IEC 62646

Edition 1.0 2012-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Control rooms – Computer based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées

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

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

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Customer Service Centre - webstore.iec.ch/csc

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

A propos de la CEI

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

A propos des publications CEI

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

Liens utiles:

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

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

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Service Clients - webstore.iec.ch/csc

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

IEC 62646

Edition 1.0 2012-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Control rooms – Computer based procedures

Centrales nucléaires de puissance – Salles de commande – Procédures informatisées

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

W

ICS 27.120.20

ISBN 978-2-83220-388-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – CONTROL ROOMS – COMPUTER BASED PROCEDURES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

c) Recommendations and limitations regarding the application of the Standard

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NUCLEAR POWER PLANTS – CONTROL ROOMS – COMPUTER BASED PROCEDURES

1 Scope

1.1 Object

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

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

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

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

1.2 CBP overview

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

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

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

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

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

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

---

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

- optional automatic plant control.

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

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

1.3 Exclusions from this standard

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

- functional analysis and assignment

  IEC 61839 specifies functional analysis and assignment procedures and gives rules for developing criteria for the assignment of functions either to operators or to systems,

- human factors design guidelines.

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

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

This standard also excludes:

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

1.4 Organisation of this standard

Clause 2 lists the reference documents.

Clause 3 gives definitions relevant to this standard.

Clause 4 lists the abbreviations used in this standard.

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

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

3.2
Computer Based Procedures
CBP
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: CBP may be implanted in the HMI system, together with other plant control functions, or may be implemented in a standalone CBP computer.

3.4
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]

3.5
high-level mental processing
human act to process and/or interpret information to obtain reduced abstract information

[SOURCE: IEC 60964:2009, 3.12]

3.6
Human Machine Interface
HMI
the interfaces 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]

3.7
navigation
a 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]

3.8
Operating Procedures
OP
a set of documents specifying operational tasks it is necessary to perform to achieve functional goals

[SOURCE: IEC 60964:2009, 3.19]

3.9
paper based procedures
OP (see 3.8) that are printed on paper sheets

3.10
Postulated Initiating Event
PIE
an event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[SOURCE: IAEA Safety glossary, 2007]

3.11
sequence
procedure sequence
a 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.

3.12
Supplementary Control Point
SCP
a 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. The supplementary control point may be a special control room, but in many cases comprises a set of control panels and displays in switchgear rooms or similar areas

[SOURCE: IEC 60965:2009, 3.5]

3.13
Visual Display Unit
VDU
type of display incorporating a screen for presenting computer-driven images

[SOURCE: IEC 60964:2009, 3.31]

4 Abbreviations

CBP	Computer Based Procedures
HMI	Human Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
MCR	Main Control Room
OP	Operating Procedures
PIE	Postulated Initiating Event
SCP	Supplementary Control Point
VDU	Visual Display Unit

5 CBP policy requirements

5.1 General

This clause provides an overview of CBP. It presents recommendations for the development of a policy for computerisation of procedures, based on the type of procedure to be implemented. Three generic types (termed “families”) are proposed, for which general and

specific guidance is provided. Guidance related to the safety requirements of CBP systems is also provided.

5.2 Computerisation policy

5.2.1 General

This activity shall be embedded in the framework 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.

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

Types of procedures that may be computerised are:

- 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, beyond design basis procedures,
- alarm response procedures,
- fire handling procedures,
- loss of electrical power procedures, and any types of procedures dedicated to unusual conditions,
- technical specification procedures,
- periodic tests procedures designed according to IEC 60671, for example dedicated to flux calibration or to reactor trip, or any other periodic tests procedures,
- technical component sheets, offering easy access to specific device data on the screen-based HMI.

5.2.2 Preliminary considerations

In addition to functional analysis and assignment and human factors design guidance which are excluded from the scope of this standard by 1.3, some other basic topics shall be considered at an early stage of the design. These are:

- national regulatory issues,
- operating strategies

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

- operating staff experience feed-back

  what is good, what should be improved, what is missing in any existing CBP or paper based solution should be identified;

  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,

- the operator training policy,
- data issued from the plant instrumentation,

  NOTE The CBP guidance level depends on available instrumentation.

- integration of the CBP processing into an HMI system, if digital, or use of a dedicated system to process CBP connected or not connected to a digital HMI system.

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

5.2.3 Final decision on use of CBP

To make a final decision on the types of procedures to be computerised, the following issues should be considered in the conceptual design:

- identification of the types of procedures that could be processed simultaneously 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,
- assessment of the amount of VDU 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 in a complementary way to CBP and paper based procedures.

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

- the set of work stations and work places where CBP are intended to be used, in the main control room and at all other control points,
- the fact that a procedure could be temporarily abandoned without being terminated, for example in case of an alarm outbreak,
- the maximum amount of information to be displayed in a format,
- the performance of the CBP system, in particular regarding displays, memory capacities, navigation,
- adequate additional margins in order to ease future modifications.

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.

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

- 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,
- the use of the final product, including maintenance facilities.

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 guidance,
- the required process inputs and outputs.

Table 1 – CBP Families

		Level of operator guidance →				
		Paper like (no data embedded)	**Basic guidance (steps only)**	**Enhanced guidance (animated)**	**Prepared decision suggestions**	Plant control
Process inputs and outputs ↓	**No process information**	Family 1	Not possible			
	Elementary process information	Not included	Family 2			Family 3
	+ Synthesised process information					
	+ Action on process					

The rows represent different kinds of process inputs and outputs. The columns represent different levels of computerisation. The intersections of rows and columns represent the possible options for CBP. For example, if the designer aims to support the operator with an animated enhanced guidance or decision suggestions, both elementary and synthesised process information is to be provided. If the designer aims to support the operator with plant control facilities, control means are to be supplied in addition to elementary and synthesised information.

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.

  CBP of this Family do not receive any process information.

- Family 2: CBP providing guidance to the operator based on information acquired by the CBP system. Every item of information may be integrated into the display formats presented.

  Three variants are distinguished in Family 2 according to the extent of guidance provided:

  – variant 2.1 provides the operator with elementary process values and equipment states in CBP formats. CBP access may be computerised, see 8.5.2,

  – variant 2.2, in addition to elementary information, provides the operator with synthesised information. Examples of synthesised information are the water level in the pressuriser or the margin to saturation or the point of reactor start-up. CBP entry, see 8.5.2, and / or diagnosis assistance may be computerised, see 8.5.3,

  – variant 2.3 provides the operator with all kinds of facilities of the previous variants completed by decision assistance,

  - optionally, possible discrepancies between operators actions and the suggested decision may be signalled.
- Family 3: CBP presenting information and operating steps with full integration of on-line plant information, states and values, so that actuators can be operated from the display, automatic control functions can be accessed, and automatic execution of sequences can be initiated by the operator from the CBP display formats.

All families may include some facilities presented in 8.7.

A different CBP family may be selected for each type of procedure listed in 5.2.1.

5.4 Overview of computerisation features

5.4.1 General

Computerisation is based on global considerations and on items related to operator guidance and to plant control.

5.4.2 Global requirements for computerisation

The procedure computerisation should:

- ensure that operators understand easily the operating strategy,
- leave full responsibility to the operators,
- give a clear view of the functional objective,
- ease progression inside procedures and limit calls between procedures,
- include the possibility for the operator to leave steps and sequences out, if they are not context relevant,
- provide adequate communication between members of the team,
- apply in the same way to all procedures of a given type, for example to all accident procedures or to all fire handling procedures,
- be consistent for different types of procedures that could be processed in parallel.

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, 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.

5.4.3 CBP guidance

Guidance provided by CBP should remind operators of the functional objective and how to achieve it.

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 in establishing 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:

- frequency of events or situations. For example, enhanced guidance should be provided for rare events compared with that for daily operation,
- the operating policy. For example, the desire for high plant availability may lead to an increase in computerisation and automation,
- 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 provides the operator with synthesised information and possibly some assistance as described in 8.7.

5.4.4 Procedure based automation

Where CBP processing system is independent from the HMI system controlling the plant, provisions in order to avoid possible discrepancies between commands sent by both of them shall be implemented or, at least, such discrepancies shall be signalled to the operator.

CBP can control the plant by:

- automatically launching and executing CBP sequences, for example a depressurisation sequence, when predefined conditions are met,
- automatically executing sequences that have been launched by an operator.

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

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

Additional considerations to be taken into account are:

- 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,
- CBP display formats may include command possibilities or may forward operators actions to control display formats of the HMI system. Another option may be to authorise CBP commands by enabling them from the HMI system.

The operator's situation awareness shall be enhanced by:

- displaying adequate information to keep the operator in the loop.

  Important decisions should not be automated, the end of automated sequences should be signalled, any problems encountered during an automated sequence should be signalled, process values reaching a predefined threshold should be signalled,
- providing him with possibilities to take control from CBP at any moment,
- 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 to implement CBP shall be concluded by definitions of:

- the type of CBP, their objectives and scope,
- the CBP implementation considering the HMI system,
- the CBP guidance options, including a description of the required information,
- the option for procedure based automation,
- the utility policy for operator training.

6 Use of CBP

6.1 General

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

6.2 Environment of use

6.2.1 General

This subclause 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.

In a general way, the overall integration of CBP in the MCR and in other control points shall be done based on IEC 60964 and on IEC 60965. Application of VDU shall comply with IEC 61772.

6.2.2 Use of CBP in computerised control rooms

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

Compatibility between CBP formats and operating formats of an HMI system should be ensured by:

- 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 plant control system and CBP formats when displayed at the same time.

  For example, "open valve" is displayed simultaneously on associated operating and CBP formats if the valve is shown on both formats.

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, 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.

Services such as HVAC (Heating, Ventilation, and Air Conditioning) capacities are also to be 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. should belong to family 1 or family 2, and should comply with 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,
- enable the operators to read CBP from their working areas, either in front of the VDU or from 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 options defined according to 5.2.3.

NOTE 1 For instance, detailed operation remaining paper based whereas operating strategy is computerised.

NOTE 2 For instance, 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

In case some local control rooms, SCP 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 Assistance to operators 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.

NOTE Procedures are designed to assist the operator by suggesting operation strategies and preparing possible actions regarding the plant state. Nevertheless, unexpected situations may 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 purpose 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 tasks of navigating 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 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 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 operators and the supervisor. Such coordination may be implemented by hold points in procedures, requesting oral dialogues and computerised acknowledgments.

NOTE For example, 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.

If several operators can access simultaneously 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 it is prevented that an operator repeats or stops 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, 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 different 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 and consistency.

7 CBP system

7.1 General

This clause deals with the digital system processing CBP, either integrated in the HMI system 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

Procedures, whether paper or computer based and whatever their level of guidance, are designed to be used by the operator, they cannot control the process without the operator actions. The latter 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 shall be determined according to IEC 61513, taking into account possible impacts on safety in case of:

- loss of CBP,
- erroneous guidance to operators or spurious control signals,
- availability of diverse information available to the operator, allowing to confirm information displayed by CBP. The operator should be trained to undertake such comparisons, see 9.10.

The classification should also consider:

- the functional coverage of CBP,
- the CBP family.

NOTE The different types of CBP are listed in 5.3.

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 CBP systems, as applicable for the CBP system's safety class. The level of redundancy of the CBP system shall be consistent with the safety class of the CBP system.

Particular attention, during development and verification phases, should be given to ensure that potential faults or failures of the CBP system cannot disable, inhibit or launch manual and automatic functions.

7.3 Integration of the CBP system into the HMI system

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

- the safety class of the HMI system is able to cope with the safety class of CBP as defined according to considerations in 7.2,
- HMI system features comply with the requirements of 5.2.3,
- HMI system features comply with the requirements of Clause 8.

7.4 CBP system independent from the HMI system

7.4.1 General

This subclause complements the safety requirements stated in 7.2 then deals with connections between the CBP system and the HMI system.

7.4.2 Non-safety requirements

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

- the CBP shall comply with the requirements of 5.2.3,
- reliability and availability requirements shall be specified,

- 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 work stations.

7.4.3 Connections between the CBP system and the HMI system

Some variables issued from the process or equipment may be used by the CBP system and the HMI system. If CBP are designed to control the plant, the CBP system and the HMI system may in addition be able to send orders to the same actuators.

Provisions should be taken to minimise time differences in updating dynamic parts of displays for the same object. A value in the range of 2 s may be considered acceptable.

The CBP system should not be jeopardised by possible failures of the HMI system. It should signal failures of its interfaces to the HMI system and failures blocking access to an actuator.

7.4.4 Maintenance of the CBP system

Maintenance of the CBP system shall be considered, i.e. specifications shall be provided for tests, for repairs, for spare parts and for specific tools. Provisions to comply with a required repair time shall be taken.

7.5 CBP system failure

Operators shall be trained to have a questioning attitude regarding the CBP performance. To support them, self-monitoring and self-test provisions detecting and signalling malfunction shall be implemented in the CBP system. Considering possible consequences of operator's misguidance, the coverage of the self-monitoring should be as high as 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 CBP or CBP system malfunction or failure, a diverse back-up means and an adapted procedures set shall be used. This back-up procedure set shall be compatible with the HMI system, if this latter is still available and used to operate the plant.

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

A diverse set of procedures designed to back-up the CBP system shall take into account that this situation is rare and stressful, and shall aim to avoid operator's mistakes or misunderstandings by:

- being independent from the CBP system, both from technical and functional points of view, i.e. 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 its safety class.

NOTE 3 Choosing as a back-up a second set of CBP 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 are implemented as a system separate from the HMI, the following apply:

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

7.6 Output documentation

Requirements and design options for the CBP system shall be documented consistently with IEC 61513 requirements.

8 Detailed design requirements

8.1 General

This clause describes how to computerise CBP features, 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.

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.

IEC 61772 and ISO 11064 series of standards should be used in order to design and display CBP formats. The CBP formats and operating formats displayed in the MCR should be compatible. This compatibility addresses HMI features such as graphic representation, variables names, format layout, navigation, etc.

CBP should be implemented with display formats according to 5.2.3, including those for display on local control stations when needed.

Any further change to the features defined accordingly to this subclause 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.

Each type of elementary CBP step is processed in the same way when encountered, but it can launch different actions due to its content. For example, a decision gate launches the execution of the formula it contains and can suggest what to do depending on the result,

- 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 their combinations, which are designed to be generically used, should be defined as re-useable elements, with a set of parameters to be specified.

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 CBPs and consistent with presentation paradigms of the HMI system,
- the possibility of operator errors using both CBP and a digital HMI system 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.

To minimise human errors, the format contents should:

- display the identification of the current procedure and of the current sequence within that procedure,
- identify clearly achieved steps, active step, and possible next steps,
- minimise the number of discrete actions to access a required format display,
- 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,
- importance of steps is displayed in a salient manner,
- warnings, cautions, and other information associated to 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 starts performing this step.

8.2.5 Requirements for presentation of individual display elements

Rules for presenting individual elements are:

- information and step parts 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 arrange that:

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

8.3 Information given by CBP

8.3.1 General

CBP should give information related to themselves, for example designation, version, release date, page number. Items of this description should either be systematically displayed or should be displayed on operator’s request.

All CBP families feature this kind of information,

- so that the operator is able to use the CBP guidance correctly,
- in order to keep the operator in the loop.

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, they indicate process and equipment values to be monitored but do not display any dynamic information from plant.

8.3.3 Information for family 2 CBP

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

- 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:

- an update frequency adapted to the needs of the procedure,
- prompt presentation of possible conflict between an operator input 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:

- summarised information,
- information related to the plant state,
- information chosen by the operator.

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 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, all 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 and CBP policies.

8.4.2 Navigation for family 1 CBP

Navigation for family 1 CBP should encompass possibilities to go directly to pages, skim through pages and to retrieve terms in pages.

Enhanced possibilities for retrieving pages or sequences, such as bookmarks, pop-up windows or thumbnails, may be implemented. 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.

Links to related procedures, for example to Technical Specification or alarm response procedure, 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 possibility to trace the path that was followed by the operator up to the current situation should be provided. 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 access,
- 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 access

Paper based procedures are accessed, depending on their nature:

- in case of a change in plant state, for example startup, outages,
- in case of an alarm or a process or equipment signal,
- periodically, for example surveillance procedures 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, for example accidents or any event indicated by safety parameters deviation, which can be clearly identified by the designer, may be identified and formalised so that their occurrence during operation could be signalled.

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

Details of the diagnosis should be displayed on operators' 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, 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 operators' choice in the case of a decision gate matches the suggestion,
- objectives of the considered procedure have been achieved.

Checkback signals from actuators may be used, for example in complex situations, to verify that the operator’s actions match CBP steps. In case of this option, inconsistencies should be signalled but shall not prevent any operator’s actions.

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 so that the operator can assimilate it, and is not distracted or puzzled by inadequate assistance,
- they leave the operator responsible for his actions, either by requesting him 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, e.g. 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 due to assistance functions should be given to the operator.

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 process 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:

- continuously inform the operator of what is being processed,
- enable the operator to take manual control at any time,
- inform the operator of the CBP state, for example read only, manual execution, automatic execution, etc.,
- enable 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 possibilities should be investigated, for example CBP may enable operators to select parts of CBP he wishes to be automatically processed.

8.6.3 Design of CBP to control the plant

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

- automated sequences begin and end in the same procedure,
- priority between control actions from control sequences of a CBP and other control actions has to be established in line with the priority rules for manual and automatic functions,
- sequences are predetermined and fixed. They may include hold points requiring operators 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.

In case 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 hidden procedures to:

- signal or alarm significant events,
- give periodic signs of life to indicate they are still processing. Alternatively, some procedures may be automatically stopped or frozen depending on designers' specification,
- 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 are not permanently displayed on VDU.

8.7 Other CBP facilities

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

- the possibility of including operator notes in the CBP may be provided. This corresponds to what operators are used to do on paper procedures. These notes could be used e.g. for indicating the need to temporarily deviate from the CBP under specific conditions that are to be detailed,
- the possibility 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 may be valuable,

- the possibility of adapting the guidance to the situation may be provided in order to enable the operator to choose a level of guidance adapted to his skill regarding specific CBP or sequences.

8.8 Output documentation

All options defined according to Clause 8 should be documented in different documents:

- 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

This clause 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 procedure computerisation project cumulates the HMI, operating strategies, and software engineering aspects. The HMI and operating strategies organisational aspects are similar to those of the paper based procedures. The software aspects should, if the CBP system is safety classified, 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,
- review and approval of procedures,
- revision of procedures.

Engineering tools should be used for ensuring quality and traceability during the typical procedure lifecycle 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 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.

  Operators experience and needs, as well as 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 project onset.

9.4 Verification and validation programme

A verification and validation programme shall be established to ensure that, throughout the development phase, the requirements of Clauses 6 and 8 are fulfilled and to prepare the final verification and validation of the complete product.

The CBP verification shall address both the compliance of the visual display formats with HMI specifications and the technical aspects which animate the procedures.

The CBP validation shall address both the functional and ergonomic aspects to ensure that a human operating team will succeed in achieving their safety and operability objectives when using CBP.

The verification and validation strategy should be defined early in the project in order to plan the necessary resources, i.e. human and digital tools. Adequate recording provisions should also be planned.

9.5 CBP Programming

The options defined in 6.3 to 6.4 should be evaluated early in the project on a mock-up in order not to be questioned during CBP development.

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 ensured,
- 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 is ensured,
- versions are correctly managed.

IEC 61513, IEC 60880 and IEC 62138 requirements may be applicable depending on the CBP safety class of the CBP system.

9.6 Verification and validation of CBP

9.6.1 General

This subclause addresses verification and validation of the technical and ergonomic aspects of the CBP, assuming that verification and validation regarding the software aspects of CBP has already been performed accordingly 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.

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 variables name and information displayed,
- inconsistencies between text of a step and guidance,
- inconsistencies between text of a step and 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:

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

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

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

In order to detect both possible programming and operating errors, a good practice may be to process automatically 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, with a complete operating team and a full scale process simulator able to simulate as accurately as possible the normal and abnormal transients that CBP are designed to operate.

The functional and ergonomic validation should aim to ensure that:

- the operator can understand and apply CBP in a correct way,
- CBP help the operator to achieve the expected functions,
- 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 HMI system.

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

- navigation between pages

  the operator may find it difficult to understand which part of a strategy he is applying and to plan his next actions by "leafing through" computerised pages,
- "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,
- 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,
- communication between members of the operating staff, and possibly with people from outside the operating staff.

9.7 CBP deployment

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:

- on-line management facilities,
- change of CBP version, which should:
  - be easy to deploy, i.e. a highly automated process,
  - not require a change in the plant state,
  - not impact plant operation,
  - not impact the HMI system, if any,

  - not impact the operating system of the CBP system,
- 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

IEC 61513, IEC 60880 and IEC 62138 should be used to issue adequate documentation regarding:

- the organisation to design, develop and validate CBP, as well as the organisation of CBP maintenance once in operation, based on the requirements of 9.3 and 9.4,
- all software programming documents, and those of 9.5,
- the results of CBP verification and validation, see 9.6,
- the documentation 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.

9.9 CBP and CBP system maintenance

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 digital HMI system, maintenance of the latter shall take into account CBP availability and reliability.

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

9.10 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.

Bibliography

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

IEC 62645[2], *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

_____

2 Under consideration.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – PROCÉDURES INFORMATISÉES

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

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

Le texte de cette norme est issu des documents suivants:

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – PROCÉDURES INFORMATISÉES

1 Domaine d'application

1.1 Objet

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

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

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

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

1.2 Vue d'ensemble des PI

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

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

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

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

---

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

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

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

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

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

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

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

- analyse fonctionnelle et répartition

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

- recommandations de nature ergonomique pour la conception

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

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

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

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

1.4 Structure de la présente norme

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

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

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

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

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

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

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

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

2 Références normatives

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

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

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

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

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

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

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

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

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

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

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

3 Termes et définitions

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

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

3.2
Procédures Informatisées
PI
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, de placer des marques page et d'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
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: CEI 60964:2009, 3.7]

3.5
démarche intellectuelle
démarche humaine de traitement et/ou d'interprétation d'une information visant à obtenir une information condensée et abstraite

[SOURCE: CEI 60964:2009, 3.12]

3.6
Interface Homme Machine
IHM
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: CEI 60964:2009, 3.13]

3.7
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: CEI 62241:2004, 3.29]

3.8
procédures de conduite
PC
ensemble de documents spécifiant les tâches de conduite qu'il est nécessaire de remplir pour atteindre les objectifs fonctionnels

[SOURCE: CEI 60964:2009, 3.19]

3.9
procédures papier
PC (voir 3.8) imprimées sur feuilles de papier

3.10
événement initiateur postulé
EIP
évènement 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, Edition 2007]

3.11
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 disfonctionnement 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.

3.12
point de commande supplémentaire
PCS
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. Le point de commande supplémentaire peut être une salle de commande particulière, mais dans la plus part des cas celui-ci correspond à un ensemble de panneaux de commande et d'affichage dans des locaux électriques ou dans des zones similaires.

[SOURCE: CEI 60965:2009, 3.5]

3.13
unité de visualisation
VDU
type d'affichage incorporant un écran pour présenter des images pilotées par calculateur

[SOURCE: CEI 60964:2009, 3.31]

4 Abréviations

PI Procédures Informatisées

IHM Interface Homme Machine

ACVC Air Conditionné, Ventilation et Chauffage

SdC Salle de Commande principale

PC Procédures de Conduite

EIP Evènement Initiateur Postulé

PCS Point de Commande Supplémentaire

VDU unité de visualisation (*Visual Display Unit*)

5 Exigences portant sur la politique associée aux PI

5.1 Généralités

Cet article donne une vue d'ensemble des PI. Il présente des recommandations pour le développement d'une politique d'informatisation des procédures, dépendant du type de procédures à mettre en œuvre. Trois types génériques (appelés «familles») sont proposés, pour lesquels des recommandations générales et particulières sont données. Des recommandations portant sur les exigences de sûreté liées aux systèmes PI sont aussi fournies.

5.2 Politique d'informatisation

5.2.1 Généralités

Cette activité doit être couverte par le cadre de travail relatif à 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'Article 5 de la CEI 60964:2009.

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 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, le niveau d'automatisation, etc. sont hors du domaine de la présente norme.

Les types de procédures qui peuvent être informatisées sont les suivants:

- 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,

- procédures de conduite accidentelles ou procédures adaptées aux évènements hors dimensionnement,
- procédures de réponse aux alarmes,
- procédures incendie,
- procédures liées aux pertes sources et toutes autres procédures liées à des conditions inhabituelles,
- procédures correspondant aux spécifications techniques,
- procédures d'essais périodiques conçues conformément à la CEI 60671, par exemple cartes de flux ou les étalonnages liés aux arrêts rapides du réacteur, ou toutes autres procédures d'essais périodiques,
- schémas techniques matériel, facilitant, à partir d'écrans associés à l'IHM, l'accès à des données particulières concernant des équipements.

5.2.2 Considérations préliminaires

En plus des recommandations liées à l'analyse fonctionnelle et à l'affectation ainsi que celles liées à la conception ergonomique qui sont exclues du domaine de la présente norme en 1.3, certains autres sujets de base doivent être pris en considération dès les premières étapes de conception. Ces points sont les suivantes:

- le cadre réglementaire national,
- la stratégie de conduite

  cette question fonctionnelle est indépendante de l'informatisation et un choix doit être fait entre les approches par état ou évènementielle pour conduire en cas d'accident,
- 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,
- le retour d'expérience de l'équipe de conduite

  les points satisfaisants et les points à améliorer, les points manquant sur toutes les solutions papier ou à base de PI et qu'il convient d'identifier;

  de plus, le concepteur peut considérer qu'il convient que seule la stratégie de conduite soit informatisée ou bien qu'au contraire il convient que seules les procédures de détail soient l'objet de l'informatisation,
- la politique de formation des opérateurs,
- les données d'installation de la centrale,

  NOTE Le niveau des recommandations des PI dépend de l'instrumentation disponible.
- l'intégration du traitement relatif aux PI dans l'IHM, si celui-ci est informatisé, ou l'utilisation d'un système dédié aux PI, connecté ou non à un IHM informatisé.

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 Décisions finales portant sur les PI

Il convient de répondre aux questions suivantes au niveau de la conception pour prendre les décisions finales portant sur le type de procédures à informatiser:

- identification du type des procédures qui peuvent être utilisées simultanément en exploitation normale, en cas d'incendie, en cas de perte des sources électriques, en cas d'essais périodiques, en cas d'EIP,
- évaluation du nombre 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'évènements 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 complémentaire des tâches de l'équipe de conduite au niveau des PI et des procédures papier.

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

- 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,
- 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,
- le volume maximum d'information qui peut être affiché sur une image,
- les performances du système PI, en particulier en ce qui concerne l'affichage, les capacités mémoire, la navigation,
- les marges supplémentaires appropriées pour faciliter de futures modifications.

Certaines réponses à ces questions peuvent poser des problèmes au niveau aspects de la mise en œuvre de la politique relative aux PI ou au niveau 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:

- 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,
- l'utilisation du produit final, y compris les dispositions relatives à la maintenance.

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 de recommandation prévu,
- les entrées/sortie procédé requises.

Tableau 1 – Familles de PI

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="4">Niveau de recommandation opérateur →</td><td rowspan="2">Commande de la centrale</td></tr>
<tr><td>Papier (aucune donnée intégrée)</td><td>Recommandations de base (seulement les étapes)</td><td>Recommandations avancées (animées)</td><td>Préparation de suggestions de décision</td></tr>
<tr><td rowspan="4">Entrée / sortie procédé ↓</td><td>Pas d'information procédé</td><td>Famille 1</td><td colspan="4">Impossible</td></tr>
<tr><td>Information procédé élémentaire</td><td rowspan="3">Non inclus</td><td colspan="3" rowspan="2">Famille 2</td><td rowspan="3">Famille 3</td></tr>
<tr><td>+ Information de synthèse procédé</td></tr>
<tr><td>+ Action sur le procédé</td><td colspan="3">Famille 3</td></tr>
</table>

Les lignes correspondent à différentes sortes d'entrée/sortie procédé. Les colonnes correspondent à différent niveaux d'informatisation. Les intersections des lignes et des colonnes indiquent les possibilités pour les PI. Par exemple, si le concepteur veut fournir à l'opérateur une aide correspondant à des recommandations animées de niveau avancé ou des suggestions de décision, les informations procédé à la fois élémentaire et de synthèse doivent être fournies. Si le concepteur veut fournir à l'opérateur des fonctionnalités de commande, les moyens de commande doivent être fournis en plus de l'information élémentaire et de l'information de synthèse.

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, qui correspondent à des pages d'information et d'instructions d'exploitation.

  Les PI de cette famille ne reçoivent aucune information de la part du procédé.

- Famille 2: Les PI qui fournissent 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.

  On distingue trois variantes dans la famille 2 suivant le niveau de recommandations données:

  – Pour la variante 2.1 l'opérateur obtient grâce aux images des PI l'information élémentaire associée au procédé et à l'état des matériels. L'accès aux PI peut être informatisé, voir 8.5.2.

  – Concernant la variante 2.2, en plus de l'information élémentaire, l'opérateur obtient une information synthétisée, par exemple le niveau d'eau pressuriseur ou la marge à la saturation ou le seuil de démarrage réacteur, les entrées des PI, les accès aux PI, voir 8.5.2, et/ou une aide au diagnostique, qui peut être informatisée, voir 8.5.3.

  – Avec la variante 2.3; l'opérateur a toutes les fonctionnalités associées aux variantes précédentes et il bénéficie en plus d'une aide à la prise de décision.

  – En option, l'opérateur peut avoir le signalement des discordances entre ses actions et les décisions qui ont été proposées.

- Famille 3: les PI 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 que les actionneurs de tranche puissent être commandés par affichage, que l'accès 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.

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

Différentes familles de PI peuvent être choisies pour chaque type de procédure dont la liste est fournie en 5.2.1.

5.4 Vue d'ensemble des caractéristiques de l'informatisation

5.4.1 Généralités

L'informatisation repose sur des considérations globales 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

Il convient que la procédure d'informatisation:

- garantisse que l'opérateur comprend facilement la stratégie de conduite,
- laisse à l'opérateur la pleine responsabilité de la conduite,
- donne une vue claire de l'objectif fonctionnel poursuivi,
- facilite la progression au sein de la procédure et limite les appels entre les procédures,
- permette à l'opérateur d'ignorer des instructions et des séquences, si le contexte n'est pas pertinent,
- offre des possibilités de communications appropriées entre les membres de l'équipe de conduite,
- 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,
- garantisse la cohérence pour les différents types de procédures qui peuvent être déroulées en parallèle.

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 des exigences associées aux capacités de traitement sont cohérentes avec les capacités offertes par le système PI.

5.4.3 Recommandations associées aux PI

Il convient que les recommandations produites par les PI rappellent à l'opérateur l'objectif fonctionnel de la procédure et les moyens pour l'atteindre.

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 diagnostique ou lui suggérer des décisions à prendre.

L'aide au diagnostique ou la suggestion de décision peuvent être:

- automatisée: un diagnostique 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 diagnostique 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:

- la fréquence des évènements ou des situations, par exemple il convient de fournir des recommandations élaborées plutôt pour des évènements rares que pour l'exploitation journalière,
- la politique de conduite, par exemple objectif d'exploitation ambitieux en termes de disponibilité peut entraîner un surcroît d'informatisation ou d'automatisation,
- 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 Conduite de la centrale par les PI

Lorsque le système de traitement des PI est indépendant du système d'IHM de conduite de la centrale, des mesures doivent être mises en place pour éviter des discordances possibles entre les commandes envoyées par les deux systèmes simultanément ou ces discordances doivent au moins être signalées à l'opérateur.

Les PI peuvent permettre de conduire l'installation à partir:

- du lancement et du traitement automatiques des séquences de PI, par exemple une séquence de dépressurisation 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 informatisé,
- le fait que l'ensemble des procédures du système de secours est indépendant du système d'IHM et des PI,
- la facilité de compréhension pour l'opérateur, en particulier en conditions anormales.

Les considérations supplémentaires à prendre en compte sont:

- 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.
- Les images PI peuvent comprendre la possibilité de passer des commandes ou peuvent permettre de lancer des actions opérateur pour contrôler des images du système IHM. Une autre option consiste à autoriser les commandes des PI en les validant à partir de l'IHM.

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

- affichant l'information pertinente pour que l'opérateur soit toujours impliqué dans la conduite.

  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; il convient que toute valeur du procédé atteignant un seuil prédéfini soit signalée,

- lui fournissant les possibilités de reprendre à tout instant le contrôle sur les PI,

- prenant en compte la coordination de l'équipe de conduite.

  Les séquences lancées par deux opérateurs peuvent être désynchronisées et il convient qu'elles n'aient pas pour conséquence l'exécution d'actions concurrentes et contradictoires.

5.5 Documentation produite

La décision de mettre en œuvre des PI doit au final définir:

- le type des PI, leurs objectifs et leurs domaines,
- la mise en œuvre des PI par rapport au système d'IHM,
- les options retenues concernant les recommandations des PI, y compris la description de l'information requise,
- les options retenues pour les procédures automatisées,
- la politique retenue par l'exploitant pour la formation des opérateurs.

6 Utilisation des PI

6.1 Généralités

Cet article fournit des exigences applicables pour l'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 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'utilisation

6.2.1 Généralités

Ce paragraphe 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, avec l'utilisation de procédures papier en parallèle en SdC ou localement par les rondiers.

De façon générale, l'intégration d'ensemble des PI dans la SdC et dans les autres points de commande doit être faite conformément aux exigences des CEI 60964 et CEI 60965. L'utilisation des unités de visualisation doit être conforme à la CEI 61772.

6.2.2 Utilisation des PI dans les SdC informatisées

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

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

- 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 de conduite du système de commande de la centrale et des images PI sans désynchronisation temporelle notable lorsqu'elles sont affichées simultanément.

  Par exemple le libellé «vanne ouverte» est affiché simultanément sur les images de conduite et sur celles des PI si la vanne est présentée sur ces images.

6.2.3 Utilisation des images 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, c'est-à-dire principalement l'espace libre, et celles liées aux zones de travail des opérateurs, 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.

Les moyens, tels que ceux de chauffage, ventilation, conditionnement de l'air sont à prendre 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, enregistreurs, 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.
- 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.

NOTE 1 Par exemple, les procédures détaillées de conduite peuvent se faire sur la base de procédures papier alors que la stratégie de conduite est informatisée.

NOTE 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, alors les procédures papier sont utilisées en attente de la mise en service de la nouvelle version corrigée des PI.

De telles situations 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,
- le passage de quart et la transmissions des explications nécessaires restent faciles.

6.2.5 Utilisation des PI hors de la SdC

Lorsque certaines salles de commande locales, par exemple les points de commande supplémentaires, 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 Aide aux 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 évènements qui surviennent.

NOTE 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 peuvent 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 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'information), et les activités secondaires (par exemple la gestion des fenêtres et la navigation qui sont liées à la recherche de l'information nécessaire).

6.3.2 Aide aux activités principales de l'opérateur

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

- 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. Les principales décisions de conception concernant ces aspects doivent être documentées, 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 Coordination des utilisateurs

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.

NOTE Par exemple, le superviseur est le seul utilisateur des PI et il coordonne les autres opérateurs, ou bien le superviseur et les opérateurs primaire et secondaire ont accès aux PI.

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, 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 différents documents:

- une synthèse donnant les options retenues et les raisons sous jacentes concernant la conception, le développement, la validation ou les phases d'agrément règlementaires,
- 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

7.1 Généralités

Cet article couvre le traitement du système numérique PI, qu'il soit intégré dans le système d'IHM de conduite 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 Exigences de sûreté

Les procédures, qu'elles soient papier ou informatisées et quel que soit leur niveau, sont utilisées par des opérateurs, elles ne peuvent pas commander au procédé sans que des commandes opérateur soient passées. L'opérateur est supposé agir de façon intelligente, ne pas appliquer les procédures automatiquement, ainsi il reste seul responsable de l'application pertinente des procédures.

Le classement de sûreté du système PI doit être fait conformément aux recommandations de la CEI 61513, en prenant en compte les conséquences sur la sûreté en cas:

- de la perte de ces fonctions;
- de recommandations erronées fournies à l'opérateur, ou de signaux de commande intempestifs,
- de la disponibilité 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 9.10.

Il convient que le classement prenne aussi en compte:

- la couverture fonctionnelle des PI,

- la famille de PI.

NOTE La liste des différents types de PI se trouve en 5.3.

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 la CEI 61513, la CEI 60880 et la CEI 62138 doivent être satisfaites pour la conception et la mise en œuvre des systèmes PI, telles qu'applicables en fonction des classes de sûreté des systèmes PI. Les niveaux de redondance des systèmes PI doivent être cohérents avec les niveaux de leurs classements de sûreté.

Il convient, pendant les périodes de développement et de vérification, de faire particulièrement attention à garantir que des défauts ou des défaillances potentiels ne puissent rendre non opérationnel le système PI, inhiber ou lancer des actions manuelles ou automatiques.

7.3 Intégration du système PI dans le système d'IHM

Pour intégrer le traitement associé aux PI dans le système d'IHM, on doit vérifier que:

- la classe de sûreté du système d'IHM est compatible avec la catégorie de sûreté des fonctions associées aux PI, telle que définie et conformément aux exigences de 7.2,
- les caractéristiques du système d'IHM satisfont aux exigences de 5.2.3,
- les caractéristiques du système d'IHM satisfont aux exigences de l'Article 8.

7.4 Système PI indépendant du système d'IHM

7.4.1 Généralités

Ce paragraphe complète tout d'abord les exigences de sûreté fournies en 7.2, puis couvre les connexions existant entre le système PI et le système d'IHM.

7.4.2 Exigences non liées à la sûreté

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

- les PI doivent être conformes aux exigences de 5.2.3,
- les exigences liées à fiabilité et à la disponibilité doivent être spécifiées,
- les autotests doivent être spécifiés,
- il convient que les capacités non utilisées soient 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 possible de connexions de stations de travail.

7.4.3 Connexions entre le système PI et le système d'IHM

Certaines variables provenant du procédé ou relatives aux matériels peuvent être utilisées par le système PI et le système d'IHM. Si les PI sont conçues pour conduire la centrale, le système PI et le système d'IHM peuvent en plus être capables d'envoyer des ordres aux mêmes actionneurs.

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 le système PI ne puisse pas être affecté par les possibles défaillances du système d'IHM. Il convient qu'il signale les défaillances de ses interfaces avec le système d'IHM et les défaillances qui empêchent l'accès aux actionneurs.

7.4.4 Maintenance du système PI

La maintenance du système PI doit être prise en compte, c'est-à-dire les spécifications doivent être fournies pour les essais et les réparations, les lots de rechange, et les outils particuliers. Les mesures nécessaires doivent être mises en place pour pouvoir réparer en un temps spécifié.

7.5 Défaillances du système PI

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 mises en place au niveau du système PI pour détecter et signaler les disfonctionnements. 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. Pour améliorer le niveau de détection des disfonctionnements des PI, une partie de l'équipe de conduite peut utiliser des procédures papier.

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

Lorsqu'un opérateur suspecte un disfonctionnement 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 disfonctionnement des PI ou du système PI ou de défaillance, 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 système d'IHM, 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 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 système d'IHM principal ne sera pas restauré.

Un ensemble de procédures diversifié conçu pour servir de secours au système PI 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 libre de 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 son classement de sûreté.

NOTE 3 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 disfonctionnements, cela représente 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 d'IHM, les points suivants sont applicables:

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

7.6 Documentation produite

Les exigences et les options de conceptions relatives au système PI doivent être documentées conformément aux exigences de la CEI 61513.

8 Exigences relatives à la conception détaillée

8.1 Généralités

Cet article décrit les moyens employés pour informatiser les fonctionnalités des PI, en partant des plus simples jusqu'aux plus sophistiquées, c'est-à-dire information, navigation, orientation et conduite de la centrale. Différentes options pouvant faciliter l'utilisation des PI sont aussi données.

8.2 Fonctionnalités de base des PI

8.2.1 Généralités

Les fonctionnalités de base des PI doivent être définies au tout début du début du projet afin de pouvoir coordonner le développement du système, d'éviter les mauvaises interprétations lors de l'utilisation des PI et de faciliter leur maintenance, de plus ces définitions de fonctionnalités doivent être utilisées durant tout le cycle de vie des PI. Elles doivent être utilisées pour concevoir, pour développer et pour maintenir l'ensemble des PI.

NOTE Les personnels qui mettent à jour les PI peuvent être différents de ceux qui ont participé au développement initial de celles-ci.

Il convient que l'équipe intégrée présentée en 9.3 soit impliquée dans la réalisation de cette activité. Il convient que le retour d'expérience acquis avec les procédures papier soit pris en compte ainsi que celui connu relatif à l'utilisation d'autres systèmes PI.

Il convient d'utiliser la CEI 61772 et la série de normes ISO 11064 de façon à concevoir et à afficher les images PI. Il convient qu'on assure la compatibilité entre les images PI et les images de conduite affichées en SdC. Ce souci de compatibilité porte en particulier sur les caractéristiques de l'IHM telles que la représentation graphique, le nommage des variables, les formats d'image, la navigation, etc.

Il convient de mettre en œuvre les PI pour que les images soient affichées conformément à 5.2.3, y compris pour celles utilisées sur les stations de commande locales lorsque nécessaire.

Il convient que toute modification des fonctionnalités définies conformément à ce paragraphe que l'on souhaite mettre en œuvre soit justifiée, formellement acceptée et documentée.

8.2.2 Eléments de base nécessaires aux PI

Il convient de définir de façon précise et non ambiguë les caractéristiques de base des PI suivantes:

- tous les termes techniques, les symboles et les éléments graphiques,
- un glossaire qui donne le sens et la manière d'utiliser chacun des éléments des images,

- les symboles et les schémas représentant les actions élémentaires des PI, de même que les liens existant entre les PI.

  Chacune des étapes des PI est traitée de la même façon lorsqu'elle est déroulée, par contre elle peut lancer différentes actions suivant son contenu. Par exemple un branchement conditionnel lance le calcul de la formule qu'il contient et peut suggérer ce qu'il faut faire suivant le résultat obtenu,

- les règles de traitement du contenu des étapes des PI,

- les règles de nommage applicables aux variables internes ou calculées,

  NOTE Les noms de variables aident les opérateurs à comprendre le type et l'utilisation des variables calculées.

- les règles de navigation entre les étapes élémentaires, les pages ou les séquences de PI ou entre les PI.

Il convient de définir comme réutilisables en spécifiant un ensemble de paramètres, les éléments tels que «les étapes», «les indicateurs», «les boîtes décisionnelles», ainsi que leurs combinaisons qui sont conçues à des fins d'usage générique.

8.2.3 Règles de présentation

De façon à minimiser la charge mentale des opérateurs et pour être cohérent avec les exigences génériques de 5.4.2, il convient de concevoir la présentation des PI de façon à ce que:

- les actions locales puissent être clairement identifiées,
- une vue d'ensemble de toutes les procédures en cours d'exécution, mêmes de celles qui sont interrompues soit fournie à l'opérateur,
- la présentation des procédures soit cohérente pour toutes les PI et soit cohérente avec les principes de présentation du système d'IHM,
- les possibilités d'erreur des opérateurs utilisant les PI et le système d'IHM informatisé pour conduire la tranche soient minimisées,
- l'information nécessaire pour dérouler la procédure soit lisible à partir de la position de travail de l'opérateur,
- la version la plus récemment approuvée et diffusée de la procédure soit toujours celle qui est présentée.

Dans le but de minimiser les erreurs humaines, il convient que le contenu des images:

- affiche l'identificateur de la procédure courante et celui de la séquence courante au sein de cette procédure,
- identifie clairement les étapes déroulées, les étapes en cours d'exécution et les étapes possibles suivantes,
- minimise le nombre de manipulations élémentaires nécessaires pour obtenir l'affichage d'une image nécessaire,
- facilite le dialogue entre l'opérateur et la procédure.

8.2.4 Modèles des images affichables par les PI

Il convient que les modèles des images affichables par les PI soient conçues de façon à ce que:

- l'identification d'une procédure, par exemple son titre, son code fonctionnel comme ses objectifs fonctionnels, soient visibles en permanence comme composants de l'image de cette procédure et que ces éléments soient positionnés toujours aux mêmes endroits dans les images,
- l'allocation de l'information suive la même méthode pour toutes les procédures,

- la division d'une procédure en séquence soit faite suivant des règles consistantes,
- l'importance de chaque étape soit affichée de façon patente,
- les avertissements, les mises en garde et les autres informations concernant chaque simple étape soient visibles à chaque affichage de l'étape,
- chacun de ces avertissements ou mises en garde ou informations soit présenté et qu'il doive être lu, par exemple en utilisant des menus qui apparaissent et disparaissent et qui demandent des confirmations à l'opérateur, avant que celui-ci ne commence à exécuter l'instruction.

8.2.5 Exigences portant sur la présentation des éléments individuels

Les règles applicables pour présenter les éléments individuels sont les suivantes:

- il convient que les parties relatives à l'information et celles relatives aux étapes aient des apparences différentes,
- il convient que quelle que soit la procédure, la présentation des branchements décisionnels et de leur choix associés (par exemple «oui» ou «non») soit uniformisée,
- si une réponse de l'opérateur est nécessaire, il convient que l'automatisme ne poursuive pas sans réponse de l'opérateur.

Chaque fois que les procédures contiennent des éléments d'information répétitifs, tels qu'un ensemble de matériels de la centrale, ou un ensemble d'actions similaires, etc., il convient que la présentation de ces éléments soit faite sous forme de listes. Il convient de prévoir à la conception que:

- les listes soient situées à part dans les procédures,
- la priorité entre les articles soit clairement indiquée,
- toutes les listes aient un titre,
- l'attention de l'opérateur soit attirée par la liste.

8.3 Informations fournies par les PI

8.3.1 Généralités

Il convient que les PI fournissent les informations qui leurs sont associées, par exemple leurs désignations, leurs versions, leurs dates de mise à disposition, leurs nombres de pages. Il convient que les éléments décrits ici soient ou bien systématiquement affichés ou bien affichés sur demande utilisateur.

Toutes les familles de PI présentent ce genre d'information de façon à ce que:

- les opérateurs soient capables d'utiliser correctement les orientations suggérées par les PI,
- les opérateurs restent impliqués dans le processus de conduite.

Les alarmes et les messages produits par le procédé ou un évènement survenant sur l'installation doivent être adaptés à la phase de conduite durant laquelle ils peuvent apparaître et ne pas induire en erreur l'opérateur ou le faire douter.

Les alarmes produites par les PI doivent être affichées de la même façon que celles produites par les évènements associés au procédé ou aux matériels. Il convient pour cela d'utiliser la CEI 62241 comme référence de conception.

8.3.2 Informations concernant les PI de la famille 1

Les PI de la famille 1 sont similaires aux procédures papier, elles indiquent les valeurs liées au procédé ou aux matériels qui sont à surveiller mais n'affichent pas d'information dynamique provenant de l'installation.

8.3.3 Informations concernant les PI de la famille 2

De façon à garantir une bonne compréhension du fonctionnement de l'installation, les informations concernant les PI doivent comprendre toutes les indications et les données d'entrée fournies par le procédé et les matériels:

- nécessaires à la compréhension et à la réalisation des stratégies de conduite,
- nécessaires à la compréhension du contexte, des états de tranche et des messages affichés, pertinentes pour la procédure.

Il convient d'assurer la qualité des informations liées aux PI par:

- une mise à jour périodique adaptée au besoin de la procédure,
- un signalement rapide des conflits potentiels entre les données fournies par l'opérateur et les valeurs acquises ou calculées.

Il convient que l'opérateur puisse accéder rapidement à des informations de type références croisées. Il convient que les résultats des étapes des procédures papier déroulées pour mettre en évidence par vérifications croisées des données soient pris en compte par les PI.

Il convient que la disponibilité des informations soit signalée à l'utilisateur. Plus généralement, il convient que le statut des informations soit accessible, par exemple: disponible, inhibée pour essai, inhibée pour maintenance, indisponible, discordante par rapport à d'autres données d'entrée.

Il convient que l'application de la politique de conception entraîne des prises de décisions concernant l'affichage:

- d'informations de synthèse,
- d'informations associées à l'état de tranche,
- d'informations choisies par l'opérateur.

Ces options peuvent entraîner le calcul de valeurs complémentaires par le système PI à partir de données d'entrée ou d'autre valeurs internes. Cela peut aussi obliger à compléter les exigences de base par un indicateur de leur fiabilité, calculé par exemple à partir de vérifications croisées de différentes valeurs.

Il convient que les valeurs calculées complémentaires:

- soient accessibles par l'utilisateur de la même façon que n'importe quelle autre valeur acquise sur le terrain,
- soient facilement identifiables lorsqu'elles sont affichées sur les unités de visualisation, par exemple en utilisant un encodage particulier ou un code couleur.

Les caractéristiques des informations peuvent dépendre suivant le type des procédures dont la liste est donnée en 5.2, pourvu que les images de l'IHM restent consistantes.

La politique de recommandation peut exiger que les éventuelles discordances entre les actions opérateur et le actions suggérées soit signalées.

8.3.4 Informations concernant les PI de la famille 3

Afin de pouvoir conduire en automatique la tranche, toutes les informations concernant les PI de la famille 2, obligatoires et optionnelles, doivent être fournies aux PI de la famille 3.

8.4 Navigation

8.4.1 Généralités

Il convient que les possibilités de navigation soient mises en œuvre conformément aux politiques mises en place pour l'IHM et pour les PI.

8.4.2 Navigation pour les PI de la famille 1

Il convient que la navigation dans les PI de la famille 1 permette d'aller directement aux pages, de les feuilleter et de rechercher des termes particuliers dans les pages.

On peut mettre en œuvre des fonctionnalités avancées permettant de retrouver des pages, des séquences, des signets, des fenêtres qui apparaissent, des croquis. Il convient que les fenêtres qui apparaissent le fassent dans des zones prédéfinies de l'image, il convient qu'elles ne masquent pas une partie trop importante de l'image, et il convient qu'il soit facile de les déplacer d'un endroit à un autre.

Des liens par rapport à des procédures connexes, par exemple aux Spécifications Techniques ou à la procédure de réponse aux alarmes peuvent être fournis. Il convient qu'on ne puisse pas les confondre avec des étapes individuelles.

Si plusieurs procédures sont actives en parallèle, il convient qu'il soit possible de passer de l'une à l'autre, même si la suivante n'est pas en cours d'affichage.

8.4.3 Navigation pour les PI des familles 2 et 3

La navigation pour les familles 2 et 3 correspond à une extension des fonctionnalités de navigation prévues pour la famille 1, aux séquences et aux étapes individuelles au sein des procédures.

De plus, les procédures peuvent être explorées en fonction du type d'étapes, par exemple pour trouver le branchement décisionnel suivant relatif à la pression primaire.

Il convient de fournir la possibilité de tracer le chemin qui a été suivi par l'opérateur pour arriver à la situation courante. Il convient qu'on ne puisse pas confondre ces images historiques avec les images correspondant à la situation courante.

8.5 Recommandations des PI pour la conduite

8.5.1 Généralités

Les recommandations fournies par les PI reposent sur les mêmes bases que celles fournies par les procédures papier, mais celles-ci sont plus développées du fait de la mise en application de la politique d'informatisation. L'étendue des recommandations va de l'information élémentaire procédé jusqu'à l'aide avancée pour ce qui concerne:

- l'accès aux PI,
- le diagnostique,
- la prise de décision.

NOTE Le niveau de détail atteint par les recommandations varie, en partie du fait de la nature des procédures, par exemple les procédures accidentelles fournissent plus de recommandations que les procédures de fonctionnement normal, et en partie du fait du niveau supposé de connaissance de l'opérateur qui repose sur la politique de formation.

8.5.2 Accès aux PI

L'accès aux procédures papier dépend de leur nature:

- en cas de changement d'état de tranche, par exemple démarrage, arrêt de tranche,
- en cas d'apparition d'alarme ou d'un signal lié au procédé ou à un matériel,
- périodiquement, par exemple les procédures de surveillance sont utilisées à chaque changement de quart.

Considérant les PI à disposition, suivant les évènements périodiques ou ceux survenant sur la centrale on peut indiquer automatiquement quel type de PI doit être utilisé. L'utilisation d'une procédure particulière peut être recommandée ou celle-ci peut être sélectionnée automatiquement.

Il convient que l'accès à la bonne procédure soit aussi rapide que possible, c'est-à-dire qu'il convient d'éviter les chemins de sélection complexes.

Les PI peuvent aussi permettre à l'opérateur de surveiller automatiquement des valeurs associées au procédé ou à des matériels et de définir des seuils par rapport à celles-ci. Lorsqu'un seuil est atteint, un signal peut être envoyé et si aucune autre information n'est nécessaire, ni aucune autre action n'est prérequise, ni aucune règle de prudence n'est transgressée, alors on peut avoir un accès direct à l'étape appropriée de la PI et celle-ci peut être affichée.

Il convient que les PI puissent être manuellement accessibles et que les évènements initiateurs puissent être affichés sur demande opérateur.

8.5.3 Aide au diagnostique

Les situations de tranche particulières, par exemple les accidents ou tout autre évènement qui se traduit par la dérive d'un paramètre de sûreté, qui peuvent être clairement identifiées par le concepteur, peuvent être identifiées et formalisées au niveau des PI pour que lorsqu'elles sont rencontrées en exploitation elles puissent être signalées.

L'opérateur doit rester seul responsable lorsqu'il accepte le diagnostique et qu'il accède à la procédure suggérée.

Il convient que les informations de détail associées au diagnostique puissent être affichées sur demande opérateur.

8.5.4 Aide à la décision

Il convient de limiter l'aide à la décision aux étapes qui nécessitent une prise de décision. Les informations, telles que les données d'entrée, les alarmes, les courbes de tendance, les valeurs de synthèse, etc., qui sont à ce moment là nécessaires doivent être disponibles et facilement accessibles.

L'opérateur doit rester responsable de la prise de toutes les décisions.

Pour améliorer l'aide à la décision, il convient que les PI indiquent que:

- la procédure suggérée a été lancée,
- chaque étape a été validée par l'opérateur,
- chaque étape a reçu un signal de confirmation d'exécution positif,
- le choix de l'opérateur dans le cas d'un branchement décisionnel confirme la suggestion,
- les objectifs de la procédure en question ont été atteints.

Les acquittements de passage des ordres renvoyés par les actionneurs peuvent être utilisés, par exemple dans des situations complexes, pour vérifier que les actions opérateur sont bien conformes aux étapes des PI. Lorsque cette option est mise en œuvre, il convient que les discordances soient signalées, mais on ne doit bloquer aucune des actions opérateur.

8.5.5 Informatisation des recommandations produites par les PI

Quel que soit le type ou le niveau de recommandation, les PI doivent être informatisées avec pour objectif:

- d'afficher tous les éléments nécessaires pour permettre à l'opérateur de comprendre et de conduire la tranche en toutes situations,
- de fournir des informations d'un niveau et d'une pertinence raisonnables pour que l'opérateur puisse les assimiler, et ne soit pas perturbé par des suggestions inappropriées,
- de laisser à l'opérateur la responsabilité de ses actions, ou bien en lui demandant de valider des suggestions ou bien en le laissant choisir une séquence d'actions différente des actions suggérées,
- de permettre sur demande opérateur l'affichage des raisons à l'origine des suggestions,
- de permettre de distinguer entre les suggestions, les étapes ou les informations,
- de ne pas cacher une partie importante de l'image affichée par de l'information de moindre importance,
- que le gel de la mise à jour des informations, par exemple du à une défaillance matériel, soit facilement détecté.

Il convient que l'aide soit affichée sur demande opérateur et il convient que l'opérateur soit capable de l'arrêter à n'importe quel instant.

Il convient que l'opérateur ait les moyens pour provisoirement ne plus avoir l'affichage des messages d'alerte qui peuvent être émis par les fonctions d'aide.

L'utilisation d'autres procédures peut être suggérée et les liens permettant d'accéder à celles-ci peuvent être fournis.

8.6 Procédures automatisées

8.6.1 Généralités

Les PI peuvent être conçues pour réaliser automatiquement un certain nombre de tâches sous le contrôle de l'opérateur.

8.6.2 Interactions entre les opérateurs et les procédures automatisées

La répartition des tâches entre les opérateurs et les systèmes informatisés doit reposer sur la CEI 61839, qu'on peut justifier sur la base de critères propres au projet considéré. Les PI doivent être conçues pour:

- informer en continu l'opérateur de ce qui est en cours de réalisation,
- permettre à l'opérateur de reprendre le contrôle manuel de la conduite à tout instant,
- informer l'opérateur de l'état des PI, par exemple lecture seule, exécution manuelle, exécution automatique, etc.,
- permettre à l'opérateur de relancer une exécution automatique après une interruption manuelle de la séquence,
- avertir l'opérateur de l'apparition d'un évènement inattendu qui peut empêcher le déroulement correct de la procédure. Il convient de mettre à disposition de l'opérateur les moyens qui permettent d'afficher les causes de la mise en garde.

Il convient de réfléchir à la mise en place de fonctionnalités supplémentaires, par exemple les PI peuvent permettre aux opérateurs de sélectionner les parties de la PI qu'ils souhaitent voir s'exécuter automatiquement.

8.6.3 Conception des PI pour conduire la tranche

Pour conduire la tranche à partir des PI, il faut qu'elles soient conçues pour:

- que les séquences automatiques commencent et se terminent dans la même procédure,
- que l'ordre de priorité entre les actions conduite d'une séquence d'une PI avec les autres actions de conduite ait été établi en cohérence avec les règles de priorité s'appliquant aux fonctions manuelles et automatiques,
- que les séquences soient prédéterminées et fixes. Elles peuvent comprendre des points d'arrêt nécessitant l'acquittement de l'opérateur,
- que la disponibilité d'un matériel ou d'un circuit s'il est nécessaire pour dérouler l'étape soit préalablement vérifiée,
- que les activités automatiques soient datées et archivées, aussi bien que les commandes manuelles opérateur.

Si certaines procédures ne peuvent pas être affichées sur les unités de visualisation, du fait qu'il y en a déjà trop d'affichées ou du fait qu'il n'y a pas assez d'unités de visualisation disponibles, il convient de mettre en place des mesures pour permettre le déroulement caché de procédure pour pouvoir:

- signaler des évènements significatifs ou donner l'alarme,
- donner un signe de vie périodique pour indiquer que ces procédures sont encore en cours d'exécution. De la même façon, certaines procédures peuvent être automatiquement arrêtées ou gelées suivant les spécifications des concepteurs,
- être affichée sur demande opérateur.

Il convient d'entreprendre durant la phase de conception les analyses permettant de démontrer que l'exploitation de la tranche n'est pas en péril même si certaines procédures ne sont pas affichées en permanence sur les unités de visualisation.

8.7 Autres fonctionnalités associées aux PI

Pour chaque type de procédure il convient de choisir différentes options concernant:

- la possibilité d'intégrer des notes préparées par les opérateurs dans les PI peut être fournie; ceci correspond à ce que les opérateurs ont l'habitude de faire sur les procédures papier. Ces notes peuvent être utilisées par exemple pour indiquer la nécessité de provisoirement s'écarter de la PI dans des conditions particulières qui doivent être détaillées,
- la possibilité de choisir les valeurs procédé pertinentes à surveiller peut aussi être offerte aux opérateurs,
- des fonctionnalités permettant de garder la trace de l'information et de l'archiver peuvent être fournies.

  Pour les situations de tranche rares, il peut être décidé d'enregistrer et d'archiver la façon dont a été gérée la situation en utilisant les PI dans un but d'analyse a postériori,
- une fonctionnalité d'enregistrement des activités.

  Un enregistrement automatique des actions lancées en fonction des étapes des PI peut présenter un intérêt,
- la possibilité d'adapter les recommandations en fonction de la situation peut être offerte de façon à offrir à l'opérateur le choix du niveau de recommandation adapté à ses capacités en fonction d'une PI ou de séquences particulières.

8.8 Documentation produite

Il convient que toutes les options définies conformément aux exigences de l'Article 8 soient documentées dans différents documents:

- une synthèse des options mises en œuvre, des raisons à l'origine de leur choix au niveau des phases de conception, de développement, de validation ou d'obtention des autorisations réglementaires,
- une synthèse pour les opérateurs. Il convient de la concevoir comme un document de rappel à utiliser facilement pour gérer les situations anormales de tranche,
- un document détaillé à utiliser comme lignes directrices pour la conception et la maintenance des PI.

Cette documentation doit être mise à jour en même temps que les PI sont modifiées pour assurer la cohérence et la complétude de l'ensemble.

9 Cycle de vie des PI

9.1 Généralités

Cet article établit des exigences et des recommandations pour l'ensemble du cycle de vie des PI, de l'organisation du projet à la maintenance des PI et à la formation des opérateurs; une attention particulière est portée à la vérification et la validation des PI.

9.2 Organisation du projet

Un projet d'informatisation des procédures touche à l'IHM, aux stratégies de conduite et au génie logiciel. Les aspects organisationnels relatifs à l'IHM et aux stratégies de conduite sont similaires à ceux rencontrés pour les procédures papier. Il convient que pour les aspects logiciels, si le système PI est classé important pour la sûreté, les exigences soient établies sur la base de la CEI 61513. On considère ici que le développement des PI est équivalent à n'importe quel développement logiciel que le système PI soit important pour la sûreté ou non.

Il convient que la première tâche soit l'organisation de l'équipe projet avec l'ensemble des compétences nécessaires et l'identification du comité décisionnel.

Sur la base de la politique PI, il convient que l'équipe projet assume les responsabilités pour ce qui concerne:

- la conception des procédures,
- le développement des procédures,
- la vérification et la validation,
- la revue et l'approbation des procédures,
- la révision des procédures.

Il convient d'utiliser des outils d'ingénierie pour garantir la qualité et la possibilité de garder la trace de l'information durant les phases d'un cycle de vie classique des procédures. Pour chaque phase du projet, l'informatisation est potentiellement un outil bénéfique qui peut faciliter la réalisation du travail à faire, en particulier pour garder trace de l'information relative aux différentes versions.

Il convient d'organiser des revues formelles dont les relevés de conclusion doivent être archivés.

9.3 Equipe projet

Il convient que des membres d'origines différentes soient rassemblés pour concevoir, développer, essayer et en particulier valider les PI:

- concepteurs de procédure,
- ergonomes,
- informaticiens, si nécessaires,
- représentants de toutes les catégories d'utilisateurs finaux, c'est-à-dire superviseur, opérateurs et éventuellement rondiers.

  Il convient de prendre en compte l'expérience des opérateurs et leurs besoins, en même temps que les possibilités liées à la flexibilité et à la capacité des affichages, lorsqu'on conçoit l'aspect externe des PI pour que celles-ci soient adoptées plus facilement par les opérateurs.

Il convient d'intégrer ces experts à l'équipe projet et il convient de travailler ensemble dès le début du projet.

9.4 Programme de vérification et de validation

On doit établir un programme de vérification et de validation pour garantir que pour chaque phase du développement, les exigences fournies aux Articles 6 et 8 sont satisfaites et pour préparer la vérification et la validation finale du produit complet.

La vérification des PI doit s'intéresser à la conformité des images affichées par rapport aux spécifications de l'IHM en même temps qu'aux aspects techniques qui font vivre les procédures.

La validation des PI doit couvrir en même temps les aspects fonctionnels et les aspects ergonomiques pour garantir que l'équipe d'opérateurs humains peut atteindre avec succès les objectifs de sûreté et d'exploitation en utilisant les PI.

Il convient de définir les stratégies de vérification et de validation dès les premières étapes du projet pour planifier les ressources qui seront nécessaires, c'est-à-dire personnel, outils logiciel. Il convient de prévoir des moyens suffisants pour conserver l'information.

9.5 Programmation des PI

Il convient d'évaluer en début du projet sur une maquette les options définies en 6.3 et 6.4 de façon à ne plus les remettre en cause au cours du développement des PI.

On doit développer un programme d'assurance qualité en prenant en compte le classement de sûreté du système PI pour vérifier que:

- les exigences contenues dans les Articles 6 à 8 sont correctement prises en compte,
- la traçabilité du développement est garantie,
- l'archivage des logiciels développés est réalisé régulièrement et que les fichiers de sauvegarde sont disponibles et fiables,
- la couverture de test est optimale et que la traçabilité et l'archivage des essais sont garantis,
- les versions sont correctement gérées.

Les exigences de la CEI 61513, de la CEI 60880 et de la CEI 62138 peuvent être applicables suivant la classe de sûreté du système PI correspondant aux PI.

9.6 Vérification et validation des PI

9.6.1 Généralités

Ce paragraphe traite de la vérification et de la validation des aspects techniques (fonctionnel procédé) et ergonomiques des PI, les évaluations relatives à la vérification et à la validation des aspects logiciel des PI ayant déjà été réalisées conformément aux exigences de sûreté et de qualité appropriées.

Une organisation qualité doit garantir que toute défaillance détectée est corrigée d'une façon satisfaisante et que la documentation est mise à jour.

9.6.2 Vérification technique des PI

Il convient que la vérification des PI ait pour objectif de détecter les erreurs dans l'application de 8.2, notamment pour ce qui concerne:

- l'utilisation de symboles, de mots, d'éléments graphiques non définis, etc.,
- les discordances entre les noms des valeurs et les informations affichées,
- les discordances entre le texte associé à une étape et les recommandations,
- les discordances entre le texte associé à une étape et la commande.

Il convient que l'objectif de la vérification soit la détection des erreurs de conception ou de programmation des procédures qui peuvent empêcher qu'un objectif de sûreté ou d'exploitation soit atteint, par exemple:

- des boucles sans fin dans la procédure,
- des inter-blocages, une information de la procédure B est attendue par la procédure A qui elle attend une information de la procédure B,
- les liens incorrects ou non définis pour des pages ou des étapes.

Il convient de mettre en place des mesures pour que la vérification technique des procédures:

- soit aussi exhaustive que techniquement raisonnable et possible,
- repose sur des méthodes et des outils qui minimisent les possibilités d'interprétation humaine ambigües,
- produise des résultats pouvant faire l'objet d'audits,
- soit tracée et facile à analyser,
- facilite le déroulement des essais de non-régression.

Pour détecter en même temps les erreurs applicatives et de programmation, une bonne pratique consiste à dérouler automatiquement toutes ou une parties des procédures de conduite sur la base d'un scénario enregistré sur un simulateur de procédé. Ces scénarii, comprenant des situations de tranche anormales, sont définis pour solliciter autant de fonctionnalités des PI que possible.

9.6.3 Validation ergonomique et fonctionnelle des PI

Il convient de réaliser la validation comme celle réalisée pour les procédures papier, avec une équipe complète de conduite et un simulateur pleine échelle pour simuler précisément tous les transitoires normaux et anormaux pour lesquels la conception des PI a prévu qu'elles soient utilisées.

Il convient que l'objectif visé par la validation fonctionnelle et ergonomique garantisse que:

- l'opérateur peut comprendre et appliquer les PI correctement,
- les PI aident l'opérateur à réaliser les fonctions prévues,

- aucune erreur ne subsiste non détectée au niveau des stratégies de conduite,
- les PI fiabilisent les actions opérateur et réduisent le risque que les opérateurs ne respectent pas les spécifications techniques,
- les opérateurs ont en permanence une bonne représentation du procédé et de leur progression au sein des procédures,
- la coordination de l'équipe de conduite est correcte,
- les opérateurs sont capables de surveiller le système PI et de détecter ses défaillances,
- les opérateurs sont capables de quitter la conduite sur le système PI et d'y revenir en utilisant l'ensemble des procédures de secours,
- l'apparence externe de l'interface des PI est compatible avec celle mise en œuvre côté système d'IHM.

Lors de la validation, certains aspects particuliers à l'informatisation doivent être couverts, à savoir:

- navigation entres les pages

  l'opérateur peut avoir des difficultés à comprendre quelle partie de la stratégie de conduite il est en train de suivre et à planifier ses prochaines actions en «feuilletant» les pages informatisées,

- "effet tunnel"

  l'opérateur peut perdre son aptitude à penser par lui-même, pour une raison ou pour une autre. Par exemple, l'opérateur a perdu de vue la stratégie de conduite et applique mécaniquement les PI ou alors une trop grande concentration mentale est nécessaire pour utiliser correctement les PI si bien qu'au bout d'un moment l'opérateur ne comprend plus leur contenu,

- charge mentale de l'opérateur

  il convient que l'opérateur soit capable de comprendre complètement et facilement l'état de la tranche et les implications associées aux actions proposées par les PI,

- communication entre les membres de l'équipe de conduite et éventuellement avec des personnes n'appartenant pas à l'équipe de conduite.

9.7 Déploiement des PI

Les PI sont mises en œuvre comme une application logiciel exécutée par un système logiciel indépendant de l'applicatif. Les recommandations suivantes font référence au déploiement de cette application logiciel. La modification du système logiciel du système PI induira généralement des contraintes qui ne sont pas couvertes ici.

Les PI doivent être déployés sous forme d'ensembles cohérents et bien identifiés. Un ensemble peut comprendre plusieurs types de procédures qui sont interdépendants.

Chaque ensemble doit être déployé en ligne en seul lot et sans impact sur l'exploitation de la tranche. Il convient que ces opérations soient très automatisées.

Pour déployer une nouvelle version des PI, on doit satisfaire aux conditions suivantes:

- les résultats des phases de vérification et de validation ont été pris en compte,
- les opérateurs ont été suffisamment formés et informés,
- si nécessaire, il est possible de réinstaller la vieille version des PI.

Pour simplifier la gestion sur site des PI, il convient de prendre en compte certains points particuliers durant les phases de conception et de développement des PI qui concernent:

- les fonctionnalités de gestion en ligne,

- les changements de version de PI pour lesquels il convient:
  - qu'ils soient faciles à mettre en œuvre, c'est-à-dire un processus très automatisé,
  - qu'ils ne demandent pas de changement d'état de la tranche,
  - qu'ils n'aient aucun impact sur l'exploitation de la tranche,
  - qu'ils n'aient aucun impact sur le système d'IHM, le cas échéant,
  - qu'ils n'aient aucun impact sur le logiciel système d'exploitation du système PI,
- l'archivage de vieilles versions des PI.

Pour chaque déploiement on doit garantir un niveau de qualité approprié, c'est-à-dire un traitement détaillé et de la traçabilité. Il convient que les déploiements trop fréquents de PI nouvellement développées ou révisées soient évités.

Avant de déployer une nouvelle version, toutes les équipes de conduite doivent avoir été formées à celle-ci.

Il convient que les incidents ainsi que les erreurs liés au système PI soient enregistrés et transmis rapidement à l'organisation en charge de la maintenance.

9.8 Documentation produite

Il convient d'utiliser la CEI 61513, la CEI 60880 et la CEI 62138 pour produire une documentation adaptée en ce qui concerne:

- l'organisation pour concevoir, développer et valider les PI, aussi bien que l'organisation de la maintenance des PI une fois celles-ci en exploitation, à partir de 9.3 et 9.4,
- tous les documents de programmation et ceux décrits en 9.5,
- les résultats de la vérification et de la validation des PI, voir 9.6,
- l'automatisation de la documentation pour faciliter le déroulement des essais de non-régression en cas de mise à jour des PI,
- la mise en service des PI, voir 9.7.

Une revue complète de la documentation produite conformément aux Articles 5 à 9 doit être menée pour s'assurer qu'elle est complète et cohérente.

9.9 Maintenance des PI et du système PI

La mise à jour des PI doit être préparée hors ligne et il convient de la planifier de la même façon que cela est fait pour les procédures papier.

Concernant la mise en place de révisions majeures, il convient de mettre en place des mesures qualité pour détecter le plus tôt possible les erreurs. Les opérateurs peuvent être impliqués dans la vérification des procédures.

Il convient que le système PI fournisse l'environnement de travail logiciel qui permet de charger les versions des PI sans modifications superflues au niveau des opérations de conduite assurées par le système PI.

La documentation chronologique pour l'exploitation, les réparations et la maintenance du système PI, si elle est autonome, doit faire l'objet de maintenance. Les logs d'exploitation et les rapports doivent faire l'objet d'évaluation à intervalle régulier pour identifier et mettre en place toutes activités de maintenance ou de modification nécessaires. Si le support des PI est le système d'IHM informatisé, la maintenance de ce dernier doit garantir la disponibilité et la fiabilité des PI.

NOTE Les exigences exactes portant sur la documentation dépendent de l'organisation opérationnelle particulière mise en place.

9.10 Formation de l'équipe de conduite

Les objectifs et l'organisation de la formation doivent être identiques à ceux mis en place pour des procédures papier. Il convient que les opérateurs qui ont participé aux phases de validation des PI aident à mettre en forme le programme de formation.

La formation doit en plus habituer l'opérateur à:

- conduire la tranche à partir des PI, le cas échéant,
- s'assurer périodiquement du bon fonctionnement du système PI, et détecter d'éventuelles défaillances,
- se replier sur le système de procédure de secours et les procédures de secours et conduire la tranche à partir de ces procédures de secours.

Lorsque des procédures de secours papier sont utilisées, la formation doit prendre en compte le manque d'habitude de s'en servir et le compenser.

Il convient de mettre en place des mesures pour collecter le retour d'expérience, et pour le capitaliser dans le but de s'en servir ultérieurement, par exemple pour mettre à jour les PI et pour améliorer la formation opérateur. Il convient que la collecte du retour d'expérience commence dès le début du projet. Il convient de faire particulièrement attention les premiers mois de conduite avec les PI.

Bibliographie

CEI 61226, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

CEI 62645[2], *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences de sécurité applicables aux programmes des systèmes programmés*

_____

2 A l'étude.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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