 CBP

Navigation for Family 2 and Family 3 CBP extends Family 1 CBP navigation features to sequences and individual steps inside a procedure.

In addition, procedures may be explored according to step types, for example to find the next decision gate regarding primary pressure.

The option to trace the path that was followed by the operator up to the current situation should be provided. This trace should include all procedures that interact between each other. Typically, such traces should start automatically for CBP related to operation in case of an accident. These historical formats should not be confused with formats related to the current situation.

8.5 CBP guidance

8.5.1 General

CBP guidance relies on the same bases as paper-based procedures but is extended to achieve the computerisation policy. This guidance ranges from elementary information on the process to enhanced assistance for:

- CBP selection, accessibility and execution,
- diagnosis,
- decision making.

NOTE The guidance detail varies, partially due to the nature of procedures, for example accident procedures provide more guidance than normal operation procedures, and partially due to the expected operator knowledge, which relies on the training policy.

8.5.2 CBP selection, accessibility and execution

A CBP, like a paper-based one, should be selectable and accessible, depending on its nature:

- if the intention is a change of the plant state, for example start-up, outages,
- in response to an alarm or a process or equipment signal,
- periodically, for example surveillance procedures that are entered on every shift changeover.

Considering CBP, plant events or periodic events may signal automatically which type of CBP is to be accessed. A specific procedure may be recommended or automatically selected.

Access to the right procedure should be as direct as possible, i.e. a too complex selection path should be avoided.

CBP may also allow the operator to automatically monitor the process or equipment values and to define thresholds for these values. When a threshold is reached, a signal may be sent and, provided that neither the information needed nor the prerequisite actions and cautions are bypassed, the relevant CBP step may be directly accessed and displayed.

CBP should remain manually accessible and the initiating event should be displayed on operator's request.

8.5.3 Diagnosis assistance

Particular plant situations clearly specified by the designer, for example accidents or any event indicated by the deviation of safety parameters, may be identified during operation and signalled. The diagnosis of the plant situation should be presented by the CBP as a set of monitoring steps and decisions, leading to possible further investigations and recommended corrective actions.

The operator shall remain responsible for accepting the diagnosis and accessing the suggested procedure.

Details of the diagnosis should be displayed on operator's request.

8.5.4 Decision assistance

Decision assistance should be limited to steps requiring a decision. Information, such as inputs, alarms, trend curves, synthesised values, etc., that are then necessary shall be available and easy to display.

The operator shall remain responsible for making any decision.

To enhance decision assistance, the CBP should signal that:

- the suggested procedure has been launched,
- each step has been validated by an operator,
- each step has received a positive feedback signal,
- the operator's choice in the case of a decision gate matches the suggestion,
- the objectives of the considered procedure have been achieved.

Feedback signals from actuators and sensors may be used, for example in complex situations, to verify that the operator's actions match the CBP steps. If this option is chosen, inconsistencies should be signalled but shall not prevent any operator actions.

NOTE The main types of feedbacks to be considered are:

- feedbacks from controller to confirm plant or equipment states,
- feedbacks to confirm controller states, especially safety interlocks,
- feedbacks to confirm hardwired panel switch or alarm states,
- feedbacks to confirm status of other display indications or related permissive functions available to the operator,
- feedbacks to confirm internal states of CBP, controller, alarm status, other display systems, etc.

8.5.5 Computerisation of CBP guidance

Whatever the type and level of guidance, CBP shall be computerised so that:

- they display all necessary elements to enable the operator to understand and be in control of the plant in any situation,
- they provide a reasonable and pertinent level of information in order for the operator to assimilate it, and not be distracted or puzzled by inadequate assistance,
- they leave the operator responsible for his actions, either by requesting the operator to validate suggestions or to choose a course of actions different from the suggested actions,
- they provide on operator request the display of rationales for suggestions,
- they distinguish between suggestions and steps or information,
- they do not hide an important part of a format being displayed by less important information,
- freeze of information update, for example due to an equipment failure, is easily detected.

Assistance should be displayed on operator request and the operator should be able to switch it off at any time.

Provisions to disable temporarily the display of warning messages that could be issued by assistance functions should be given to the operator. It shall not be possible to inhibit process alarms.

The use of other procedures may be suggested, and links to them may be provided.

8.6 Procedure-based automation

8.6.1 General

CBP may be designed to automatically execute some operating tasks under the operator's control.

8.6.2 Interactions between operators and procedure based automation

The task allocation between operators and digital systems shall be based on IEC 61839, possibly justified by criteria relevant to a specific project. CBP shall be designed to:

- make the operator aware of the safety significance of the sequence,
- continuously inform the operator of what is being processed,
- enable the operator to take manual control at any time,
- support appropriate operator confirmations, for example by checking parameters, prior to execution of automatic sequences,
- provide adequate automatic (or require manual operator) checks on plant or equipment states to ensure requested sequences are permitted and safe at that time and in the current plant state,
- make the operator aware of time dependent operator actions, for example via task timers,
- inform the operator of the CBP state, for example read only, manual execution, automatic execution, etc.
- enable, after adequate checking of parameters, the operator to resume automatic execution after a manual interruption of a sequence,
- alert the operator to an unexpected event which could prevent the correct processing of the procedure. Means to display the cause of such an alert should be given to the operator.

Additional options should be investigated, for example CBP may enable operators to select parts of CBP they wish to be automatically followed.

8.6.3 Design of CBP to control the plant

In order to control the plant, CBP shall be designed so that:

- unless overridden by the operator automated sequences should begin and end within the same procedure,
- priority between control actions launched from CBP and control actions launched manually or from the DPDS is established in line with the priority rules for manual and automatic functions,
- sequences are predetermined and fixed. They may include hold points requiring operator's acknowledgment,
- the availability of equipment or of a circuit, when required to process a step, is first verified,
- automatic activities are time-stamped and archived, as well as manual operators commands.

For control sequences important to safety, adequate feedback confirmations (or alternatively request for manual operator confirmation, or both) of appropriate plant or equipment state prior to initiation of automated control sequences and again to confirm successful completion of control actuations should be provided. Deviations should be logged and alarms sent (as appropriate) to the operator.

If some procedures cannot be displayed by VDU, either because there are too many of them or because of limited VDU capacity, provisions should be made to enable them to:

- a) signal or send alarms for significant events,
- b) give periodic signs of life to indicate the procedures are still processing. Alternatively, some procedures may be automatically stopped or frozen depending on designers' specification,
- c) be displayed on operator's request.

Analyses should be undertaken during the design phase to demonstrate that operation is not jeopardised even if some procedures that are in operation are not continuously displayed on the VDU.

If a Family 3 CBP automation function is available from more than one HMI then appropriate warnings, interlocks and handover of control should be implemented to prevent more than one CBP display location having active control of the same sequence (or possibly an interfering sequence) at any one time.

NOTE This minimizes the number and complexity of possible failure modes between CBP display stations and other plant displays and/or controllers. It also reduces the likelihood of operator coordination error under such circumstances.

8.7 Other CBP facilities

For each type of procedure, different options should be considered:

- the option of including operator notes in the CBP may be provided. This corresponds to what operators are used to doing on paper procedures. These notes could be used, for example for indicating the need to temporarily deviate from the CBP under specific conditions that are to be detailed,
- the option of selecting relevant process values to be monitored may be given to the operator,
- traceability and archiving facilities may be provided. In case of infrequent plant situations, it may be decided to record and archive the situation management through the use of CBP in order to analyse it later,
- recording of activities. An automatic record of the actions taken in response to the CBP steps should be made,
- the option of adapting the guidance to the situation may be provided in order to enable the operators to choose a level of guidance adapted to their skill regarding specific CBP or sequences.

8.8 Output documentation

The detailed design shall be documented in a manner consistent with the requirements of IEC 61513, IEC 60880 and IEC 62138, as applicable, according to the safety category of the CBP functions being implemented.

All the options defined according to Clause 8 should be documented in appropriate documents, including:

- a summary of options and rationales for the design, development, validation or licensing phases,
- a summary for operators. It should be conceived as a reminder that is easy to use in abnormal plant situations,
- a detailed document to be used as a guideline for CBP design and maintenance.

This documentation shall be updated together with further CBP modifications to ensure completeness.

9 CBP life cycle

9.1 General

Clause 9 establishes requirements and recommendations for the whole CBP life cycle from the project organisation to the CBP maintenance and the operator training, with specific attention given to CBP verification and validation.

9.2 Project organisation

A project for computerisation of procedures brings together the HMI, operating strategies, and software engineering aspects. The organisational aspects of the HMI and operating strategies are similar to those of the paper-based procedures. The software aspects should, if the CBP system is important to safety, be established based on IEC 61513, considering it is similar to any other software development, and addresses safety classified CBP or non safety classified CBP.

The first task should then be to organise a project team with all necessary competences and to identify a decision committee.

Based on the CBP policy, the project team should take responsibility for:

- design of procedures,
- development of procedures,
- verification and validation of procedures,
- review and approval of procedures,
- revision of procedures.

Engineering tools should be used for ensuring quality and traceability during the typical procedure life cycle phases. In all the project phases, computerisation is of potential benefit and may facilitate the work to be accomplished, especially traceability and archiving of different versions.

Formal reviews should be organised, any recommendations addressed and the conclusions archived.

9.3 Project team

Different kinds of participants should be brought together in order to design, develop, test and especially validate CBP:

- procedure designers,
- human factors specialists,
- computer specialists, when needed,
- all categories of end users, i.e. supervisors, operators, possibly field operators.

The operators' experience and needs, as well as the flexibility and capacity of displays, should be taken into account when designing the CBP look-and-feel in order to make the CBP more readily adopted by the operator.

These experts should be integrated into a team and should begin to work together from the beginning of the project.

9.4 CBP detailed design and implementation quality assurance (QA)

The detailed design and implementation QA requirements of IEC 61513, IEC 60880, IEC 62138 and IEC 61772 shall be applied depending on the safety class of the CBP system. In case the CBP system is not safety classified, requirements for safety class 3 systems may be used.

Whatever its safety class, the system processing CBP shall be self-monitored and detected failures shall be signalled.

A quality assurance programme, taking account of CBP safety classification, shall be defined to verify that:

- the requirements of Clauses 6 to 8 are correctly taken into account,
- traceability of development is assured,
- archiving of developed software is regularly performed, and back-up files are available and reliable,
- coverage of tests is optimal, and traceability and archiving of tests results is ensured,
- versions are correctly managed.

9.5 Verification and validation programme

The verification and validation programme requirements of IEC 61513, IEC 60880, IEC 62138 and IEC 61772 shall be applied depending on the safety class of the CBP system. In case the CBP system is not safety classified, requirements for safety class 3 systems may be used.

The verification and validation (V&V) of CBP consists of:

- V&V of the CBP system, hardware and software parts, according to its safety classification,
- technical, or static, verification of CBP (see 9.6.2).
The CBP verification shall address both the compliance of the visual display formats with HMI specifications and the technical aspects which animate the procedures,
- functional and ergonomic validation of CBP, involving a full scale simulator and operators (see 9.6.3).

The first two activities may be scheduled throughout the development phase, whereas the last one should be performed using comprehensive and coherent subsets of CBP or using the complete CBP set.

A verification and validation programme shall be established early in the project to ensure that, throughout the development phase, the requirements of Clauses 6 to 8 are fulfilled, to identify the necessary resources, i.e. human and digital tools, and to prepare the final verification and validation of the complete product. Adequate recording provisions should also be planned.

9.6 Verification and validation of CBP

9.6.1 General

Subclause 9.6 addresses system verification and validation of the technical and ergonomic aspects of the CBP, assuming that detailed design verification, including the software aspects of the CBP unit and module level testing, has already been performed according to appropriate safety and quality requirements.

A quality organisation shall ensure that any detected failure is corrected in a proper way and that associated documentation is adequately updated.

Clarity of presentation and easiness of use for implementation of the options defined in Clause 6 should be evaluated early in the project in order not to be questioned during CBP development.

Functional scenarios shall be designed to represent significant process events or operating situations.

Equivalency between CBP procedures and paper procedures shall be validated.

NOTE 1 Functional scenarios are the master plans for validating paper or computer-based procedures. Unfortunately, it is impossible to demonstrate that they cover exhaustively all plants situations, so that they are carefully designed.

NOTE 2 Consideration of additional types of validation scenarios will be needed for CBPs (i.e. over and above paper-based procedures) to validate events arising due to faults (and subsequent failures) within the CBP implementation.

9.6.2 Technical verification of CBP

The CBP verification should aim to detect erroneous application of 8.2 features, such as:

- use of undefined symbols, words, graphs, etc.,
- inconsistencies between the variables names and the information displayed,
- inconsistencies between the text of a step and the guidance,
- inconsistencies between the text of a step and the associated command.

The verification should aim to detect erroneous procedure design or programming that would prevent a safety or operational objective from being achieved, such as:

- a) procedures loops,
- b) deadlocks: information from procedure B is awaited by procedure A while procedure B is waiting for information from procedure A,
- c) open or wrong links to pages or steps.

Provisions should be taken so that the technical verification of CBP:

- 1) is as exhaustive as technically possible and reasonable,
- 2) relies on methods and tools which minimize ambiguous human interpretations,
- 3) issues auditable results,
- 4) is traced and easy to analyse,
- 5) facilitates regression tests.

In order to detect both possible programming and operating errors, consideration should be given to automatically processing all or selected procedures to pilot predefined scenarios computed by a process simulator. These scenarios, including abnormal plant situations, are defined in order to activate as many CBP functionalities as possible.

9.6.3 Functional and ergonomic validation

Validation should be performed in the same way as for paper-based procedures. Validation should be completed in an MCR training facility representative of the real MCR and of the real CBP and DPDS with capability to adequately emulate plant conditions and scenarios, including upset conditions, emergency and accident conditions as appropriate, to stimulate and confirm the response of the CBP being tested.

Appropriately qualified and experienced MCR operators should be involved in the review and acceptance of the test plan for any safety-related CBP.

Appropriately qualified and experienced MCR operators shall be involved in conducting the actual validation test of safety-related CBP.

The functional and ergonomic validation should aim to ensure that:

- functional allocation of tasks between operators and machines is correct and effective,
- the operator can understand and apply CBP in a correct way,
- CBP help the operator to achieve the expected functions, even in case of abnormal situations,
- no operating strategy errors remain undetected,

- CBP improve the reliability of the operator actions and reduce the risk that the operator does not respect technical specifications,
- operators have a good representation of the process and of their progression in procedures at all times,
- the team coordination is correct,
- operators are able to monitor and detect any failure in the CBP system,
- operators are able to switch back and forth from CBP and the CBP system to the back-up procedures set,
- the CBP look-and-feel is compatible with the look-and-feel implemented in the DPDS.

During validation, specific computerisation issues that could arise shall be assessed, as follows:

a) navigation between pages

the operators may find it difficult to understand which part of a strategy they are applying and to plan their next actions by "leafing through" computerised pages,

b) "tunnel effect"

the operator may become unable to think on his own, whatever the reason. For example, the operator may have lost grasp of the strategy and applies CBP mechanically or too much concentration is required to use CBP correctly so that the operator no longer understands their content,

c) mental processing of operators

the operator should be able to understand fully and easily the plant state and the implications of the actions proposed by CBP,

d) communication between members of the operating staff, and possibly with people from outside the operating staff.

The behaviour of Families 2 or 3 type CBP should be recorded while operating a scenario and analyzed by a functional team regarding the consistency between expected operating actions and actions processed by the CBP emulator.

NOTE Recording the behaviour of CBPs enables comparison of different operating strategies in order to select the best one. It is also useful to build a reference file which can be used to test future versions of CBP.

9.6.4 Output documentation

The system verification and validation requirements and results shall be documented in a manner consistent with the requirements of IEC 61513, IEC 60880 and IEC 62138, as applicable, and according to the safety category of the CBP functions being implemented. They will typically be needed to support issuance or renewal of the operating license.

9.7 Implementation of CBP in NPP

CBP will be typically implemented as application software executed in an application-independent system software. The following statements refer to the deployment of this application software. Modification of the system software of the CBP system will typically imply additional constraints which are not presented here.

CBP shall be deployed in coherent and well identified sets. A set may encompass several types of procedures that are interdependent.

Each set shall be deployed on line in a single batch and without impacting plant operations. The processing should be highly automated.

To deploy a new CBP version, the following conditions shall be fulfilled:

- the verification and validation phase results have been taken into account,
- operators have been adequately trained and informed,
- if needed, it is possible to re-install the old CBP version.

In order to simplify on-site management of CBP, some specific considerations should be given during the CBP design and development phases to:

- a) on-line management facilities,
- b) change of CBP version, which should:
 - 1) be easy to deploy,
 - 2) not require a change in the plant state,
 - 3) not impact plant operation,
 - 4) not impact the DPDS, if any,
 - 5) not impact the operating system of the CBP system,
- c) old CBP version archiving.

Adequate quality, i.e. detailed processing and traceability, shall be provided for each deployment. Too frequent deployments of newly developed or revised CBP should be avoided.

Before deploying a new version, all operating shifts shall have been trained in its use.

CBP system incidents and CBP errors should be recorded and transmitted promptly to the maintenance organisation.

9.8 Output documentation

As a general requirement, the various outputs required for Clause 9 shall be documented in a manner consistent with the requirements of IEC 61513, IEC 60880 and IEC 62138, as applicable, according to the safety category of the CBP functions being implemented.

The requirements of IEC 61513, IEC 60880 and IEC 62138 should also be used as appropriate to issue adequate documentation regarding:

- the organisation set up for design, development and validation CBP, as well as the organisation of CBP maintenance once in operation, based on the requirements of 9.3 and 9.5,
- all software programming documents, and those of 9.4 and 9.5,
- the results of CBP verification and validation, see 9.6.
- the documentation that should be automated to ease non-regression tests in case of CBP updating,
- the deployment of CBP, see 9.7.

A review of the complete documentation, issued from Clauses 5 to 9, shall be conducted to ensure that it is complete and coherent.

It is important to recognize CBPs will need to be modified, maintained, and possibly upgraded or replaced in the future. Design basis knowledge will be needed at various times over the CBP system life cycle. It is important to document complete design requirements, including design criteria, key assumptions, rationale, and constraints.

9.9 Training of the operating staff

The fundamental objectives and organisation of the training shall be similar to those for paper-based procedures. Operators who participated in the CBP validation phases should help to elaborate the training programme.

The training shall additionally accustom the operator to:

- operate the plant with CBP, wherever they are implemented,
- ensure periodically the correct functioning of the CBP system, and to detect potential failures,
- migrate to the procedure back-up system and back-up procedures and to operate the plant with them.

In case paper-based procedures are used as back-up, the training shall compensate for the lack of experience in applying them.

Provisions should be made to collect feedback of experience and to capitalise on it for further use, for example to upgrade CBP and to improve the operator's training. Gathering the feedback of experience should take place from the onset of the project. Particular attention should be paid to the first months of operation with CBP.

9.10 CBP and CBP system maintenance

Maintenance instructions for hardware, software, configuration and application shall be provided for tests, for repairs, for spare parts and for requalification. The use of specific tools shall be documented. IEC 61513, IEC 60880 and IEC 62138, as applicable, shall be applied in case the CBP system is safety classified.

Provisions to comply with a specified repair time shall be taken.

A V&V programme as detailed in 9.5 shall be defined and performed adequately with any CBP or CBP system maintenance. An assessment of change impact shall be done to determine appropriate test scope coverage, including regression tests, to fully test the changes made each time. Training of operators prior to installation and commissioning of changes is also required.

Updating of CBP shall be prepared off-line and should be planned in the same way as for paper-based procedures.

For each implementation of major revisions, quality provisions should be made to detect errors as early as possible. Operators may be involved in the verification of the procedures.

The CBP system should provide a framework of system software that allows loading of CBP versions without unnecessary change in the operation provided by the CBP system itself.

Chronological documentation for operation, repair and maintenance of the CBP system, if autonomous, shall be maintained. Operation records and reports shall be evaluated with a defined periodicity in order to identify and initiate any maintenance or modification activities that might become necessary. If CBP are processed as a part of a DPDS, maintenance of the latter shall take into account CBP availability and reliability.

NOTE The exact requirements for documentation depend on the specific operating organisation.

9.11 Feedback of experience

The use of CBP should be integrated in the plant's operating experience review, especially for a new design or modification.

Bibliography

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

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61227, *Nuclear power plants – Control rooms – Operator controls*

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems for nuclear power plants*

IAEA SSR 2/1, *Safety of Nuclear Power Plants: Design*

IECNORM.COM : Click to view the full PDF of IEC 62646:2016

SOMMAIRE

AVANT-PROPOS.....	49
INTRODUCTION.....	52
1 Domaine d'application.....	55
1.1 Objet de la présente norme	55
1.2 Contexte à l'origine de l'utilisation et du développement des PI	55
1.3 Vue d'ensemble des PI.....	55
1.4 Utilisation de la présente norme avec les normes associées	56
1.5 Structure de la présente norme	57
2 Références normatives	57
3 Termes et définitions	58
4 Termes abrégés	61
5 Politique associée aux PI et exigences conceptuelles.....	61
5.1 Généralités	61
5.2 Politique d'informatisation	61
5.2.1 Généralités	61
5.2.2 Règles sous-jacentes à la mise en œuvre des PI	62
5.2.3 Domaine des PI	63
5.3 Les familles de PI.....	64
5.4 Vue d'ensemble des caractéristiques de l'informatisation	65
5.4.1 Généralités	65
5.4.2 Exigences d'ensemble portant sur l'informatisation	65
5.4.3 Mesures de recommandation à l'opérateur.....	66
5.4.4 Mesures relatives aux procédures automatisées	67
5.5 Documentation produite	68
5.6 Conditions hors dimensionnement	68
6 Contextes d'utilisation des PI.....	68
6.1 Généralités	68
6.2 Environnements d'application pour l'utilisation des PI	68
6.2.1 Généralités	68
6.2.2 Utilisation des PI dans les SdC informatisées	69
6.2.3 Utilisation des PI dans une SdC conventionnelle ou hybride.....	69
6.2.4 Utilisation des PI en parallèle des procédures papier	69
6.2.5 Utilisation des PI hors de la SdC	70
6.3 Formes d'assistance fournies par les PI pour les activités des opérateurs	70
6.3.1 Généralités	70
6.3.2 Aide aux activités principales de l'opérateur	70
6.3.3 Aide aux activités secondaires de l'opérateur	71
6.4 Assistance à la coordination des opérateurs	71
6.5 Documentation produite	72
7 Système PI et exigences fonctionnelles.....	72
7.1 Généralités	72
7.2 Aspects de sûreté	72
7.3 Considérations sur l'IHM	74
7.4 Intégration du système PI dans le SANC.....	74
7.5 Système PI mis en œuvre de façon externe au SANC	74

7.5.1	Généralités	74
7.5.2	Exigences de dimensionnement et de fiabilité	74
7.5.3	Connexions entre le système PI et le SANC	75
7.5.4	Maintenance cohérentes des systèmes	75
7.6	Défaillances du système PI	75
7.7	Documentation produite	76
8	Exigences relatives à la conception détaillée	77
8.1	Généralités	77
8.2	Fonctionnalités de base des PI	77
8.2.1	Généralités	77
8.2.2	Eléments de base nécessaires aux PI	77
8.2.3	Règles de présentation	78
8.2.4	Modèles des images affichables par les PI	78
8.2.5	Exigences portant sur la présentation des éléments individuels	79
8.3	Informations présentées par les PI	79
8.3.1	Généralités	79
8.3.2	Informations concernant les PI de la Famille 1	79
8.3.3	Informations concernant les PI de la Famille 2	79
8.3.4	Informations concernant les PI de la Famille 3	80
8.4	Navigation	80
8.4.1	Généralités	80
8.4.2	Navigation pour les PI de la Famille 1	80
8.4.3	Navigation pour les PI des Familles 2 et 3	81
8.5	Recommandations des PI pour la conduite	81
8.5.1	Généralités	81
8.5.2	Sélection, accessibilité et exécution des PI	81
8.5.3	Aide au diagnostic	82
8.5.4	Aide à la décision	82
8.5.5	Informatisation des recommandations produites par les PI	83
8.6	Procédures automatisées	83
8.6.1	Généralités	83
8.6.2	Interactions entre les opérateurs et les procédures automatisées	83
8.6.3	Conception des PI pour conduire la tranche	84
8.7	Autres fonctionnalités associées aux PI	85
8.8	Documentation produite	85
9	Cycle de vie des PI	85
9.1	Généralités	85
9.2	Organisation du projet	86
9.3	Equipe projet	86
9.4	Assurance de la qualité (AQ) pour la conception détaillée et la mise en œuvre des PI	86
9.5	Programme de vérification et de validation	87
9.6	Vérification et validation des PI	87
9.6.1	Généralités	87
9.6.2	Vérification technique des PI	88
9.6.3	Validation ergonomique et fonctionnelle des PI	88
9.6.4	Documentation produite	89
9.7	Mise en œuvre des PI sur une centrale nucléaire de puissance	90
9.8	Documentation produite	90

9.9	Formation de l'équipe de conduite	91
9.10	Maintenance des PI et du système PI	91
9.11	Retour d'expérience	92
Bibliographie		93
Tableau 1 – Familles de PI.....		64

IECNORM.COM : Click to view the full PDF of IEC 62646:2016

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) nouveaux 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.

IECNORM.COM : Click to view the full PDF of IEC 62646:2016

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 cybersécurité, 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.

IECNORM.COM : Click to view PDF of IEC 62646:2016

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 opérateurs¹, 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 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 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 clés 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*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>.

3.1

système de secours

autre ensemble de matériel conçu pour réaliser la surveillance et la commande de la centrale destiné à être utilisé en cas de défaillance du système d'IHM utilisé normalement

Note 1 à l'article: Le système de secours peut devenir indisponible si un accident hors dimensionnement survient.

3.2

PI

procédures informatisées

application informatique interactive utilisée pour présenter à l'opérateur de conduite des recommandations relevant des procédures et qui peuvent en plus contenir de l'information procédé évoluant, ceci couvrant en particulier l'accès aux commandes opérateur

Note 1 à l'article: Contrairement aux procédures papier qui sont des documents statiques, les PI offrent la possibilité de lire des informations évoluant. Cette possibilité permet à l'opérateur de naviguer d'une étape à une autre par différents moyens avancés, placer des marques page et utiliser des affichages en parallèle.

3.3

système PI

système numérique support des PI

Note 1 à l'article: Les PI peuvent être mises en œuvre dans l'IHM en même temps que d'autres fonctions de commande de la centrale ou elles peuvent être mises en œuvre seules sur un calculateur PI dédié.

3.4

SANC

système d'affichage numérique de conduite

système numérique élaborant des images (affichages d'images) dédiées à la surveillance de l'installation et sa conduite (par exemple diagrammes fluides), de façon à les afficher sur les unités de visualisation

3.5

image (affichage d'image)

représentation graphique d'informations affichées sur écran de visualisation telle qu'un texte de message, une représentation numérique, des symboles, des synoptiques, des bargraphes, des courbes, des curseurs, une présentation multi-angulaire

[SOURCE: IEC 60964:2009, 3.7]

3.6

démarche intellectuelle

démarche humaine de traitement et/ou d'interprétation d'une information visant à obtenir une information condensée et abstraite

[SOURCE: IEC 60964:2009, 3.12]

3.7

IHM

interface homme machine

interface entre l'équipe de conduite d'une part, les systèmes d'I&C et les calculateurs reliés à la centrale d'autre part. Elle inclut les afficheurs, les commandes et l'interface «système support de l'opérateur»

[SOURCE: IEC 60964:2009, 3.13]

3.8

navigation

fonction d'aide à l'opérateur lui permettant de localiser la position de l'information recherchée dans un système d'information intégrant des unités de visualisation et qui permet aussi de s'orienter pour la sélection des affichages

[SOURCE: IEC 62241:2004, 3.29]

3.9

PC

procédures de conduite

ensemble de documents spécifiant les tâches de conduite qu'il est nécessaire de remplir pour atteindre les objectifs fonctionnels

[SOURCE: IEC 60964:2009, 3.19]

3.10

stratégie de conduite

approche formalisée définissant les grandes lignes, par exemple la dépressurisation ou le refroidissement des boucles primaires, pour garder l'installation ou la ramener en état sûr et dont l'objectif est de servir de lignes directrices lors de l'élaboration des procédures de conduite

3.11

procédures papier

PC (voir 3.9) qui sont imprimées sur feuille papier

3.12

EIP

événement initiateur postulé

événement dont on détermine au stade de la conception qu'il peut entraîner des incidents de fonctionnement prévus ou des conditions accidentelles

[SOURCE: Glossaire de sûreté de l'AIEA, 2007]

3.13

séquence

séquence de procédure

ensemble d'étapes élémentaires d'une procédure qui est à exécuter complètement pour atteindre un objectif fonctionnel

Note 1 à l'article: L'exécution partielle d'une séquence peut entraîner un dysfonctionnement ou une défaillance de circuits ou de matériels ou mettre en péril l'exécution d'une fonction.

Note 2 à l'article: Généralement, une procédure comprend plusieurs séquences qui permettent d'atteindre un objectif fonctionnel global.

Note 3 à l'article: Une séquence peut correspondre à une seule étape.

3.14

étape

simple vérification de paramètres, simple action sur un élément de l'installation, ou simple décision ou passage de message oral entre opérateurs à réaliser et qui est demandé par une procédure

3.15

SdCS

salle de commande supplémentaire

emplacement à partir duquel la commande limitée de la centrale et/ou sa surveillance peuvent être assurées pour réaliser les fonctions de sûreté identifiées dans l'analyse de sûreté, comme prescrit en cas de perte de la possibilité de réaliser ces fonctions à partir de la salle de commande principale

Note 1 à l'article: Pour les installations existantes, la salle de commande supplémentaire peut être une salle de commande particulière, mais dans la plus part des cas celle-ci correspond à un ensemble de panneaux de commande et d'affichage dans des locaux électriques ou dans des zones similaires. Dans ce dernier cas, le terme «point de commande supplémentaire» est utilisé.

[SOURCE: IEC 60965:2016, 3.6]

3.16

VDU

unité de visualisation

type d'affichage incorporant un écran pour présenter des images pilotées par ordinateur

Note 1 à l'article: L'abréviation VDU est dérivée du terme anglais développé correspondant "visual display unit".

[SOURCE: IEC 60964:2009, 3.31]

4 Termes abrégés

PI	procédures informatisées
SANC	système d'affichage numérique de conduite
HFE	ergonomie
IHM	interface homme machine
ACVC	air conditionné, ventilation et chauffage
AIEA	Agence internationale de l'énergie atomique
I&C	instrumentation et contrôle-commande
SdC	salle de commande principale
CNP	centrale nucléaire de puissance
PC	procédures de conduite
EIP	événement initiateur postulé
SdCS	salle de commande supplémentaire
VDU	unité de visualisation
V&V	vérification et validation

5 Politique associée aux PI et exigences conceptuelles

5.1 Généralités

L'Article 5 donne des recommandations pour définir:

- une politique claire portant sur le domaine des procédures, le niveau de recommandation et le contrôle direct possible sur le procédé, par exemple, en prenant en compte l'expérience opérationnelle et les possibilités humaines aussi bien que les problèmes technologiques et organisationnels,
- les types de famille de PI,
- les caractéristiques clef des PI,
- la documentation à produire.

5.2 Politique d'informatisation

5.2.1 Généralités

L'élaboration d'une politique doit faire partie de la spécification du concept de la salle de commande, de l'architecture d'ensemble de l'I&C, de la définition de la politique ergonomique et des principes de conduite de l'exploitant (voir l'IEC 60964:2009, Article 5).

Il convient qu'elle repose sur l'analyse du retour d'expérience, des études conceptuelles, si possible de certaines activités de prototypage et qu'elle soit réalisée ou en entrée de conception avant le début de celle-ci, ou comme une des premières phases de la conception.

Le concepteur doit décider du type des procédures qui sont objet de l'informatisation et de l'étendue de l'informatisation.

Les raisons sous jacentes à l'informatisation des procédures doivent être déclarées dans un plan de gouvernance du projet du fait de leur influence importante pour déterminer l'ensemble des procédures à informatiser et le niveau d'informatisation. La décision de mettre en œuvre des PI ne résout pas nécessairement les problèmes liés aux stratégies de conduite ou les problèmes de personnel. Par contre, les études menées au niveau de la conception des PI peuvent permettre de clarifier la nature de ces problèmes et aider pour identifier les façons permettant de résoudre précocement au niveau du processus de conception les problèmes.

NOTE Les conséquences possibles sur l'organisation du personnel de conduite, le plan de la SdC, les stratégies de conduite, le domaine des procédures, la conception et le développement de l'automatisation, etc., sont hors du domaine de la présente norme.

Les types de procédures qui peuvent être informatisées comprennent:

- les procédures d'orientation liées à l'exploitation courante de l'installation en conditions normales, par exemple démarrage de l'installation, ou procédures d'orientation liées aux tâches élémentaires, lignage des circuits pour le chauffage, ou réduction de charge et remontée en puissance,
- les procédures de conduite accidentelles,
- les procédures de réponse aux alarmes,
- les procédures incendie,
- les procédures liées aux pertes sources et toutes autres procédures liées à des conditions inhabituelles,
- les procédures d'essais périodiques conçues conformément à l'IEC 60671, par exemple cartes de flux ou les étalonnages liés aux arrêts rapides du réacteur.

D'autres documents peuvent être aussi informatisés:

- les spécifications techniques,
- les schémas techniques matériel, facilitant, à partir d'écrans associés au SANC, l'accès à des données particulières concernant des équipements.

5.2.2 Règles sous-jacentes à la mise en œuvre des PI

En plus des recommandations liées à l'analyse des tâches, l'analyse fonctionnelle et à l'affectation ainsi que celles liées à la conception ergonomique qui sont couvertes par d'autres normes IEC dont la liste est fournie par l'Article 2, les aspects techniques suivants doivent être pris en considération au niveau de la planification du projet et dès les premières étapes de conception. Ces points sont les suivants:

- a) le cadre réglementaire national,
- b) la stratégie de conduite:

cette question fonctionnelle doit être considérée indépendamment de l'informatisation, par exemple si un choix doit être fait entre les approches par état ou événementielle pour conduire en cas d'accident,
- c) l'organisation de l'équipe de conduite:

lors de la construction d'une nouvelle tranche ou de la rénovation d'une centrale préexistante, la conception des PI peut faire partie de la conception des salles de commande ou de la reprise de conception de celles-ci. Ceci rend nécessaire l'utilisation de méthodes ergonomiques reconnues,
- d) le retour d'expérience de l'équipe de conduite:
 - 1) les leçons tirées au niveau des solutions papier ou à base de PI et qu'il convient d'identifier;
 - 2) de plus, le concepteur peut considérer que seule la stratégie de conduite doit être informatisée ou bien qu'au contraire seules les procédures de détail doivent être l'objet de l'informatisation,
- e) la formation des opérateurs,
- f) les données liées à l'instrumentation de la centrale,

NOTE 1 Le niveau des recommandations des PI dépend de l'instrumentation disponible.

- g) il convient que les avantages et les inconvénients liés au traitement des PI et des autres fonctions dans le même système, soient soigneusement évalués par rapport à l'ergonomie, aux capacités du système numérique et à la disposition de la SdC. En particulier, l'indisponibilité simultanée des PI et des autres fonctions de conduite est à

prendre en compte. Conformément à l'IEC 61513, l'ensemble de l'architecture comprenant les systèmes PI, comme le système PI de façon individuelle, sont à prendre en compte.

NOTE 2 Le système PI peut avoir des interfaces avec de nombreux autres systèmes, aussi la prise en compte des modes de défaillance et des réponses opérateur peuvent être importante.

Il convient qu'une politique préliminaire concernant les PI et les types de procédures qui pourraient faire l'objet d'une informatisation soit définie à partir de ces considérations.

5.2.3 Domaine des PI

On doit d'abord utiliser l'IEC 61839 pour identifier les fonctions à affecter aux opérateurs humains.

Il convient de prendre en compte l'IEC 61772:2009, Articles 4 et 5, ainsi que de répondre aux questions suivantes au niveau de la conception pour prendre les décisions finales portant sur le type de procédures à informatiser et sur le degré ou la forme d'informatisation (c'est-à-dire en faisant référence aux familles PI, voir 5.3):

- identification du type des procédures qui peuvent être utilisées en parallèle (c'est-à-dire par plusieurs opérateurs) en exploitation normale, en cas d'incendie, en cas de perte des sources électriques, en cas d'essais périodiques, en cas d'EIP,
- importance vis-à-vis de la sûreté des recommandations fournies par les PI à l'opérateur et des limites du temps de réponse opérateur supposées ou requises,
- évaluation du nombre d'images et de VDU nécessaire au déroulement de ces procédures,
- évaluation du nombre maximum de procédures qui peuvent être déroulées en parallèle par un opérateur unique ou par une équipe de conduite au complet dans le cas de la survenance de la pire des combinaisons d'événements de dimensionnement,
- évaluation du nombre maximum de fenêtres qui peuvent être affichées en parallèle dans le pire des cas sur une seule station de travail ou sur l'ensemble des stations de l'équipe de conduite,
- répartition des tâches de l'équipe de conduite au niveau des PI et des procédures papier de façon cohérente (par exemple pour éviter les erreurs opérateur).

Il convient de faire les évaluations précédentes en prenant en compte les concepts liés à la SdC. Les éléments suivants sont à considérer:

- a) l'ensemble des stations de travail et des postes de travail à partir desquels on peut utiliser les PI, dans la SdC et dans tous les autres points de commande,
- b) le fait qu'une procédure peut temporairement faire l'objet d'un abandon sans avoir été terminée, par exemple en cas d'apparition d'alarme,
- c) le volume maximum d'information qui peut être affiché sur une image,
- d) les performances du système PI, en particulier en ce qui concerne l'affichage, les capacités mémoire, la navigation,
- e) les marges supplémentaires appropriées pour faciliter de futures modifications.

De plus, il convient de prendre en compte précocement dans le processus de conception, la classe de sûreté à laquelle pourra être attribuée le système PI (pour cela voir l'IEC 61513), dès que les décisions relatives à l'allocation fonctionnelle sont prises. La classe de sûreté atteignable par le système PI sera souvent déterminée au regard de la faisabilité de la qualification des divers éléments de l'architecture d'ensemble dans laquelle le système PI est mis en œuvre. Ces éléments sont généralement: le système PI lui-même, le SANC et les systèmes de commandes qui servent d'interfaces entre les PI et l'installation, ainsi que les réseaux sous jacents supports des communications entre ces éléments, et enfin la conception des PI elles mêmes.

Certaines réponses à ces questions peuvent mettre en doute certains aspects de la mise en œuvre de la politique relative aux PI ou de la conception proposée pour le système PI, de ses

capacités, de son fonctionnement ou de l'indicateur coût-bénéfice associé, aussi bien qu'au niveau de l'organisation de l'équipe de conduite ou qu'au niveau des stratégies de conduite.

Il convient de définir la portée et le domaine des activités d'ergonomie ainsi que ceux des études portant sur l'organisation, tout en prenant en compte en même temps:

- 1) l'identification des ressources humaines nécessaires au projet, c'est-à-dire les spécialistes à intégrer à l'équipe projet, les spécialistes pour la vérification et la validation, l'organisation de la maintenance des PI,
- 2) l'utilisation du produit final, y compris les dispositions relatives à la maintenance.

Les normes IEC 60964, IEC 61772, IEC 61839, IEC 62241, l'ISO 11064 et en particulier l'ISO 11064-1, l'ISO 11064-3, l'ISO 11064-4 et l'ISO 11064-5, peuvent être utilisées pour prendre des décisions. L'IEC 60965 peut être utilisée si certaines PI sont à mettre en œuvre dans la salle de commande supplémentaire.

5.3 Les familles de PI

Bien que les PI puissent être informatisées de différentes façons suivant la politique de conception retenue, il convient de choisir une des trois familles génériques pour la mise en œuvre, telles qu'indiquées dans le Tableau 1. Ces trois familles sont définies en considérant:

- le niveau prévu de recommandation à l'opérateur,
- les entrées/sorties procédé requises.

Tableau 1 – Familles de PI

Détermination de la famille de PI		Niveau d'assistance opérateur		
		Pas de suivi des étapes/déroulement manuel	Suivi automatique des étapes	Capacité de recommandation
Type d'interfaces de données avec les PI	Pas d'entrée d'information procédé	1	<i>Impossible</i>	<i>Impossible</i>
	Entrées manuelles d'information procédé	1	<i>Impossible</i>	2 ou 3
	Entrées automatiques d'information procédé	2	2	2 ou 3
	Action sur le procédé	3	3	3

Les lignes correspondent à différents niveaux de connectivité du système PI, de l'absence d'information procédé à l'action sur le procédé. Les colonnes représentent les différents niveaux d'informatisation et d'intelligence associés. Pour le niveau le plus élevé de recommandation pour l'opérateur, le système est capable de fournir une aide à la décision pour l'opérateur; cette fonctionnalité est appelée recommandation pour la conduite (voir 8.5). Les intersections des lignes et des colonnes indiquent les possibilités pour les PI.

Ces trois familles de PI présentent les caractéristiques suivantes:

- Famille 1: les PI qui sont essentiellement de simples substitutions à l'identique des procédures papier, et correspondent à des pages d'information et d'instructions d'exploitation. L'opérateur peut avoir la possibilité d'entrer certaines données manuellement pour faciliter la compréhension de la procédure.

Les PI de cette famille ne reçoivent aucune information automatiquement de la part du procédé et ne comportent aucune fonctionnalité de commande du procédé.

- Famille 2: les PI qui peuvent fournir des recommandations à l'opérateur à partir de l'information acquise par le système PI. Chaque élément d'information peut être intégré aux images affichées. Si des recommandations de type avancé sont fournies, par exemple sous la forme d'assistance à la décision (voir 8.5.4), alors il convient que les PI appartiennent à la Famille 3.
- Famille 3: les PI qui présentent l'information et les instructions d'exploitation en ayant pour cela intégré complètement l'information en ligne relative à la centrale, à son état et les valeurs associées, pour qu'un actionneur de tranche puisse être commandé par un opérateur à partir des images PI, que l'accès à partir d'images PI aux fonctions de commande automatique soit possible et que l'exécution automatique de séquence puisse être lancée par l'opérateur à partir des images des PI.

L'affectation des PI aux familles et les arguments associés doivent apparaître dans la documentation.

Toutes les familles peuvent intégrer certaines des fonctionnalités présentées en 8.7.

NOTE 1 Les entrées manuelles correspondent à un volume d'information limité, dans le cas contraire la tâche de renseignement de ces entrées serait trop exigeante pour l'opérateur.

Différentes familles de PI peuvent être choisies pour chaque type de procédure dont la liste est fournie en 5.2.1, tant qu'une approche d'ingénierie simple et claire peut être maintenue.

Le choix du type de famille PI, la conception des PI et l'architecture d'ensemble dans laquelle les PI seront mises en œuvre auront un impact sur la façon d'affecter chaque fonction PI (ou de les répartir) entre les opérateurs humains, les autres IHM câblés ou numériques de la SdC, le système PI et les autres différents éléments de l'architecture d'ensemble. La répartition fonctionnelle détermine la confiance de sûreté (c'est-à-dire la dépendance par rapport à la sûreté, y compris les exigences requises portant sur un comportement sûr en cas de défaillance ou un comportement approprié à la défaillance détectée) que l'on aura dans le système PI et les différents éléments de l'architecture d'ensemble qui mettent en œuvre ou contribuent à chacune des différentes fonctions PI. Ainsi la classe requise pour le système qui en résultera sera le résultat direct de la conception PI, y compris du type de famille PI, et de la répartition fonctionnelle dans l'architecture d'ensemble des PI.

NOTE 2 En fonction de l'architecture d'I&C de l'installation, et en particulier pour les rénovations, il peut ne pas être possible de mettre en œuvre des systèmes de PI de famille 2 et de famille 3.

5.4 Vue d'ensemble des caractéristiques de l'informatisation

5.4.1 Généralités

L'informatisation repose sur des exigences et des règles génériques et sur la base d'éléments relatifs aux recommandations utilisateur et à la conduite de la centrale.

5.4.2 Exigences d'ensemble portant sur l'informatisation

Pour toutes les familles de procédures:

- il convient que les PI offrent les fonctionnalités permettant d'afficher l'information associée à l'objectif global de la procédure ainsi que la vue d'ensemble de ses séquences, de façon permanente ou sur demande de l'opérateur. Sur demande de l'opérateur, il convient que les informations complémentaires nécessaires au déroulement des étapes ou des séquences, telles que les actions préliminaires, les informations relatives au procédé ou aux matériels, soient affichables par les PI,
- le concepteur doit vérifier que l'ensemble des procédures et les exigences associées portant sur les capacités de traitement sont cohérentes avec les capacités du système PI.

Concernant la Famille 1 de PI, il convient que la procédure d'informatisation:

- a) soit intuitive et aussi simple que possible,

- b) donne une vue claire de l'objectif fonctionnel poursuivi,
- c) garantisse que l'opérateur comprend facilement la stratégie de conduite,
- d) garantisse que le contexte lié à la séquence de la PI ne soit pas perdu de vue par l'opérateur,
- e) laisse à l'opérateur la pleine responsabilité de la conduite,
- f) facilite la progression au sein de la procédure et limite les appels entre les procédures,

Concernant les familles 2 et 3 de PI, il convient que la procédure d'informatisation:

- 1) respecte les recommandations formulées pour la Famille 1,
- 2) permette à l'opérateur d'ignorer des instructions et des séquences, si elles ne sont pas pertinentes pour atteindre l'objectif de haut niveau de la procédure,
- 3) offre des possibilités appropriées de vérification (si possible automatiques) et de verrouillage de sûreté sur le statut des équipements et de l'installation pour garantir que les séquences nécessaires sont autorisées et qu'à l'instant où elles se déroulent cela se fait en toute sûreté ou bien dans le cas contraire qu'elles en informent l'opérateur,
- 4) évite que le système PI puisse mettre en œuvre des actions ayant priorité sur la sûreté (c'est-à-dire qu'il convient qu'elles ne soient pas autorisées),
- 5) demande des confirmations appropriées à l'opérateur avant l'exécution de séquences automatiques,
- 6) fournisse une information et des images appropriées et cohérentes aux membres de l'équipe de conduite, qui peuvent avoir accès à des affichages PI indépendants, et garantisse que toutes les incohérences qui pourraient apparaître sur des affichages PI indépendants du fait de fautes internes au système PI sont détectées et clairement indiquées à l'opérateur,
- 7) garantisse que les procédures d'un même type sont appliquées de la même façon, par exemple pour toutes les procédures accidentelles ou pour toutes les procédures incendie,
- 8) garantisse la cohérence pour les différents types de procédures qui peuvent être déroulées en parallèle.

5.4.3 Mesures de recommandation à l'opérateur

Il convient que les recommandations produites par les PI rappellent à l'opérateur les objectifs fonctionnels et l'information détaillée spécifiques à la séquence d'étapes de la procédure d'exploitation ainsi que les informations et les recommandations relatives aux moyens nécessaires pour atteindre chaque étape et les objectifs d'ensemble.

En plus de fournir à l'opérateur l'information procédé élémentaire, l'accès aux PI peut lui proposer de l'information procédé élaborée, de l'aide au diagnostic ou lui suggérer des décisions à prendre.

L'aide au diagnostic ou la suggestion de décision peut être:

- automatisée: un diagnostic ou une décision est suggéré à l'opérateur qui peut alors demander des informations détaillées sur le sujet,
- guidée: les PI affichent des schémas qui aident l'opérateur à établir un diagnostic ou une proposition de décision. La recherche des informations nécessaires à l'opérateur pour réaliser les choix élémentaires est facilitée ou fait partie des schémas pour que l'opérateur puisse valider successivement chaque étape.

Il convient pour concevoir les PI de prendre en compte:

- a) les états de tranche pour lesquels l'utilisation des PI sera nécessaire,
- b) la fréquence des événements ou des situations, par exemple il convient de fournir des recommandations élaborées plutôt pour des événements rares que pour l'exploitation journalière,

- c) la politique de conduite, par exemple un objectif d'exploitation ambitieux en termes de disponibilité peut entraîner un surcroît d'informatisation ou d'automatisation,
- d) si, lorsque des actions opérateur sont nécessaires elles le sont dans un délai imparti (c'est-à-dire prise en compte requise par l'opérateur d'alarmes ou de notifications, ou action(s) conservative(s) au niveau sûreté nécessaire(s) en cas de défaillance de l'opérateur à agir),
- e) les exigences et le retour d'expérience de l'équipe de conduite.

Le concepteur doit prendre en compte les possibilités inhérentes offertes par le système PI, par exemple ses performances, sa facilité d'utilisation, pour définir les recommandations.

La possibilité pour l'opérateur de demander des informations élémentaires peut être suivie d'un calcul permettant d'obtenir de l'information résumée de haut niveau.

Les PI fournissent à l'opérateur de l'information synthétisée et peuvent aussi lui assurer une certaine aide, voir 8.7.

5.4.4 Mesures relatives aux procédures automatisées

Les PI peuvent assister l'opérateur dans la conduite de l'installation à partir:

- de messages d'avertissement automatiques lorsque certaines conditions prédéfinies sont satisfaites,
- de l'exécution automatique des séquences qui ont été lancées par un opérateur.

Comme pour les procédures papier, il convient de définir les PI en prenant en compte:

- la répartition des fonctions entre l'opérateur et le système PI, le système d'automatisation de l'installation ou le SANC,
- le fait que l'ensemble des procédures du système de secours est indépendant du SANC et du système PI,
- la facilité de compréhension pour l'opérateur, en particulier en conditions anormales.

Les considérations supplémentaires à prendre en compte sont:

- a) il convient, sauf pour la conception des moyens de secours, d'éviter la duplication des fonctions entre l'opérateur et le système et les conceptions doivent avoir pour objectif la recherche de complémentarité fonctionnelle de l'opérateur et du système PI,
- b) les images PI peuvent comprendre la possibilité de passer des commandes ou peuvent permettre de lancer des actions opérateur pour contrôler des images du SANC. Une autre option consiste à autoriser les commandes des PI en les validant à partir du SANC.

On doit améliorer le niveau d'attention des opérateurs en:

- 1) affichant l'information pertinente pour que l'opérateur soit toujours informé des changements d'état de tranche:

il convient de ne pas automatiser la prise des décisions importantes; il convient que les fins de séquences automatiques soient signalées; il convient que tous les problèmes survenant durant une séquence automatique soient signalés ainsi que toute valeur du procédé atteignant un seuil prédéfini,

- 2) lui fournissant l'option de reprendre à tout instant le contrôle sur les PI,

NOTE Certaines situations peuvent exiger que l'action relative à une PI soit terminée, alors que d'autres peuvent amener l'opérateur à reprendre les commandes pour un nombre limité d'étapes.

- 3) prenant en compte la coordination de l'équipe de conduite:

les séquences lancées par deux opérateurs peuvent être désynchronisées et ne doivent pas avoir pour conséquence l'exécution d'actions concurrentes ou contradictoires.

5.5 Documentation produite

Les hypothèses et les raisons sous jacentes à la prise de décision de mettre en œuvre des PI (comme définies de 5.1 à 5.4 ci-dessus) doivent être documentées de façon précoce au niveau du projet et doivent couvrir les points suivants:

- la politique, les exigences conceptuelles, et la philosophie sur lesquelles repose la mise en œuvre des PI,
- le type des PI, leurs objectifs et leurs domaines,
- l'approche de la mise en œuvre des PI et les hypothèses faites, y compris par rapport à la prise en compte du SANC,
- les options retenues concernant les recommandations des PI, y compris la description des données d'entrée de conception et autres informations requise,
- les options retenues pour les procédures automatisées,
- la politique retenue par l'exploitant pour la formation des opérateurs.

5.6 Conditions hors dimensionnement

En cas d'apparition de conditions hors dimensionnement, il ne faut pas faire l'hypothèse que le système PI soit disponible (voir NOTE). Un ensemble de procédures papier conçu pour faire face à un tel contexte doit être disponible pour conduire l'installation à partir de la SdC, c'est-à-dire qu'il convient que les PI ne soient pas conçues pour la conduite dans de telles situations.

NOTE N'étant pas conçu pour faire face aux conditions hors dimensionnement, on fait l'hypothèse que le système PI peut devenir indisponible ou non fiable n'importe quand.

La mise à jour des ensembles de PI et de procédures papier doit être coordonnée et mis en cohérence avec l'ensemble des procédures de secours.

L'équipe de conduite doit être formée à utiliser ces ensembles de procédures et des exercices doivent être réalisés périodiquement.

6 Contextes d'utilisation des PI

6.1 Généralités

L'Article 6 fournit des exigences applicables pour différents contextes d'utilisation des PI. Il prend en compte différents environnements d'utilisation par rapport à la SdC et avec l'utilisation possible en parallèle de procédures papier. Il considère ensuite les exigences portant sur les différentes formes d'activités d'aide à l'opérateur, et la coordination des utilisateurs. Enfin il traite des aspects relatifs à la documentation attendue.

6.2 Environnements d'application pour l'utilisation des PI

6.2.1 Généralités

Le paragraphe 6.2 prend en compte les différents environnements dans lesquels les PI peuvent être utilisées, que ce soit dans une SdC informatisée neuve, ou dans des SdC conventionnelles ayant fait l'objet d'une modernisation partielle, conjointement avec les procédures papier ou localement par les rondiers.

L'intégration d'ensemble des PI dans la SdC et dans les autres points de commande doit être faite conformément aux exigences de l'IEC 60964, l'IEC 60965 et l'IEC 61513. L'utilisation des unités de visualisation doit être conforme à l'IEC 61772. Les fonctionnalités et la présentation des alarmes doivent être conformes à l'IEC 62241. Le logiciel doit être conforme à l'IEC 60880 ou à l'IEC 62138 suivant la catégorie de sûreté.

6.2.2 Utilisation des PI dans les SdC informatisées

Il doit être possible de commander séparément les affichages d'images du système PI et les autres affichages d'images du système du SANC.

Il convient d'assurer la compatibilité entre les images des PI et les images de conduite du SANC en:

- assurant la compatibilité à la conception des présentations d'IHM et des détails des images, c'est-à-dire au niveau des abréviations, des symboles, des couleurs, etc.
- évitant que surviennent des discordances lorsque les images des PI et celles du système d'IHM pointent sur le même objet, circuit ou matériel,
- mettant à jour les images du SANC et des images PI sans désynchronisation temporelle notable lorsqu'elles sont affichées simultanément.

6.2.3 Utilisation des PI dans une SdC conventionnelle ou hybride

Une SdC conventionnelle est une salle conçue sans intégrer d'équipement numérique. Une SdC hybride est une salle qui intègre des appareils numériques pour surveiller ou commander certaines parties de la centrale, mais pas toute l'installation. Les SdC conventionnelles peuvent lors de modernisation devenir des SdC hybrides. L'étendue de l'informatisation des SdC hybrides, qui exclut l'ensemble de l'installation, peut beaucoup varier suivant les objectifs de l'exploitant.

Lors de la mise en œuvre des PI dans une SdC conventionnelle ou dans une SdC hybride, on doit prendre en compte les contraintes liées à la SdC existante, à savoir l'espace libre et la zone de travail opérateur, en plus de celles dont la liste est fournie en 5.2.3. L'introduction d'appareil d'affichage pour les PI dans une SdC conventionnelle peut entraîner le déplacement de certains équipements existants, indicateurs, boutons-poussoirs, etc. de façon à libérer de la place pour installer les ensembles d'unités de visualisation et les équipements associés, tels que les claviers, les pavés sensibles, les boules roulantes, etc.

NOTE Les moyens, tels que ceux de chauffage, ventilation, conditionnement de l'air sont pris en compte.

Pour les SdC conventionnelles ou hybrides, il convient que le défi particulier représenté par l'utilisation simultanée des PI avec des appareils discrets tels que: indicateurs, boutons-poussoirs, dispositifs de commande auto-manu, etc. soit étudié. De plus, on doit s'attendre à avoir une utilisation simultanée des PI et des procédures papier et ceci doit être analysé.

Prenant en compte le fait que l'informatisation des commandes de l'installation est limitée, il convient que les PI soient conçues pour fournir de l'information et des recommandations, par exemple il convient que celles ci appartiennent à la Famille 1 ou à la Famille 2, et il convient qu'elles satisfassent aux exigences associées à ces familles.

De plus, il convient que des mesures particulières soient mises en place pour:

- la conception de l'IHM des PI, pour que l'affichage d'informations sur les unités de visualisation en présence d'autres images affichées ne sème pas la confusion dans l'esprit des opérateurs, et ceci en particulier en conditions accidentelles. S'il n'y a pas d'autres images numériques, l'ISO 11064-1, l'ISO 11064-3, l'ISO 11064-4 et l'ISO 11064-5 et l'IEC 61772:2009 en particulier l'Article 4, doivent être utilisées pour définir toutes les images nécessaires,
- permettre aux opérateurs de lire les PI à partir de leurs zones de travail, qu'ils soient en face des unités de visualisation ou à une certaine distance de celles-ci.

6.2.4 Utilisation des PI en parallèle des procédures papier

Les PI peuvent être utilisées en même temps que des procédures papier, pour des raisons liées à la conception, ou pour des raisons temporaires liées aux options retenues conformément aux recommandations de 5.2.3.

EXEMPLE 1 Les procédures détaillées de conduite peuvent rester sur la base de procédures papier alors que la stratégie de conduite est informatisée.

EXEMPLE 2 Des ensembles particuliers de procédures papier peuvent être utilisés pendant les arrêts de tranche. Ils peuvent être aussi utilisés lorsqu'une erreur a été détectée dans les PI, et les procédures papier sont utilisées en attente de la mise en service de la nouvelle version corrigée des PI.

De telles situation doivent être conçues de telles façon que:

- il n'y ait pas de lacunes entre les PI et les procédures papier,
- les chevauchements entre les PI et les procédures papier soient fonctionnellement justifiés,
- les références et le nommage des PI et des procédures papier sont consistants et ne provoquent pas d'erreur humaine,
- le passage des PI aux procédures papier est clair,
- la possibilité de tracer les actions faites pour les PI et les procédures papier est garantie,
- la transmissions des explications nécessaires reste facile durant le passage de quart.

6.2.5 Utilisation des PI hors de la SdC

Lorsque certaines salles de commande locales, par exemple la SdC, sont informatisées et quelles sont utilisées avec les PI, alors celles-ci doivent être adaptées aux tâches opérateurs à réaliser.

La conduite à partir des points de commande locaux, s'ils sont informatisés, ou à partir de n'importe quel type de terminal portable, doit satisfaire aux exigences de 6.4.

6.3 Formes d'assistance fournies par les PI pour les activités des opérateurs

6.3.1 Généralités

Les PI doivent être conçues pour permettre aux opérateurs de faire face à différentes conditions, en prenant en compte l'état réel de la centrale, en surveillant le procédé et en détectant les événements qui surviennent.

Les procédures sont conçues pour aider l'opérateur en lui suggérant la stratégie de conduite à suivre et en préparant les actions qu'il est possible de lancer par rapport à l'état de la centrale. Néanmoins, des situations imprévues pourraient survenir, pour lesquelles l'opérateur est en capacité d'atteindre un objectif ambitieux défini par une procédure même si certaines parties de celle-ci ne sont plus pertinentes.

Pour les besoins de la présente norme, les fonctions fournies par les PI sont réparties entre les activités principales de l'opérateur (par exemple la mise à disposition de l'opérateur d'informations), et les activités secondaires (par exemple la gestion des fenêtres et la navigation dans l'information nécessaire).

6.3.2 Aide aux activités principales de l'opérateur

Les concepts suivants doivent être pris en compte lors de la conception avec une justification documentée des décisions de conception prises par rapport à chacun des thèmes suivants:

- la compatibilité avec les représentations intellectuelles de l'opérateur
les aspects IHM sont compatibles avec les traitements mentaux de l'opérateur, c'est à dire avec la compréhension de l'opérateur, son expérience, ses attentes par rapport à l'état de la centrale et son évolution et par rapport au comportement des PI
- la représentation de la situation
l'information affichée est facile à identifier et à comprendre, la précision des valeurs affichées est consistante avec celle des valeurs mesurées, dans le but de faciliter les

traitements et le cheminement intellectuels de l'opérateur vers l'objectif fonctionnel de la procédure. Il convient d'afficher un indicateur de validité des données

- la structure de l'IHM

les aspects liés à l'IHM reposent sur des règles logiques et consistantes. Les principaux aspects liés à l'IHM sont la présentation de l'information, la hiérarchie des séquences au sein d'une procédure, la terminologie, l'aide à la phraséologie, la structuration des listes etc.

- l'adéquation de l'information avec l'activité principale

l'information affichée est pertinente par rapport à la situation de la centrale

- les capacités de l'opérateur

le volume d'information affichée permet à l'opérateur de la comprendre et le temps nécessaire lui est donné pour qu'il puisse prendre une bonne décision

Les informations contextuelles peuvent être affichées pour souligner la pertinence de l'information et pour aider l'opérateur à comprendre.

6.3.3 Aide aux activités secondaires de l'opérateur

Afin de simplifier les tâches opérateur et lui permettre de se concentrer sur les tâches principales, les aspects suivants doivent être pris en compte au niveau de la conception. Il convient de documenter les principales décisions de conception concernant ces aspects, y compris les justifications concernant:

- la charge mentale de l'opérateur

la mémorisation d'éléments, tels que les listes de codes, les codes de commande, les informations à mémoriser en passant d'une page à l'autre, est minimisée

- les actions opérateur

il est facile de réaliser une action et toute action redondante est à éviter

Il convient que les activités secondaires liées aux PI soient faciles à réaliser d'une manière fiable, pour que la réalisation des activités principales n'en souffre pas.

6.4 Assistance à la coordination des opérateurs

Il convient que les PI soient explicites pour ce qui concerne les communications par rapport aux séquences affectées aux membres individuels de l'équipe de conduite, par exemple la communication nécessaire du fait du partage des tâches entre opérateurs et superviseur. Une telle coordination peut être mise en œuvre à l'aide de points d'arrêt positionnés dans les procédures, demandant des échanges oraux ou des acquittements informatiques.

Par exemple, si le superviseur est le seul utilisateur des PI et qu'il coordonne ensuite les autres opérateurs, ou bien le superviseur et les opérateurs primaire et secondaire ont accès aux PI, alors la procédure doit indiquer quelle communication il est nécessaire d'établir entre eux.

Si plusieurs opérateurs peuvent accéder en même temps à la même PI, on doit mettre en place les règles pour contrôler les accès concurrents à une même procédure. Les points suivants doivent être couverts:

- identification de celui qui peut accéder à la procédure, par rapport au niveau d'autorisation,
- identification du type d'accès autorisé: lecture seule, ou utilisation complète,
- identification de la façon d'accéder à une PI par rapport aux PI en cours de déroulement,
- mesures mises en place pour empêcher un opérateur de répéter ou d'arrêter une action déjà lancée par un autre opérateur, en particulier lorsque la PI est conçue pour conduire

la centrale. Ceci peut être satisfait en se servant de sémaphores, qui garantissent qu'un seul opérateur à la fois peut utiliser une PI pour passer une commande sur la tranche, alors que tous les autres opérateurs n'ont que des accès en lecture pendant ce temps.

La réservation par les procédures nécessite qu'une politique soit définie pour cela, prenant en compte les demandes des autres procédures ou des autres sous procédures,

- fourniture des signaux d'utilisation des PI, c'est à dire des indicateurs prévenant qu'une PI est en cours d'exécution, ou des signaux indiquant lorsqu'une PI est réservée depuis trop longtemps sans être utilisée.

Toutes ou seulement certaines procédures particulières peuvent être affectées à des stations de travail particulières.

Les PI doivent permettre aux utilisateurs de se synchroniser en cas d'utilisation en parallèle de plusieurs PI dans la SdC et à partir d'autre points de commandes locaux. Il convient que les défaillances possibles affectant les communications numériques ne dégradent pas la fiabilité et la disponibilité des PI, ni en SdC, ni en des points de commandes locaux. Il convient que toute différence significative d'avancement pour des opérateurs appliquant la même PI soit signalée de façon à éviter l'apparition d'un processus de commande non coordonné.

6.5 Documentation produite

Il convient que toutes les options retenues pour satisfaire aux exigences fournies en 6.3 et 6.4 soient documentées dans des documents appropriés:

- une synthèse donnant les options retenues et les raisons sous jacentes concernant la conception, le développement, la validation ou les phases d'agrément réglementaires,
- une synthèse à destination des opérateurs. Il convient que ce soit un rappel, et qu'il soit facile à utiliser dans les situations de tranche anormales,
- une documentation détaillée servant de recommandation pour la conception et la maintenance des PI.

Cette documentation doit être mise à jour en même temps que les PI sont modifiées pour garantir cohérence et complétude.

7 Système PI et exigences fonctionnelles

7.1 Généralités

L'Article 7 couvre le traitement du système numérique PI, qu'il soit intégré dans le SANC de la centrale ou qu'il soit indépendant de celui-ci. Les exigences de sûreté et non liées à la sûreté sont prises en compte.

Il fournit des exigences concernant les cas de défaillances du système PI. Enfin il traite de la documentation à produire.

Quelle que soit la solution choisie les économiseurs d'écran ne doivent pas être utilisés.

7.2 Aspects de sûreté

Il est nécessaire de prendre en compte soigneusement le rôle de sûreté fondamental d'une PI, et si elle a un rôle de sûreté ou non, ou si elle fait partie de la stratégie de défense en profondeur de l'installation dans son ensemble. Le système PI ne doit pas pouvoir mettre en péril le principe de défense en profondeur de l'I&C de l'installation.

Les procédures, qu'elles soient papier ou informatisées et quel que soit leur niveau, sont conçues pour être utilisées par des opérateurs, et elles ne doivent pas commander au

procédé sans la participation de l'opérateur (c'est-à-dire lancement et surveillance par l'opérateur). L'opérateur est supposé agir de façon intelligente, ne pas appliquer les procédures automatiquement, et rester seul responsable de l'application pertinente des procédures.

Le classement de sûreté du système PI peut se faire en classe 1, 2 ou 3 ou peut ne pas être classé conformément à l'IEC 61513. La classe doit être déterminée en prenant en compte:

- a) la couverture fonctionnelle des PI;
- b) le type de famille PI;

NOTE 1 La liste des familles de PI est donnée en 5.3.

- c) les impacts possibles sur la sûreté:

- 1) de la perte des PI;
- 2) de recommandations erronées fournies à l'opérateur, ou de signaux de commande intempestifs,

EXEMPLE Les modes de défaillances acceptables et possibles de chaque PI, les impacts sur l'attention des opérateurs et leur aptitude à répondre aux événements survenant sur l'installation, la probabilité d'une erreur opérateur (par exemple due au temps disponible, à la complexité et à l'importance pour la sûreté de la décision à prendre etc.) et la disponibilité des moyens de secours pour récupérer d'une défaillance.

- d) l'affichage d'informations diversifiées qui serait mise à disposition de l'opérateur, permettant de confirmer l'information affichée par les PI. Il convient que l'opérateur soit formé pour réaliser de telles comparaisons (voir 9.9).

NOTE 2 Bien que l'IEC 61226:2009, 7.3.2.1 ouvre la possibilité de réaliser manuellement des fonctions de catégorie A en interfaçant le système PI avec un système de classe 1, l'attention des concepteurs est attirée sur le fait que cela nécessiterait une analyse significative venant en support de la démonstration de sûreté, en particulier pour ce qui concerne les aspects ergonomiques.

Les PI peuvent être mises en œuvre dans différents sous systèmes appartenant à des classes de sûreté différentes.

Les exigences et les recommandations fournies par l'IEC 61513, l'IEC 60880 et l'IEC 62138 doivent être satisfaites pour la conception et la mise en œuvre de l'architecture d'ensemble d'I&C comprenant le système PI, ainsi qu'au système PI lui-même. Le niveau de redondance du système PI doit être cohérent avec son niveau de classement de sûreté. Les exigences fournies par l'IEC 61772:2009, 4.3, doivent être satisfaites.

NOTE 3 La classe que le système pourra atteindre peut limiter l'approche de conception des PI en termes d'options de faisabilité, y compris au niveau du type de famille qui pourrait être mis en œuvre. Si la classe requise pour le système ne peut être atteinte et qualifiée, une approche alternative sera considérée. Ceci pourrait contribuer à exiger de changer le type de famille, l'approche de conception et les répartitions fonctionnelles. Il pourrait être aussi nécessaire de changer de choix de plateforme support des PI, de changer de mécanismes de communication, ou de modifier l'architecture d'ensemble. A défaut de prendre en compte ces questions de façon précoce au niveau du projet de mise en œuvre du système PI, on s'expose à des retards coûteux et à devoir reprendre la conception.

Dans le cas où le système PI ne serait pas classé de sûreté, il convient de définir sur la base des normes IEC citées dans l'alinéa précédent des exigences adaptées aux incidences opérationnelles qui pourraient être provoquées par le système.

Une vérification appropriée des séquences lancées par les PI doit être mise en œuvre au niveau des systèmes de conduite de l'installation. Ceci doit comprendre les verrouillages nécessaires pour assurer la sûreté.

Pendant les périodes de développement et de vérification, on doit faire particulièrement attention pour garantir que des défauts ou des défaillances potentiels ne puissent rendre non opérationnel le système PI, inhiber ou lancer des actions manuelles ou automatiques. Il convient de réaliser des investigations au niveau des conséquences fonctionnelles dues à des données erronées ou désynchronisées, reçues d'autres systèmes, en particulier des systèmes d'automatisation. Les études de sûreté doivent prendre en compte l'architecture d'ensemble d'I&C, comprenant le système PI, ainsi que le système PI de façon individuelle.

7.3 Considérations sur l'IHM

L'IEC 61772:2009, en particulier les Articles 4 et 5, ainsi que l'ISO 11064, en particulier l'ISO 11064-1, l'ISO 11064-3, l'ISO 11064-4 et l'ISO 11064-5 fournissent des recommandations pour l'IHM.

Pour ce qui concerne l'IHM des images des PI, seuls trois cas sont possibles:

- 1) un système numérique, le SANC, est déjà utilisé pour conduire l'installation au moment où les PI et le système PI sont conçus: l'IHM des deux systèmes doit être compatible,
- 2) un système numérique, le SANC, est défini en parallèle des PI et du système PI: l'IHM des deux systèmes doit être compatible. Il convient d'utiliser l'IEC 61772 et l'ISO 11064 pour définir les affichages d'images des deux systèmes,
- 3) il n'y a pas d'autre système numérique affichant des informations sur écran pour conduire l'installation. On doit utiliser l'IEC 61772 et l'ISO 11064 pour définir les affichages d'images du système PI.

7.4 Intégration du système PI dans le SANC

Pour intégrer le traitement associé aux PI dans le SANC, on doit vérifier que:

- la classe de sûreté du SANC est compatible avec la catégorie de sûreté des fonctions associées aux PI, conformément aux considérations de 7.2,
- les caractéristiques du SANC satisfont aux exigences de 5.2.3,
- pour les PI de la Famille 3 réalisant des fonctions de catégorie B, il convient que le système d'affichage de la tranche et les communications de et vers celle-ci, satisfassent aux exigences de l'IEC 61513 et de l'IEC 62138 pour la classe 2,
- les caractéristiques du SANC satisfont aux exigences de l'Article 8.

Les exigences et les recommandations de l'IEC 61772 doivent être appliquées.

7.5 Système PI mis en œuvre de façon externe au SANC

7.5.1 Généralités

Le paragraphe 7.5 complète les exigences de sûreté fournies en 7.2, et couvre les connexions existant entre le système PI et le SANC.

Pour les PI appartenant aux Familles 2 ou 3 qui sont interfacées avec l'installation au travers du SANC, il convient que la classe de sûreté du système PI et du SANC soit déterminée et qu'ils satisfassent aux exigences de sûreté associées à celle-ci, sinon des justifications appropriées sont à apporter.

Pour les PI appartenant à la Famille 3, il convient que la répartition des tâches entre le système PI et les systèmes de conduite de l'installation prennent en compte les points suivants:

- il convient que les lancements des séquences automatiques comme la mise en place de points d'arrêt des traitements en cours par l'opérateur puissent se faire au niveau des images numériques,
- il convient que les séquences automatiques lancées par les PI, qui potentiellement peuvent utiliser des données d'entrée provenant de l'installation et des acquittements relatifs aux actionneurs, soient traitées par les systèmes de conduite de l'installation.

7.5.2 Exigences de dimensionnement et de fiabilité

En sus des exigences de sûreté, des points supplémentaires doivent être pris en compte:

- le système PI doit être conforme aux exigences de 5.2.3,

- les exigences liées à fiabilité et à la disponibilité doivent être compatibles entre le système PI et le SANC,
- les autotests doivent être spécifiés,
- les capacités de réserve doivent être spécifiées pour que des extensions soient possibles, par exemple en termes de mémoire, de capacité de traitement des processeurs, de capacité de stockage de données, de capacités réseau, de nombre de connexions de stations de travail.

7.5.3 Connexions entre le système PI et le SANC

Les aspects architecture et système doivent être conformes à l'IEC 61513.

On doit mettre en œuvre des mesures pour éviter les discordances entre les commandes envoyées en même temps par le système PI et le SANC, ou au minimum, on doit signaler de telles discordances à l'opérateur.

Considérant que certaines variables provenant du procédé ou relatives aux matériels peuvent être utilisées à la fois par le système PI et le SANC pour réaliser différentes fonctions et potentiellement être affichées sur différentes images, alors:

- il convient que les deux systèmes soient analysés ensemble pour ce qui concerne les modes de défaillance, mais aussi pour les traitements de secours en cas de défaillance ou de réalisation d'essai périodiques;
- il convient que le système PI ne puisse pas être compromis par les défaillances possibles du SANC et vice-versa;
- il convient que les défaillances du système PI soient signalées au SANC et que les défaillances totales ou partielles du SANC soient signalées par une alarme indépendante;
- il convient que la défaillance de l'interface entre les deux systèmes soit signalée au moins sur un des deux systèmes;
- l'envoi de commandes des deux systèmes vers un même actionneur, simultanément ou séparées de quelques minutes, doit être signalé. Les ordres contradictoires doivent être signalés d'une façon explicite;
- il convient de mettre en place des mesures pour limiter les discordances temporelles lorsqu'on met à jour des parties dynamiques d'un même objet. Une valeur de discordance inférieure à 2 s est considérée comme acceptable, il convient que les valeurs plus grandes soient signalées.

7.5.4 Maintenance cohérentes des systèmes

On doit prendre en compte la maintenance des points de vue matériel, logiciel, configuration et application, pour l'ensemble des deux systèmes, y compris pour le processus de requalification.

7.6 Défaillances du système PI

Des considérations génériques concernant les défaillances des unités de visualisation sont fournies dans l'IEC 61772:2009, 4.3 et 4.4.

Les opérateurs doivent être formés pour qu'ils gardent un esprit critique par rapport au déroulement des PI. Afin de les aider, des mesures d'auto surveillance et des autotests doivent être mis en place au niveau du système PI pour détecter et signaler les dysfonctionnements. Prenant en compte les conséquences potentielles liées à de mauvaises orientations fournies aux opérateurs, il convient que le taux de l'auto surveillance soit aussi élevé que possible. Il convient de mettre en place lorsque c'est possible des mécanismes de position de sécurité sur défaillance appropriés pour les PI de la Famille 3. Pour améliorer le niveau de détection des dysfonctionnements des PI, une partie de l'équipe de conduite peut utiliser des procédures papier.

NOTE 1 Les principales méthodes courantes de détection des dysfonctionnements sont celles relatives à l'auto surveillance mises en œuvre conformément à l'IEC 60671, les mécanismes de surveillance indépendants et la surveillance périodique réalisée par le personnel.

Lorsqu'un opérateur suspecte un dysfonctionnement des PI qui n'aurait pas été détecté ou signalé par le système, par exemple la dérive d'un paramètre, le système PI, ses parties constitutives ou les sous systèmes d'I&C supports peuvent être considérés comme indisponibles.

En cas de dysfonctionnement d'une PI importante pour la sûreté ou de défaillance du système PI réalisant des fonctions liées à la sûreté (catégories B ou C), un moyen de secours diversifié et un ensemble de procédures adapté doivent être utilisés. Cet ensemble de procédures de secours doit être compatible avec le SANC, si ce dernier est encore disponible et utilisé pour conduire la tranche.

NOTE 2 L'étendue des moyens de secours et les procédures associées seront typiquement limitées à l'ensemble des fonctions nécessaires à la mise et au maintien de l'installation dans un état sûr, et à la réduction de l'impact sur le fonctionnement de l'installation tant que le système PI ou le SANC ne sera pas restauré.

Un ensemble de procédures diversifié conçu pour servir de secours au système PI (par exemple des procédures manuelles papier) doit prendre en compte le fait que cette situation est rare et stressante, et il doit avoir pour objectif d'éviter les erreurs opérateur ou les incompréhensions en:

- étant indépendant du système PI, des points de vue technique comme fonctionnel, c'est-à-dire sans référence à des informations uniquement présentes sur le système PI,
- étant basé sur des stratégies de conduite similaires à celle utilisées par le système PI,
- étant conçu pour la même équipe de conduite,
- utilisant autant que possible le même vocabulaire et les mêmes éléments graphiques, et des procédures d'affichage cohérentes avec celles des PI.

L'ensemble des procédures de secours, et tous les systèmes de secours associés, doivent être facilement accessibles.

Le système de secours et l'ensemble des procédures de secours, s'ils sont informatisés, doivent avoir été conçus, développés et validés conformément à leur classement de sûreté et ils doivent satisfaire aux exigences de l'Article 9.

NOTE 3 Le choix d'un deuxième ensemble de PI comme solution de secours est un gros pari, car cela implique que le système PI diversifié prenne en compte la détection des dysfonctionnements, une maintenance plus complexe et suppose une formation opérateur. C'est pour cette raison que les procédures papier sont souvent préférées. Pour prendre une telle décision les aspects économiques sont aussi à prendre en compte.

Si les PI sont mises en œuvre dans un système séparé de celui du SANC, les points suivants sont applicables:

- il convient que le SANC surveille le système PI et signale les défauts détectés à l'équipe de conduite,
- il convient que le SANC ne soit pas bloqué en cas de défaillance du système PI.

7.7 Documentation produite

Les exigences système et fonctionnelles et les options et décisions de conceptions relatives à l'architecture d'ensemble et à l'approche système PI doivent être documentées conformément aux exigences de l'IEC 61513 (et par rapport aux normes filles telles que l'IEC 62138) de façon cohérente par rapport la classe de sûreté du système.