

TECHNICAL REPORT

RAPPORT TECHNIQUE

**Nuclear power plants – Instrumentation and control important to safety –
Guidance for the decision on modernization**

**Centrales nucléaires de puissance – Instrumentation et contrôle-commande
importants pour la sûreté – Guide pour décider d'une modernisation**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

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

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

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.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: csc@iec.ch

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00

TECHNICAL REPORT

RAPPORT TECHNIQUE

**Nuclear power plants – Instrumentation and control important to safety –
Guidance for the decision on modernization**

**Centrales nucléaires de puissance – Instrumentation et contrôle-commande
importants pour la sûreté – Guide pour décider d'une modernisation**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XA

ICS 27.120.20

ISBN 2-8318-1034-0

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope and object.....	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviations	11
5 Motivation for modernization.....	12
5.1 General.....	12
5.2 Economic motivating factors	12
5.2.1 General	12
5.2.2 Cost reductions	12
5.2.3 Revenue.....	13
5.2.4 Economically motivated modernization	13
5.3 Safety motivating factors	14
5.4 Summary of motivations for modernization	14
6 Modernization decision overview	14
6.1 I&C life cycle	14
6.2 Long-term I&C strategy	17
6.2.1 General	17
6.2.2 Preliminary evaluation of I&C systems status and future needs	17
6.2.3 Renewing/upgrade priority for I&C systems	18
6.2.4 Budget boundary conditions	18
6.2.5 Evaluation of different modernization scenarios	18
6.3 Feasibility studies.....	19
6.3.1 General	19
6.3.2 Evaluation of plant related preconditions and goals	19
6.3.3 Licensing.....	20
6.3.4 Preliminary budget costs	21
6.3.5 Implementation strategy	21
6.3.6 Evaluation of as-built documentation	22
6.3.7 Basic requirement specification	23
6.3.8 Function allocation	24
6.3.9 Function and task analysis for the HMI	24
6.3.10 Data management	25
6.3.11 Design tools	25
6.4 Tender specification and purchasing of the individual systems	26
6.4.1 General	26
6.4.2 Specification of I&C system properties for candidate solutions	26
6.4.3 Specification of requirements for quotations	27
6.4.4 Tenders for each system	27
6.4.5 Order placement.....	27
7 Considerations for modernization	28
7.1 General.....	28
7.2 Technology considerations	28
7.3 Economic considerations.....	29
7.4 Regulatory codes and standards	30

7.5	Company policy and engineering standards.....	30
7.6	Safety and process control system future needs.....	30
7.7	I&C system reliability.....	32
7.8	Risks and benefit study	32
7.9	Safety classification	33
7.10	Equipment qualification requirements	33
7.11	Software qualification requirements.....	34
7.12	Physical constraints	35
7.13	Equipment availability (delivery and support).....	35
7.14	Human factors	35
7.15	Defence-in-Depth and Diversity analysis (3D analysis).....	37
7.16	Separation and protection against fire and flooding	38
7.17	Uncertainty and set point calculation	38
7.18	Response time analysis.....	38
7.19	Test procedures	38
7.20	Documentation management	39
7.21	Update of plant technical documentation	40
7.22	Training and staff qualification.....	40
7.23	Project organization	41
7.24	Configuration management.....	41
7.25	Interfaces to the other existing systems.....	41
7.26	Standardisation	42
8	Implementation.....	42
8.1	General remarks.....	42
8.2	Target architecture	42
8.3	Sequence of upgrading steps	43
8.3.1	General	43
8.3.2	One large versus several small work packages.....	44
8.3.3	Definition of work packages	44
8.3.4	Parallel operation and replacing equipment at power	45
8.3.5	Sequence of work packages	45
9	Recommendations	46
	Bibliography.....	48
	Figure 1 – IEC 62096 structure	8
	Table 1 – I&C life cycle phases	16

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GUIDANCE FOR THE DECISION ON MODERNIZATION

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62096, which is a technical report, has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 2002.

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

- update on the format to align with the current IEC/ISO directives on style of documents;
- update on references, taking into account Standards published since the first edition;
- update on the terminology;

- incorporation of a number of clarifications proposed by National Committees.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
45A/711/DTR	45A/726/RVC

Full information on the voting for the approval of this technical report 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 maintenance result 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.

INTRODUCTION

a) Technical background, main issues and organisation of this Technical Report

Normal procedures for evaluation of plant safety, operations and maintenance provide information about potential needs for renewal or upgrades. After many years of operation, the Instrumentation & Control (I&C) systems may no longer fulfil actual or anticipated safety requirements, may be obsolete or unreliable, or may no longer be fit for required lifetime extensions. In such cases, modernization provides the way forward to adapt the I&C systems to meet the requirements or to deal with the problems and costs caused by the obsolescence or aging of the equipment. During modernization, the benefits offered by modern I&C equipment can be evaluated.

It is intended that this Technical Report be used by operators of NPPs (utilities), systems evaluators and by licensors.

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

IEC 62096, as a Technical Report, is the fourth level IEC SC 45A document tackling the issue of guidance for decision for modernisation.

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

c) Recommendations and limitations regarding the application of this Technical Report

There are no particular recommendations, neither limitations regarding the use of this Technical Report.

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 and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate

consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO standards, as well as to IAEA 50-C-QA (now replaced by IAEA GS-R-3) 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.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GUIDANCE FOR THE DECISION ON MODERNIZATION

1 Scope and object

This technical report is intended to support owners of an NPP in the decision-making process and in the preparation for partial or complete modernization of the I&C. For this, it provides:

- a summary of the motivating factors for I&C modernization,
- the principal options for the elaboration of different scenarios for I&C modernization,
- the technical and economic criteria for the selection of a long term I&C strategy,
- the principal aspects to be taken into account for a detailed technical feasibility study.

In addition, this report contains detailed recommendations and practical advice for:

- the technical evaluation of the actual status of the I&C systems,
- the content of the I&C system requirement specification and for the project management following the guidance given in IAEA TECDOC 1016 and 1066,
- considerations on modernization strategy.

Special attention is paid to the improvement of reactor safety and of the human machine interface. The report does not provide I&C design requirements. For these it is assumed that the IAEA Codes and Guides are used as top level documents while IEC publications are mainly used for system design, requirements on equipment and some work methods. IAEA Reports and other documents are referenced to give information that is more detailed on specific areas.

The structure of the report is given in Figure 1. The recommended sequence is, first, to summarize the more easily obtained motivations (Clause 5) and then establish a project that works in structured and more and more detailed steps: Long term I&C strategy – Feasibility studies – Tender specification and order (Clause 6). Clauses 7 and 8 may be used as checklists during each step.

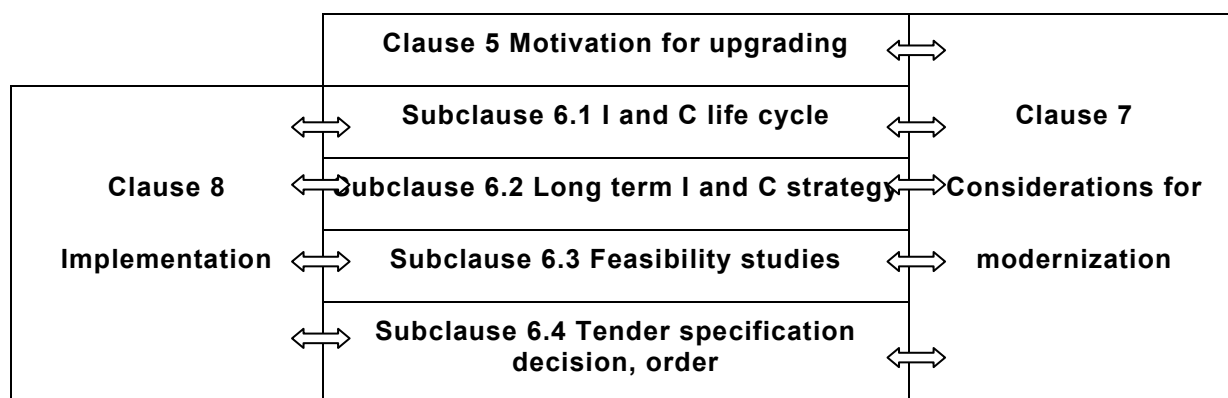


Figure 1 – IEC 62096 structure

IEC 437/09

2 Normative references

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

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60300-3-3:2004, *Dependability management – Part 3-3: Application guide – Life cycle costing*

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

IEC 60880:2006, *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 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

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

IEC 61888, *Nuclear power plants – Instrumentation important to safety – Determination and maintenance of trip setpoints*

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

IEC 62342:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing*

IAEA-TECDOC-1066:1999, *Specification of requirements for upgrades using digital instrument and control systems* (only available in English)

IAEA-TECDOC 1147:2000, *Management of aging of I&C equipment in nuclear power plants* (only available in English)

IAEA:2007, *IAEA safety glossary terminology used in nuclear safety and radiation protection*

3 Terms and definitions

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

3.1 availability

the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

[IEV 191-02-05]

NOTE This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance.

3.2 configuration management

the process of identifying and documenting the characteristics of a facility's structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation

[IAEA Safety Glossary, 2007]

3.3

Human Machine Interface

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

[IEC 60964, 3.13]

3.4

I&C system

system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources

[IEC 60964, 3.14]

3.5

life cycle

time interval between a product's conception and its disposal

[IEC 60300-3-3, 3.1]

3.6

life cycle cost

cumulative cost of product over its life cycle

[IEC 60300-3-3, 3.3]

3.7

maintainability

probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval, when the maintenance is performed under stated conditions and using stated procedures and resources.

[IEV 191-02-07, modified]

3.8

modernization

replacement or upgrading with newer systems and components. Replacement is the term to be used when there is no change in requirements; upgrading is the term to be used when the level of requirements increases

NOTE 1 Backfit, refit, retrofit, refurbish and upgrade are similar terms which are often used interchangeably – They only differ in shades of meaning (IAEA-TECDOC-1066).Upgrading also includes the implementation of new functionality.

NOTE 2 Replace and renew are similar and often interchangeable. The terms are used from a single component up to the complete I&C.

[IEC 62342, 3.10]

3.9

nuclear safety

achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards

NOTE Often abbreviated to safety in Agency publications on nuclear safety, particularly when other types of safety (e.g. fire safety, conventional industrial safety) are being discussed.

[IAEA Safety Glossary, 2007]

3.10 requirements

expression in the content of a document conveying criteria to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted

[ISO/IEC Directives, part 2, 2004, 3.12.1]

NOTE 1 In IEC/SC 45A documents the following types of requirement are distinguished:

Safety requirements – Requirements imposed by authorities on the safety of the NPP in terms of impact on individuals, society and environment during the NPP lifecycle.

Functional and performance requirements – Functional requirements state what actions the system must take in response to specific signals or conditions, and performance requirements define features such as response times and accuracy.

Operational requirements – Requirements on the operational capacity and ability of the plant imposed by the owner.

Plant design requirements – Technical requirements on plant general design for the fulfillment of the safety requirements and operational requirements on the plant.

System design requirements – Design requirements on individual systems to give a design of the complete plant fulfilling the plant design requirements.

Equipment requirements – Requirements on individual equipment for its fulfillment of the demands of the system design.

NOTE 2 The IAEA Safety glossary (2007) contains the following definition:

Required, requirement – Required by (national or international) law or regulations, or by IAEA Safety Fundamentals or Safety requirements.

The requirements aimed at by this IAEA definition are the same designated by the IEC/SC 45A definition "Safety requirement".

3.11 specification

document that specifies, in a complete, precise, verifiable manner, the requirements, design, behaviour, or other characteristics of a system or component and, often the procedures for determining whether these provisions have been satisfied

[IEC 60880, 3.39]

4 Abbreviations

CAD	Computer Aided Design
CDF	Core Damage Frequency
CMF	Common Mode Failure
DBA	Design Basis Accident
DCS	Distributed Control System
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

FAT	Factory Acceptance Tests
HMI	Human Machine Interface
I/O	Input/Output
I&C	Instrumentation & Control
LOCA	Loss Of Coolant Accident
O&M	Operation & Maintenance
PAM	Post Accident Monitoring
PLC	Programable Logic Controller
PSA	Probabilistic Safety Assessment
SAT	Site Acceptance Tests
SCC	Station Control Computer
SW V&V	Software Verification&Validation
VDU	Visual Display Unit
3D analysis	Defence-in-Depth and Diversity analysis

5 Motivation for modernization

5.1 General

The motivating factors for modernization can be considered under two headings according to the main benefits: economic and safety. The replacement of I&C equipment with a more modern equivalent usually leads to increased functionality and performance improvements, but it is likely that most upgrades are primarily motivated by problems with the old equipment rather than the perceived benefits of the new.

5.2 Economic motivating factors

5.2.1 General

The economic yield should be optimised using a life-cycle costing approach, taking into account not only lower costs but also increased production.

5.2.2 Cost reductions

Cost reductions can be achieved in the following areas:

- Operating costs can be reduced through efficiency improvements leading to savings in fuel, power consumption, consumables, or operational manpower requirements.
- Maintenance costs can be reduced by extending maintenance intervals and/or reducing the time and effort required for maintenance tasks. Improvements in the reliability of equipment reduce the cost of repair work and spares inventory. Also the reduction of the number of equipment families by the use of a single system platform may lead to a

reduced spare parts inventory. In some cases, high redundancy design can allow preventive maintenance during normal operation.

- Administration costs can be reduced through improvements in the way in which information is collected, processed, stored, and presented.

Cost reductions should be considered using a life-cycle costing approach focused on minimizing the total cost of the system over its intended life cycle. Note that a modernization with an expensive type of component with high reliability may increase the procurement cost but reduce the long-term support cost, and may give the lowest overall life cycle cost.

5.2.3 Revenue

Revenue can be increased in the following ways:

- Higher generation level
Improvements in monitoring and protection systems can give greater confidence in plant status, allowing reduction of safety margins at the same plant safety level and more power output.
- Increased availability
Shorter shutdowns for repairs, routine maintenance and fuelling, and a lower probability of spurious trips result in better plant utilisation. This can be achieved through improvements in reliability and stability, and through the use of 'smart' systems with capabilities for self-checking, diagnostics and auto-calibration, and improved operator support by HMI and I&C functions. The upgrading of obsolete equipment reduces the probability of a prolonged shutdown due to the unavailability of replacement parts.
- Increased plant lifetime
If the operation of the plant can be extended beyond its planned economic lifetime, there is a considerable benefit in accounting terms, because the revenue is no longer offset by capital charges. It is necessary to modernize any equipment or systems whose predicted residual life will be insufficient for the planned plant life extension.

5.2.4 Economically motivated modernization

Economically motivated modernization may be initiated by one or more of the following factors:

- Obsolescence
Equipment obsolescence occurs towards the end of a product's life cycle. When an item of equipment is no longer in production, the level of service available from the manufacturer decreases, and spare parts and consumables become unavailable or unacceptably expensive. Obsolescence also occurs at the electronic component level, where life cycles can be as short as a few years.
The initial effect of obsolescence is to increase timescales and costs for maintenance and repair work. Ultimately the equipment will be rendered unserviceable by the non-availability of spare parts.
- Competence of personnel
A related problem is the decreasing availability of suitably skilled maintenance personnel. Recently trained personnel do not have the required skills for analogue electronics. Technical education and training courses tend to concentrate on digital technology.
- Aging
The aging effects suffered by electronic components and assemblies can lead to problems with noise, drift, response time, EMI susceptibility, and general reduced reliability.
Examples of degradation due to aging include:
 - chemical effects such as oxidation or corrosion, which lead to high resistance contacts in connectors, switches and solder joints,
 - drying out of electrolytic capacitors,

- loss of insulation due to the build-up of surface contamination (particularly in high-voltage equipment),
- cables and other components made from organic material are subject to aging effects (e.g. embrittlement) when exposed to temperature, radiation, oxygen, etc,
- mechanical effects such as wear, seizure, and loss of spring tension, all of which eventually lead to the failure of mechanisms in switches, connectors, relays, etc.
- Compatibility issues

It is sometimes necessary to upgrade equipment which would otherwise be considered satisfactory because of the effects of changes elsewhere. The following are examples of compatibility issues:

 - changes to reactor or process equipment resulting in differing I&C requirements,
 - changes to other I&C equipment using newer interfacing connections or protocols.
- Operational issues

I&C modernisation may become necessary to implement changes in operational requirements, such as a change from 'base load' to 'load following'.

5.3 Safety motivating factors

A safety improvement upgrade may become necessary to comply with regulatory requirements. Such an upgrade may have a significant cost and no apparent economic benefits. Nevertheless, the decision is ultimately an economic one where the plant owner should compare the costs of performing the upgrade versus the costs associated with operating restrictions on the plant.

Safety improvement upgrades may be initiated by one or more of the following:

- recommendations of a safety review,
- changes in licensing requirements,
- deficiencies revealed by an incident or reportable occurrence,
- deficiencies revealed by testing.

5.4 Summary of motivations for modernization

A report should be written summarizing the various aspects of modernization for use in the decision on future actions. Where possible, the report includes a cost benefit analysis where each argument can be quantified. Clause 7 may be used as a checklist for defining the most important aspects. When a decision is taken to investigate and define a modernization, the I&C lifecycle description in Clause 6 should be followed.

6 Modernization decision overview

6.1 I&C life cycle

A reference life cycle should be established for the modernization project, and a suggested outline for a lifecycle is given by Table 1.

Based on the input from Clause 5 on motivation for modernization this subclause focuses on the life cycle for modernization. With reference to the IAEA-TECDOC-1066, which mainly addresses the potential suppliers of nuclear plant services, this technical report addresses just those life cycle phases which require specific activities from the NPP utilities. Table 1 gives in close co-relation to IAEA-TECDOC-1066 an overview of all life cycle phases of I&C systems.

This subclause focuses on the phases which determine the strategy for modernization and the tender process up to the point where any necessary new equipment or plant I&C changes are ordered (1 to 3 in Table 1). The life cycle phases described are:

- 6.2 Long- term I&C strategy,
- 6.3 Feasibility studies,
- 6.4 Tender specification and purchasing of the individual systems.

In Clause 7, Considerations for modernization, and clause 8, Implementation, more details are described for use when applicable in the appropriate subclauses .

Table 1 – I&C life cycle phases
(see also Table XI of IAEA-TECDOC-1066)

I&C life cycle phases		IEC/TR 62096
Generic modernization strategy	Relating actions, results, plans	
1 Long-term I&C strategy to meet the needs for plant operation	Evaluation of I&C systems status Renewing/upgrade priorities Budgetary boundary conditions Different modernization scenarios	
2 Feasibility studies	A. Generic feasibility studies – Plant related preconditions and goals – Licensing – Preliminary budget costs – Implementation strategy – I&C architecture – Sequence of modernization steps	
	B. Studies of technical feasibility aspects – Evaluation of as-built documentation – Basic requirements specification – Function allocation – Function and task analysis for HMI – Data collection and design goals	
Modernization phases of individual systems	Relating actions	
3 Tender specification and purchasing of individual systems or complete I&C	Specification of I&C properties Specification of requirements Suppliers' tenders Order to the supplier	
4 Specification of the individual I&C systems	Validated specification and plans on: System validation (FAT & SAT) System operation and maintenance Staff training	
5 System realization Detail design of individual I&C systems Manufacturing and system integration	Detailed manufacturing and installation documentation and operating and maintenance manuals System ready for tests	
6 Factory acceptance test (FAT)	System ready for shipment to site FAT test report	
Plant related phases		
7 Installation and setting to work of the individual systems	Start of system failure reporting	

Table 1 (continued)

I&C life cycle phases	
8 Training and contractual documents	All contractual documents provided
9 Site acceptance test (SAT) and commissioning with plant	System ready for operation SAT test report
10 Operation and maintenance	Continued system failure reporting Reporting of the result of routine tests Simulator upgrading Operator training
11 Decommissioning	Decommissioning plans Replacement strategies Disposal of system

6.2 Long-term I&C strategy

6.2.1 General

A long-term I&C strategy ensures the planning of the long-term maintenance of all I&C functions necessary for plant operation. The utility's overall strategy, objectives, financial situation and operational plans affect the modernization programme. These strategic factors influence the more detailed work of preliminary evaluations and set the goals for detailed feasibility studies. The preliminary evaluation should suitably identify these factors.

6.2.2 Preliminary evaluation of I&C systems status and future needs

A preliminary evaluation of the potential for modernization should be made. This should discuss the basic reasons for requiring modernization work, the goals of that work, and the main expected impact on operation, safety and efficiency, giving the expected benefits and budget costs.

Essential inputs can be derived from the long-term operation and maintenance history of the individual I&C systems:

- failure records give details of specific failure modes, specific fault levels and quantified failure rates,
- the experience of I&C faults and the respective potential consequences on power generation,
- yearly man-hour records for maintenance and repair work together with procurement records for spare and replacement parts form an economical base line, documenting the trend of rising difficulties in the procurement of obsolete spare parts and the repair of faulty, obsolete I&C systems,
- declining competence of the utility staff and suppliers with the present I&C systems.

An overview of the records of the above criteria in correlation with the intended time schedule for further plant operation gives the basis for the scope of I&C systems which should be considered for potential modernization and the relative priority between different I&C systems.

Additionally it should be considered that in the case of faults in safety or safety-related I&C systems, specific reports may be required by the licensing authority, even if these faults did not directly or indirectly cause a safety threat or hazard.

The I&C should be reviewed for compliance with the current safety requirements and expected future safety requirements. For future safety requirements, there should be

strategic/planning decisions taken at a high organizational level. These safety requirements and any safety reviews of the plant or of similar plants of the same reactor family (such as those made by IAEA) should be used as an input to the preliminary evaluation of requirements.

The functionality of the I&C should be evaluated from the point of view of the operators and the operation management, and the need for improvements should be stated in the evaluation summary.

It should be understood from the beginning that the process leading to a firm decision on a certain scope for modernization requires an iterative procedure. This is because the costs for any modernization project will only be properly determined from an inquiry and bidding process, and should be compared with the budgetary framework which depends on the economics of the plant.

6.2.3 Renewing/upgrade priority for I&C systems

The status evaluation of the I&C systems also gives the first indications of the priority to renew or to upgrade the individual I&C systems. Generally the I&C systems under discussion are grouped according to their priority (i.e. which I&C systems “must”, “should” or “may” be renewed or upgraded in the coming years). This forms an essential input for the generic feasibility study. The detailed upgrade sequence for these I&C systems results from the technical feasibility studies such that

- technical plans are produced for the installation, commissioning and operation of the I&C systems concerned,
- intermediate system configurations that allow plant operation and are licensable, and
- the costs for temporary installations of systems or interfaces are minimized.

More detailed considerations about the *need* to perform a modernization are found in Clause 7 whereas Clause 8 provides more details on the *optimization* of the modernization sequence.

6.2.4 Budget boundary conditions

The budgetary framework for I&C renewal and upgrading results from consideration of:

- the time span for intended further plant operation,
- the scope of I&C systems with high renewing/upgrade priority (“must”-systems),
- the yearly costs to maintain the existing I&C systems.

6.2.5 Evaluation of different modernization scenarios

The decision to include the renewal or upgrading of ‘should-’ or ‘may-’ systems is made by considering the marginal costs of these systems and the additional benefits that the renewal or upgrading would bring.

Based on the evaluations from previous subclauses, possible options for future I&C structure and technology should be defined. The content may be I&C structure, platform structure, distributed systems, or a mix of digital and analogue and relay-based technology.

The long term I&C strategy should be based on a thorough economical evaluation of a number of scenarios related to different options. These depend strongly on the anticipated lifetime of the plant.

The evaluation should consider different lifetime perspectives (if adequate) with:

- no modernization at all, or
- only modernization of “must” systems, or
- modernization of “must”, “should” and “may” systems.

The evaluation should also consider:

- staged modernization of the relevant systems, or
- one-step modernization

This evaluation should take into account:

- the anticipated operation and maintenance costs of the retained systems,
- the anticipated modernization costs,
- the anticipated operation and maintenance costs for the new systems,
- the lifetime of the new systems,
- the economic evaluation of the risks linked to plant availability or license due to failures caused by equipment aging and obsolescence,
- other aspects associated with the modernization (see 7.8, Risks and benefit study).

One or two optimal scenarios will result from this evaluation. They are considered candidates for the long term I&C strategy. They should be analyzed in more detail in subsequent feasibility studies. Since the evaluations can at that time only be made on the basis of preliminary cost estimations for modernization, the selected scenarios should be later reviewed based on formal tenders; therefore possibly some iterations may be necessary.

6.3 Feasibility studies

6.3.1 General

Where the long-term I&C strategy demonstrates the need to renew or technically upgrade a certain scope of I&C systems, *feasibility studies* should be started.

Preferably the total scope of tasks to be evaluated during the feasibility studies should be structured into two blocks:

- the *generic* feasibility studies (see 6.3.2 – 6.3.5) should identify which systems and which time frames are intended for the renewal/upgrading projects,
- the *subsequent* feasibility studies should focus primarily on the technical aspects of the feasibility (see 6.3.6 – 6.3.11).

The long-term I&C strategy should be evaluated mainly by the utility staff, possibly with support from consultants. A relatively large and competent technical organization is necessary to deal with the quantity of work and the depth of information required in the feasibility studies. If such an organization is not available to the plant operator, the task may be evaluated by potential suppliers working in close contact with the staff of the utility. For optimal feasibility study results, a joint team comprising utility staff together with personnel from a potential supplier is recommended. The negative aspect is that over-reliance on a single supplier may commit the utility to that supplier, which can affect the costs. To avoid premature commitment to a specific supplier, the utility should consider the possibility of commissioning feasibility studies from two or more suppliers in parallel.

6.3.2 Evaluation of plant related preconditions and goals

The main objective of this activity is to identify and specify the overall goals for the renewal or upgrade of the I&C system. Normally, the utility is in the best position to identify these goals which form the essential inputs to the feasibility studies.

The list of goals may include the following:

- to maintain or increase safety,
- to maintain or increase plant capacity and/or load factor,
- to simplify plant maintenance,

- to define acceptable availability (reliability, maintainability and maintenance support) in relation to the I&C life cycle cost,
- to ensure staff competence with currently installed older items of equipment.

With the focus on those I&C systems to be modernized, the technical conditions for the intended renewal/upgrades should be analysed:

- key properties and physical space available and needed for possible products,
- the available capacity of electrical supplies and other services, and
- product reviews, to identify suitable I&C technologies and equipment families/suppliers with respect to:
 - interfaces to the existing I&C systems which should be maintained,
 - requirements and capability of service personnel,
 - references according to the required licensing level,
 - the HMI (see 6.3.9 and 7.14),
 - previous experience with similar modernization projects,
 - optimisation of balance between new and old equipment,
- the expectations for the future supply of spare parts,
- system support from the supplier,
- the status of as-built documentation.

When considering upgrading and renewing the current I&C system, the following human resources should be considered:

- availability of qualified design personnel to engineer the modernized system,
- availability of qualified personnel to install and commission the modernized system,
- availability of qualified personnel to operate and maintain the modernized system.

6.3.3 Licensing

Licensing considerations can have an important influence on the modernization project. In most countries, the licensee should give prior information to the safety authorities for all modifications to systems and equipment classified as important to safety. The methods for doing this which have been agreed with the safety authorities may well already exist. However, legal requirements specifically related to I&C modernization may well not exist or still be in the stages of development. The regulatory authorities should be kept informed from the start of the project planning. Even if the scope of the modernization is not directly related to safety, the utility should investigate any potential impact of the planned modernization on safety in the anticipated areas of change.

In order to define all the licensing issues that will be considered for the modernization project, a preliminary safety case document should be prepared and agreed by the licensing authority at the earliest possible stage of the project.

The safety case is the licensee's documented demonstration that:

- the correctness and completeness of the overall requirement specification are justified in relation to the intended system's functions,
- the system is developed to a standard compatible with the safety importance of the application,
- the delivered system satisfies all aspects of its requirement specification,
- adequate means and arrangements are specified, which ensure the required performance of the system throughout its operational life,
- the system fits its intended purpose.

(See bibliography for more information about what may be needed for the safety demonstration.)

With a clear definition of the scope and the required methodology, the overall licensing effort required to meet the regulator's expectations can be assessed, and it should be possible to minimise or eliminate the risks associated with meeting emerging licensing requirements.

A complete set of design requirements for the I&C should be established and validated as early as possible. The existing plant safety analysis may need to be updated. The plant I&C system should be examined for safety and operational margins not explicitly described in existing documentation, and the findings recorded. A revision of the PSA may be needed for the upgraded system.

In preparing the licensing procedure, the utility should take into account the experience of its authority with the licensing of digital safety I&C. The effort required for the safety demonstration may vary if:

- the authority already has experience with the assessment of digital safety I&C systems, or
- licensing experience of comparable applications in other countries may be transposed to a certain degree, or
- the anticipated systems have already been designed or pre-qualified with the safety issues with respect to common standards and requirements, or
- the system has already been assessed by a regulator.

Where novel solutions are proposed, the utility should be prepared to supply specific justifications.

6.3.4 Preliminary budget costs

To ensure a successful modernization, it is essential that the scope of I&C systems to be upgraded or renewed is defined in line with the budgetary framework. This generally requires an iterative procedure. It is helpful to include a preliminary price-limit as one of the inputs to the feasibility studies, because this is a key factor for possible solutions. The budget should include allowances for any high-cost supplementary item, such as training simulators and software V&V.

Of course the basis for a contractually binding offer requires a detailed scope of deliverables and services. A prime objective of the feasibility studies is to evaluate the budget costs as a basis for the tender process.

Typical costs include:

- capital and equipment costs,
- re-engineering and detailed engineering implementation cost (see 6.3.6 and 7.21),
- dismantling, installation and commissioning costs,
- operating and maintenance costs of the modernized system,
- documentation and training costs for operational and maintenance personnel,
- replacement cost of power generation loss during the I&C system modernization outage period.

6.3.5 Implementation strategy

6.3.5.1 General

The implementation strategy to be applied should be stipulated in sufficient detail to allow the technical and economical impact of alternative approaches to be considered.

The strategy should contain requirements for operation and for supportability. Reactor and turbine I&C may require differing strategies. If a large amount of the existing cabling cannot be used because of aging, mechanical damage, etc, greater changes to architecture and strategy should be considered.

The two main elements affecting the choice of implementation strategy are:

- definition of the overall I&C architecture, and
- definition of the sequence of renewal/upgrading steps, with special emphasis on the definition of interfaces to the remaining equipment, and minimization of plant outages.

6.3.5.2 Overall I&C architecture

The definition of the overall architecture has to take account of the revised plant general design and the total scope of all I&C systems, including existing systems which will remain in service as well as those which will be modernized. Inputs for this activity are the as-built architecture in conjunction with the safety categorization of the I&C functions, together with (in a first step) a coarse subdivision of the I&C into functional complexes, and a subdivision of the I&C systems to be replaced according to their priorities.

This allows a break-down of the overall I&C into several units, each having common characteristics, and a preliminary allocation of I&C functions to I&C systems, which ensures that each system:

- can provide adequate equipment performance,
- is subject to consistent licensing and qualification requirements.

This approach also supports the requirements of a "defence in depth" approach, or requirements for diversity with respect to a common plant safety objective.

6.3.5.3 Sequence of modernization

The second element of the implementation strategy is the optimal sequence of implementation of the I&C modernization. It has to consider the different priorities of the systems to be replaced, as well as the boundary conditions to be considered in the project. This will decide whether to modernize all systems in one step, or to split the installation over several outages. Typical criteria to be considered are:

- the possibility of identifying subsystems which can be separated without the need for intermediate interfaces,
- the possibility of carrying out preparatory work or performing installations during power operation,
- the possibility to synchronising the renewal with the modernization of mechanical or electrical systems,
- manpower on site,
- economics, including cash-flow considerations.

The feasibility study does not necessarily need to identify the optimal implementation sequence; however, it should stipulate the possible alternatives so as to allow a first assessment of their economical and technical impact on the overall project. The detailed implementation sequence needs to be elaborated only in a later phase when the supplier has been selected and when the detailed properties of the new I&C system are known. Clause 8, Implementation strategy, provides additional guidance for both phases.

6.3.6 Evaluation of as-built documentation

This step in the feasibility studies serves as preparation for evaluation of the requirement specification, as well as to provide input for the request for tenders.

A design basis review which covers functional and physical requirements and the licensing basis should be carried out. Any changes or deviations from the existing design basis should be identified with respect to the modernization. The design basis should be kept the same as the existing basis, unless an upgrading of the design basis is necessary due to new licensing requirements, new equipment specifications or future needs foreseen by the utility. The review should also ensure that the modernization does not degrade the current design basis. Special attention should be given to functions with fail-safe designs.

The review should verify that all necessary as-built documentation is available and correct. If this is not the case, then, the review should provide means and actions to compensate. Plant walk-downs may be used to field-verify documents, and often reveal important features which are not apparent from the documentation.

In this context, the main documentation of interest is:

- system design requirements, equipment data, past operating experience, and past engineering change notices (modifications),
- safety reports,
- design specifications on functionality,
- functional diagrams,
- set points,
- accuracy,
- time constants and tolerable delay times,
- process parameters,
- lists of signals (analogue and contacts),
- processing algorithms, with operational and functional logic diagrams and definitions,
- qualification requirements,
- cabinet wiring diagrams and connection schedules,
- cable routing diagrams,
- design specifications for the HMI,
- arrangement drawings of indications and controls for the main control room and the remote shut-down station,
- design specifications for the process information system,
- operating procedures.

6.3.7 Basic requirement specification

Design basis events, postulated initiating events and following event sequences, should be considered when preparing the basic requirement specification. Beyond-design-basis accidents (BDBA) and severe accidents should also be considered to the extent practicable.

The basic requirements are based firstly on the original design specifications and the as-built documentation. Secondly, the requirements and recommendations resulting from the above-mentioned studies should be considered.

These reflect to a large extent the operational experience since the commissioning of the plant, but also the expected benefits and features linked to the new I&C, such as signal fault treatment, handling of signal quality codes, digital filtering, remote calibration and diagnostic features.

In the case of planned functional upgrades, special care should be given to the availability of adequate measurements and actuators.

For the safety-related I&C, any functional upgrades or extended features will be included in the safety demonstration, and their validity will should be justified.

The basic requirement specification should contain sufficient information on the following topics:

- general requirements,
- functional requirements,
- equipment requirements, including environmental and seismic requirements,
- scope of functions and equipment,
- interfaces (standard signals, unusual types, types of serial interfaces, etc),
- installation requirements,
- others.

This suggested content is expanded in subclause 7.5 and detailed guidance is given in IEC 61513 on the development of the system architecture and function allocation.

A reference form of specification is also given in IAEA-TECDOC-1066.

6.3.8 Function allocation

Based on the results of the previous design steps, the identified functions are allocated to I&C systems and their sub-functions are allocated to subsystems within the total I&C architecture. The main activities of this design step are:

- to ensure that the functional scope of each subsystem is met by an adequate equipment performance,
- to ensure that the assignment of functions to independent I&C systems meets the requirements for 'defence in depth' or that the functions are diverse with respect to a common plant safety objective,
- the assignments of tasks to operating and maintenance staff.

6.3.9 Function and task analysis for the HMI

The basic requirement specification leads to the assignment of functions to operators and I&C systems. In cases where the function assignment deviates from that of the existing I&C design i.e.

- changed degree of automation,
- introduction of additional systems,
- changes to the concept for periodic tests and other operator tasks,
- transition to VDU display based operation,
- re-arrangement of control boards,

a task analysis should be performed as the basis for the detailed specification of the HMI. This analysis should not only take into account process control tasks, but also the operator's role with respect to maintenance tasks, maintenance of I&C systems, communication tasks etc. as far as these are influenced by the scope of I&C modernization.

The task analysis should then result in:

- operator information requirements,
- operator action requirements,
- requirements on communication between shift members,
- requirements concerning reach, sight, distance, frequency of use, etc.

The depth and scope of the analysis should be commensurate with the extent of the I&C modernization, and the degree of similarity of the existing and the new HMI. In case of minor modifications, the analysis might then be restricted to an assessment of the area of change, and an assessment of the absence of negative impact on unmodified features, whereas a major modification may require a complete re-assessment of operator tasks.

This analysis provides a sound basis for the specification of:

- the arrangement of displays in the control room (for final design and intermediate stages),
- the contents, formats and design of VDU displays,
- information processing for the presentation of system status information, including any additional operator support systems,
- the necessary adaptation of existing operating procedures to suit the modified HMI and the new functions.

The task analysis should also be used to identify work situations having a potentially high workload and risk of operator error, to be studied in more detail in a later set of validation case studies. These will then allow verification of workload acceptability, and of the adequacy of the finally designed HMI.

The selection of operating situations to be analysed, and the analysis of different scenarios considered in the task analysis should be done with the help of safety and process engineers.

6.3.10 Data management

To ensure consistency and availability of all design data for the complete life cycle of an I&C system, it is essential, soon after the start of the project, to plan the introduction and installation of a powerful database system, to hold all project information on sensors, actuators and other devices, equipment cubicles, etc. As far as possible, facilities for later automated links to the design tools should be provided. Provisions should be made to ensure the consistency of common data of different I&C systems. Therefore, the application of a commercial standard database management system is recommended. Maintaining database consistency on a long-term basis is a very challenging and demanding task.

The database system should have facilities for automatic format checks during data entry. It should be noted that for a complete installation of an I&C system including a control room, several million items of data should be identified accurately, entered into the database and verified. It is often found that the design documentation available as drawings and instrument lists is out of date or otherwise unsatisfactory. On-site validation of this data requires a flexible yet secure method of correction of errors found in the data, by comparison with the plant, and with suitable supporting QA.

6.3.11 Design tools

The methodology for producing the design documentation for the intended I&C system renewal or upgrade should meet the following requirements:

- the specification should be understandable by I&C engineers, safety engineers and evaluators, as well as by process engineers,
- the formats of the specification should be standardized,
- the design data should be kept in a data management system (with adequate QA) which contains each data item only once and supports all phases of the I&C lifecycle.

The system for names of internal signals, etc., in the I&C system should be specified. The design methodology should result in documentation that is clear and consistent.

If a set of VDU displays is being designed for the HMI, it should be noted that typical plants may need several hundred or more different displays. Design of these displays should follow

accepted human factors engineering practice, including the use of reference project standards on character sizes, colour, names of plant items, types of measurements and symbols for plant devices such as pumps and valves. Care should be taken to limit the number of measurements on any given display in order to ensure rapid understanding and clarity for the operator. Presentations should include the current state of the plant, and also the ability to show historical traces. The design of these displays can be significantly facilitated by the use of good tools, preferably with CAD facilities, and if possible automatic links to the database management system for signal characteristics. A human factors review of all display layouts should be undertaken. Some guidance on display design is given by IEC 61772.

The same data collection and design tools should be used for the project as for the future operation and maintenance, see also 7.20.

6.4 Tender specification and purchasing of the individual systems

6.4.1 General

In the project basic requirements specification phase, the relevant requirements for an intended I&C system realization are documented. These requirements then need to be broken down and developed into the detailed requirements for each individual system of the total project. These are described here as the specifications of the I&C systems, and are generated from the basic requirement specification. These specifications form the input reference for quotations by suppliers and the subsequent contract placement, detailed design, manufacture, software production and installation work. The clear identification of the scope of work of each participant in the modernization project and the division of responsibilities is of great importance, and should be defined in principle in the specification.

6.4.2 Specification of I&C system properties for candidate solutions

This subclause describes the basic requirements, which are necessary for the successful production of the I&C system specification. The properties listed are recommended with the aim of easing the licensing procedure for the realization of category A functions (IEC 61226). For the realization of lower category functions, category A requirements may be omitted or reduced consistent with the safety or operational importance. The following points should be covered in the requirements:

- the hardware of the I&C system should be qualified or qualifiable to assure sufficient seismic and environmental robustness (IEC 60987, IEC 61000 series, IEC 60780, IEC 60980, IEC 61513),
- the system shall comply with requirements for redundancy and separation (IEC 60709),
- the software should have a clear modular structure with a coordinated development according to IEC 60880, IEC 62138, or other relevant software standards,
- the I&C system should have sufficient flexibility and performance capability to ensure the required functionality, with a satisfactory response time,
- the required I&C system behaviour should be specified and should reflect the functional categorization,
- the system should have an open architecture supported by several vendors.

For reasons of effort in design and software maintenance during the total life cycle, the state of the art is to have engineering tools with the capability of automatic code generation. The licensing of digital I&C systems may be eased by the use of:

- a proven procedure for code generation based on proven software modules,
- a graphic representation of the application functions for ease of understanding,
- integration of formal checks to ease the verification of design results,
- a standard language code for functional validation, used to enable the direct use of the generated code in the target system,
- validated tools, well documented and accessible,

- configuration management support.

6.4.3 Specification of requirements for quotations

The documentation of the detailed requirements for each system should take the form of a specification for the equipment, software and services required. Where several systems are involved, possibly originating from different suppliers, common specifications should be produced for such aspects as environmental qualification testing, equipment construction standards, software general requirements and standards, and to define the site services and interfaces.

An important precondition for issue of the specifications and invitations to bid is that the utility or sponsor agree to a list of potential suitable suppliers. They should be experienced in the class of equipment required, in the class of modernization work involved, and the work involved on site, which may be in a difficult location.

Tenders should include verification of conformance with requirements.

The method of assessment and criteria for acceptance of tenders should be agreed before the specification is issued to potential suppliers. It is important that the suppliers are aware that the assessment will be complete and fair, and that they will be informed of their standing in the assessment, since considerable work is involved in the production of tenders for nuclear plants.

6.4.4 Tenders for each system

The potential suppliers need to undertake preliminary design, based on the tender specifications issued to them, sufficient to provide suitable quotations and technical tenders for the systems concerned. If the tenderers are required to include a feasibility study in their tenders, then the terms of reference for the study should be clearly stated.

An important part of modernization work may be the use of existing designs or software, previously supplied for similar applications. It is important that the operational experience and details of such designs and software are well described by the tenderer, and that he is prepared to make available full details, with suitable agreements on confidentiality, to allow assessment for re-use in the application. The project should review evidence of software quality to ensure that no problems occur later during the licensing process.

The selected supplier should have given evidence of conformance to requirements and shown good confidence in the meeting of time schedules and costs. References on earlier installations should be given.

6.4.5 Order placement

When tenders have been submitted and assessed, and the purchaser and any sponsoring organization have agreed on the choice, a formal order will be placed to the selected supplier. Part of this work should be the detailed negotiation of options and any additional aspects, agreement on any non-compliant aspects of the offer, full clarification of any work areas (such as cable design, task analysis or VDU display design) which the utility itself may wish to undertake and the detailed interfaces with the remaining parts of the plant.

It is good practice to provide a new document issue of a binding specification, revised in detail to reflect the agreements made during the contract negotiations, for subsequent contract use. This document may be based on the tender specification or tender document and should clearly specify the interface between supplier and customer. The agreed document then serves as a reference for proceeding with design, implementation and installation of the system.

7 Considerations for modernization

7.1 General

The modernization of the existing I&C system should be evaluated at a preparatory phase on a technical and economic basis. This usually includes consideration of the issues discussed in the following subclauses, which should be reflected in the tendering specification.

7.2 Technology considerations

It should be noted that the life cycle of current I&C equipment is being continually shortened as a result of rapid change in the underlying and driving electronic technology.

Sensors, transducers and control units are becoming “smarter” as embedded micro-controllers are employed in their design. Auto-calibration, self-test and built-in diagnostics, and digital communications are now commonplace features. The trend is to convert analogue measurements to a digital format from the front end, as close to the sensor/transducer (and process) as possible. Analogue circuits used in discrete instrumentation are becoming increasingly obsolete, being replaced by digital counterparts, which in some cases offer higher accuracy and better performance and reliability.

Individual analogue control loops configured from discrete analogue instrumentation equipment and hardwired interconnections are becoming obsolete, being replaced by a different control architecture, based on digital control systems. In this new digital architecture, the physical analogue loop, excluding the process signal transducer and the final control element, is replaced by a digital controller equivalent. The platform for this digital architecture may be PLC or Digital Control System based. The digital equivalent of the control loop may or may not have a dedicated hardware processor, or it may be implemented as one of several software controller modules.

Once a process measurement signal enters the digital control system at the input interface, the transfer and processing of the signal information is no longer performed by discrete hardware and interconnection wiring. The transfer of information is done digitally, over network communications hardware (data highways), and the control algorithms are performed by software. At the digital control system's output interface, hardwired interconnections again transfer the control signal to the final control element.

It should be noted that with the availability of the remote I/O capability of digital control systems, a great portion of the trunk cabling required for conventional discrete analogue control loops can be eliminated, being replaced by data highways.

The fact that all digital control systems and instrumentation relies on the execution of software programs for computation and manipulation of measurement and control signals raises the issue of SW V&V. Current experience in the nuclear industry, which evolved based on the regulatory bodies' interpretation of SW V&V requirements on computerised safety systems, has led to the situation where a significant amount of time is required for SW V&V tasks, even in cases where program code changes are minimal, i.e. a set point change.

The selected I&C equipment may be sensitive to fluctuations in ambient temperature, and it may be necessary to locate such equipment in air-conditioned rooms. DCS equipment is also known to be susceptible to EMI, and the new digital equipment should be located in a shielded, low EMI level environment. Electronic equipment is sensitive to radiation and should be suitably qualified for its proposed location, taking into account dose rates from normal operation and accident conditions.

The decision to upgrade a discrete analogue control loop I&C system to the newer, digital architecture system depends on the resolution of the following issues:

- a reasonable approach to the SW V&V issue. This includes acceptance standards for manufactured equipment. Applicable IEC standards are found in the bibliography,
- the scope of the I&C modernization and the impact of having multiple architectures in the same plant. Digital equipment designed to replace analogue-based equipment in discrete analogue loops using the existing wiring should not be difficult. However, the replacement of complete analogue loops with a digital control system will result in hardware and wiring differences,
- compatibility with existing SCC, interface/communications with the SCCs,
- future modernization and migration to new generations of control systems, and protection from obsolescence,
- it should be taken into account that digital equipment does not always behave in the same way as its analogue or relay based equivalent,
- software qualification is a major point to be considered before choosing a digital instrument.

7.3 Economic considerations

Prefabricated modules to replace portions of existing systems could be considered. The objective of using modules is to simplify the installation and to reduce the cost, particularly for parts of systems that are of a complex design or that are installed in a limited space. The scale of the modules would be comparable to the size of the existing system equipment, and could be easily moved into the space occupied by the existing equipment.

Economic consideration should include the costs of any lost generation during the implementation of the modernized I&C system. It should also include station de-rating caused by the installation of modernized I&C system.

Excessive outage costs may be avoided by installing parts of the system during reactor operation where possible. Prefabrication of modules may reduce the time and radiation exposure during plant installation.

If the renewed or upgraded I&C system components are located inside the containment building, the cost of disposal of radioactive materials, labour costs, and radiation dosage costs should be factored into the cost estimate.

Costs may be reduced if the new system makes it possible to carry out maintenance and testing during plant operation rather than during outage periods.

State of the art developments in instrumentation should be investigated. Some examples are:

- Some smart instruments provide means for remote or self-calibration. This feature should be evaluated for those instruments that require frequent calibration, especially for applications where high availability or high accuracy is necessary.
- There are instruments that can measure more than one variable within the same sensor package such as pressure and temperature, or flow, pressure and temperature. The cost effectiveness of such instruments should be evaluated. However, consideration should be given to the simultaneous loss of several process parameters caused by a single instrument failure.
- Transmitters are available with local area network connections so that many of them may be interconnected to share the same data highway to the control computer. There may be savings in reduced cabling and in simpler computer input interfaces.

Consideration should be given to the loss of information in the event of data highway failure.

- A distributed control system provides a cost-effective method for eliminating pneumatic-only control loops such as those sometimes used for feed water control.

It should be noted that the adoption of state-of-the-art developments may require additional justification to the regulatory authority, in which case due account should be taken of the resources required.

7.4 Regulatory codes and standards

The modernized I&C system probably has to meet the currently-effective regulatory codes and standards. The effective codes and standards and their applicable revision status should be agreed and endorsed by the authorities before the implementation of the engineering design and the procurement of equipment. These codes and standards may include IAEA Safety Codes and Safety Guides, IEC standards, and most importantly, any codes and standards issued by the local safety regulatory body.

The bibliography provides some useful references.

7.5 Company policy and engineering standards

Changes in company policies and engineering standards may affect the design of the modernized I&C system.

Important considerations in selecting the modernized I&C system for a NPP are:

- to limit the number of control system suppliers to allow overall plant standardization on a cost-effective basic industrial system that would result in low O&M costs,
- to select suppliers with known and proven records of successful projects,
- to select an open architecture supported by several vendors which is desirable to allow operations of modernization as they become available, as opposed to a closed proprietary architecture from a single supplier,
- to consider the use of a standardized control system throughout the NPP, such as the DCS; otherwise, suitable interfacing standards should be provided if more than one type of control system is used,
- to limit the application of nuclear grade control systems to the safety functions of safety and safety related systems.

7.6 Safety and process control system future needs

The objectives and requirements of the modernized I&C system should be clearly defined. The equipment specification should be prepared, based on these requirements. Future needs should be considered, and particular attention should be paid to any restricting requirements in the design.

The following requirements should be specified:

1) General requirements

- revised safety requirements and operational requirements,
- revised plant design requirements,
- revised system design requirements,
- determination of the revision or edition of codes and standards to which the existing I&C system was designed. Any non-compliances with these codes and standards, and the reasons for the non-compliances should be documented,
- level of automation,
- reliability requirements,
- maintainability requirements,

- safety classification.

2) Functional and performance requirements

- full identification of the functions to be renewed or upgraded, and their allocation to the safety or other goals identified in the feasibility study,
- identification of functional assignments between the operators and the I&C system (IEC 60964 and IEC 61839),
- formal safety categorization of the intended functions and the identification of their relation to the safety or other objectives, the single failure criterion, the use of defence-in-depth and functional diversity,
- the identification of operator interaction with the system,
- the processing to initiate alarms,
- control logic,
- accuracy,
- time response,
- repeatability,
- the level of automation of the upgraded system, and the required operator actions under normal and accident conditions should be defined.

3) Equipment requirements

- identification of deterministic features for failure tolerance and changeover, and for design values of probability of failure and spurious trips or actuations,
- the extent of functional processing of the signals,
- identification of deterministic requirements on the management of common cause failures, and the probabilistic target values for availability and reliability design,
- equipment general technical requirements,
- the qualification requirements for EMI, environmental (incl. accident conditions) and seismic,
- the quality assurance of software or programmable equipment,
- input and output signals.

4) Scope of functions/equipment

- the identification of the use of existing measurements,
- the identification of the need for the installation of new sensors,
- the need for on-line validation of input signals,
- the identification of command signals to trigger the actuators,
- the removal of old equipment which is no longer required,
- the scope of related simulator functions to be modernized.

5) Interfaces

- system internal interfaces,
- interfaces with other support systems, such as electrical power supplies, instrument air, fire protection, heating and ventilation systems, should be specified,
- the detailed interface and extent of responsibility between the utility and supplier and between suppliers.

6) Installation requirements

- limitations of power supplies,
- cabinet and cable tray space,
- sensor installation limitations,
- penetrations,

- ventilation,
- access for installation work, including preparatory work during normal operation and work which can only be carried out during the outage.

7) Others

- design review requirements,
- V&V, qualification,
- information on available documents and re-engineering of documentation,
- the identification of required documentation, e.g. qualification and analysis reports,
- equipment data, operational experience,
- quality control,
- self-documenting capability,
- mounting methods at factory and plant (for the reduction of risk for systematic failures),
- security (configuration control, work methods for software changes during project and operation, protection against internal non-authorized access, protection against external intrusion).

7.7 I&C system reliability

System or component reliability targets for the upgraded I&C system should be determined. The targets will be derived from the overall system performance requirements, which may be dictated by the overall safety system assessment and the productivity factor of the NPP.

Consideration should be given to system redundancy as a means to improve system reliability.

Critical components should be of proven and simple design, to achieve the highest reliability.

Access control and change control management should be provided to prevent unauthorized intrusion into the I&C system's program and database areas, in order to maintain the integrity and security of critical information.

The I&C should be designed for suitable robustness, failure tolerance, safe failure, and graceful degradation. The probability of a complete loss of communication via the data highways should be reduced to the lowest possible level, and redundant hardware should be provided to maintain continued safe operation of the plant in the event of a single data highway failure. The design should enable the I&C system to recover as gracefully as possible from failures in the I&C.

Aging components may lead to increased system failures. Preventative maintenance should be considered. See also IAEA-TECDOC-1147 giving guidance on management of aging.

7.8 Risks and benefit study

In the risks and benefit study, the following factors should be included in motivation calculations:

- the revenue from higher generation levels, increased availability and increased lifetime,
- the reduction of maintenance costs: maintenance during operation, increased maintenance intervals, reliability-driven maintenance and improved reliability,
- the possibility of shortening future plant outages, which will subsequently improve the productivity of the NPP,
- the reduction of administration costs through improved data handling,
- the risk of delay on restart following the modernization outage,

- the continued safe operation of the plant during the implementation of the modernized I&C system, and possible unavailability of the modernized system,
- any risks associated with maintaining the old system, i.e. due to obsolescence, aging,
- the influence of aging equipment and the availability of personnel capable of maintaining old equipment,
- the risks of incompetence of personnel with the new system due to insufficient training or lack of operating experience.

7.9 Safety classification

Safety classifications have evolved in most countries with the development of different reactor series. In later plants, safety classes have been elaborated with respect to defence-in-depth concepts, post-accident operation and other safety related functions.

The latest standards (e.g. IEC 61226) provide finer graduations in the safety classification of I&C functions and equipment, in order to consider constraints associated with the safety qualification of industrial grade I&C equipment (e.g. PLCs and digital HMI systems).

When assessed against the latest safety classifications, the separation of I&C systems performing safety-related functions on older plants is often incomplete, resulting in the need to classify functions which have no direct safety relevance.

A cost advantage can be gained in the design of new I&C systems by exploiting the finer subdivisions of safety classification permitted by modern standards

When a new classification scheme is applied in the context of a modernization project, it is necessary to precisely define the areas to which the new classification scheme and associated requirements are applied. This may lead to the co-existence of different sets of requirements for new and old systems.

7.10 Equipment qualification requirements

Equipment qualification requirements of the current system and components should be determined. The equipment requirements and accident environments (room conditions) of the modernized system and its components should be included in the study. The equipment and qualification cost, technical difficulties, and time required to qualify the components of the modernized I&C system are factors to consider. The future costs of preserving and maintaining the equipment qualification of the modernized system and its components should be considered.

For example, consideration should be given to avoiding the extension into the reactor building of the data highways carrying signals that would be required following a loss of coolant accident. Signals travelling within these data highways should not be corrupted and should not impair the safe operation of other safety systems at any time during a DBA. The hardware inside the reactor building should then be as maintenance-free as possible under normal operating conditions.

The following types of equipment qualification should be considered:

- LOCA,
- vibration,
- EMC,
- aging,
- seismic qualification,
- environmental (normal and extremes of temperature, humidity, radiation etc.).

The current seismic design requirements should be determined. Upgraded equipment may have to comply with the latest seismic requirements. The level of seismic requirements and the safety function of all the safety devices during and after a seismic event shall be defined.

Anchored furniture and storage cabinets for manuals, personnel safety equipment, special tooling, etc. should be included in the design to prevent un-anchored objects from jeopardizing the seismically qualified equipment in the same area.

7.11 Software qualification requirements

Modernization of safety I&C systems performed using digital I&C systems typically relies on functions implemented by software.

The complexity of software based systems exceeds that of the hardwired systems being replaced. This has focused attention on the problem of errors in specification and design not completely revealed by testing and inspection, with the consequence of potential systematic failures.

Typically, the design basis and standards endorsing the hardwired systems to be modernised do not deal specifically with software errors and software qualification. However, for most of the topics linked to the qualification of software based systems, international consensus has now emerged and is reflected by a set of international standards providing the key requirements. See bibliography.

- A classification scheme should be used for the I&C functions, allowing different categories of functions and for different classes of I&C systems implementing those functions.
- A Defence-in-Depth and Diversity analysis (3D analysis) should be used to identify the potential for software related common mode failures, and to evaluate potential countermeasures.
- Appropriate requirements should be imposed upon the software design.

Since absolute freedom from software errors cannot be proven, emphasis is to be placed on the quality of the design process, in addition to requirements for testing.

The key requirements are defined below:

- the software design should be supported by the following documentation:
 - software safety plan
 - software QA plan
 - software verification and validation plan, including independent V&V
 - software configuration management plan
- the software should be designed according to a software life cycle plan, with well defined design phases and documentation.

A basic principle for the execution of safety functions is that the required software is executed cyclically and independently from the plant conditions. Such a system, with constant processor and bus loads, can be verified relatively easily.

As a practical approach, reusable standard software should be used as much as possible. The reusable components such as operating system kernel, libraries and tools should have undergone a generic licensing procedure or should have been assessed in a plant-specific licensing procedure.

It is also recommended practice that the plant-specific application software should be generated automatically by code generators from a formal specification. This avoids the need for project-specific manual coding, simplifies the review, verification and validation processes, and minimises the project-specific licensing effort and risk.

7.12 Physical constraints

The following factors should be reviewed in locating the modernized system equipment:

- limitations in buildings,
- limitations in cabinets,
- limitations in process systems,
- limitations in existing penetrations,
- cable routing limits, including evaluation of the requirements of new technologies e.g. special cable trays for fibre-optic cables, bus cables and requirements for separation,
- floor loading,
- auxiliary systems capacities, e.g. power supplies, cooling equipment, ventilation, fire detection and protection,
- limitations in space and access for installation, operation and maintenance.

Depending on the scope of changes, if a new digital communications network is to replace a hard-wired system, space for equipment racks and I/O termination panels is required. If single components are being replaced, there is not much impact on the existing wiring.

7.13 Equipment availability (delivery and support)

An inventory of equipment and materials should be produced for the modernized future I&C system. This should identify long term delivery items, expensive items, and potential suppliers.

The availability of spare parts and technology support for the rest of the station life should be reviewed. The continued support of the supplier in the future is always an issue, regardless of the technology used. Usually, if obsolete equipment is retained, the assurance of continued and future product support is less likely than when new equipment is used.

Protection from future obsolescence, even of new technologies, can never be fully guaranteed, but certain approaches can be used to minimise the possibility, i.e.:

- the use of industry standard equipment from manufacturers with a large installed base of systems,
- the use of proven technology. Most manufacturers will have several installations in which their systems have been operational for several years,
- the following of nuclear industry trends. See what other utilities have tried and found to be successful.

The use of open architectures and standard communication protocols can reduce the effects of obsolescence in the future life of the station.

7.14 Human factors

Human factors considerations should be incorporated into the design process and into the development of operating and maintenance procedures to enhance the ability of the staff to operate the plant safely during normal, abnormal and accident conditions.

A Human Factors Plan is normally a requirement for all new NPP designs. The plan identifies and commits engineering design for human factors considerations early in the design phase. The process requirements on I&C including the control room and other control places in the plant should be identified using appropriate methods, e.g. IEC 61839. Other IEC standards supporting HMI design can be found in the bibliography. Operator and maintenance staff inputs have a heavy influence in the ergonomic design of the control centre to ensure that both the cognitive and physical workloads of the operator are achieved with the maximum

efficiency and minimum stress. Some examples of the ergonomic factors to be considered include:

- main control room panel layout, alarm annunciation, labelling, and console functions,
- supplementary control point considerations similar to the main control room, but allowing for functional differences,
- HMI and its impact on operating procedures,
- field panels and their interface with the control room,
- data acquisition and assessment using new consoles.

PAM and human factors consideration requirement is part of a larger overall statement of design principles and may impose requirements on the control system architecture.

HMI are usually supplied by the control system manufacturer as part of an integrated system, both hardware and software. The ability for handling custom interfaces should be determined if there is a requirement to use an existing or foreign HMI.

The HMI has the following distinct functions:

- display of process status,
- manual input devices and information feedback displays,
- alarm annunciation,
- status (data) logger,
- information reduction.

The manual input and information feedback system is meant to be:

- the operator's window through which he can visualise the plant operation, and
- the interface where he can enter commands for change of status or set points to the DCS.

Significant changes to the overall panel devices and their layout are expected to occur, and these will require a human factors study before the final design will be acceptable. Operator functional task analysis should be performed. Many tasks that were formerly done standing at a control panel may be done sitting at an operator workstation. Means for the First Operator and Shift Supervisor to efficiently monitor the overall plant status, as well as current control room operator activity, should be provided in such a manner that eliminates interference with each other's tasks.

In the case of phased or partial modernization, the new parts should be consistent with the existing layout and design philosophy.

In the case of complete modernization, the new control room main panel layout may have a significantly different look. Former control room design guides should be updated. For example, the dark panel philosophy should be revisited. The criteria for highlighting post accident monitoring devices should be reviewed. The alarm annunciation design criteria (flashing sequence, type of horn, push buttons functions) should also be reviewed.

Main control room seismic requirements, lighting arrangements, air conditioning and purification, noise abatement, access control etc. are some areas that may need upgrading to provide a suitable environment for the operators during accident as well as normal conditions.

The ease of producing alarms increases with the use of a DCS, and suitable alarm conditioning criteria should be developed to limit the number of nuisance alarms. A separate status logging function can eliminate many nuisance alarms associated with the normal operation of equipment, such as breaker status change, valve position changes, etc. In these cases, only the failure to produce the expected change of state should be alarmed. The change of status information will be recorded by the status logger. For redundant or triplicated

alarm signals, the alarm server could annunciate the first alarm signal to arrive. When the second or third alarm signal is detected, the alarm message would confirm when the signal arrived. The status logger would list all the alarms individually. A clear philosophy on alarm filtering for the suppression of less important alarms should be established in line with the requirements of IEC 62241.

Experienced operators and shift supervisors, as well as maintenance engineers should participate early in the development of the criteria for the HMI operator and maintenance workstation display screens. Operators and designers tend to have very different views of the systems, and often what the designer may think is important may not be so from the operator's viewpoint. Designers need the guidance of experienced operators to be able to understand their viewpoint and to provide control room information that meets their requirements.

7.15 Defence-in-Depth and Diversity analysis (3D analysis)

Recent I&C upgrading usually replaces old analogue equipment with new digital equipment due to the obsolescence of analogue components. The digital equipment executes software programs in order to implement functional requirements. Digital equipment suppliers have tried to convince regulators that these modern software systems do not introduce failures that were not previously considered in the design of their analogue predecessors. However, for programmable electronic systems, the software is inherently vulnerable to software errors and may lead to unpredictable behaviour. A lack of hardware integrity and excessive sensitivity to environmental conditions are postulated as potential sources for CMF. Regulators require that a CMF that occurs simultaneously in all systems/divisions be considered within the plant accident design basis. In cases where digital equipment is adopted in a protection system, it should be verified that the common mode failure in protection systems does not increase the core melt frequency. This is commonly referred to as a 3D analysis. The 3D analysis should show that the total I&C system has sufficient defence-in-depth capability and diverse means to perform safety functions to mitigate accidents and transients assuming a common failure in the protection system software

Although most regulatory agencies require a 3D analysis that demonstrates the ability to cope with common mode failure, there is still significant industry variance regarding the initial boundary conditions, acceptable coping measures and final acceptance criteria for this analysis. The following paragraph describes some of the key differences seen in digital modernization programs to date:

- Accidents that should be considered coincident with the CMF
Some regulators require that all accidents be considered. Others have accepted probability arguments that eliminate some accidents from consideration due to the combined low probability of the CMF and the low probability of the accident. Typically coping with lower probability accidents with a CMF requires more functionality in the credited diverse systems.
- Effect of CMF on the response of the I&C systems
Some regulators have accepted arguments that the CMF results in only passive (sleeping) conditions within the I&C systems. Others require consideration of CMFs that result in active failures that have the potential to adversely interfere with other plant defences. Examining these potential interactions including their time dependencies can be very complex and often requires design changes to ensure acceptable results.
- Systems that can be credited in the analysis
Some regulators have accepted credit for any plant system/equipment that is diverse (i.e. not subject to the same CMF). Others limit the systems that can be credited to only those with acceptable safety qualification. This may raise the qualification pedigree of the credited diverse systems.
- Extent of diversity to allow crediting
In some cases, regulators have accepted the adequacy of functional diversity (e.g. different applications running on the same product platform or software operating system).

Other regulators require diversity in all levels of the system/product to allow the system to be credited in the 3D analysis.

– Time constraints on operator action

In establishing methods to cope with the CMF during accident conditions, regulators have accepted credit for any operator actions that can be defended using accepted human factors engineering principles. Others have restricted operator action times to be consistent with current safety analysis constraints. Limiting operator action times may increase the requirement for automation in the credited diverse I&C systems.

In spite of these differences, it has been demonstrated in several plant modernization programs that this issue of Common Mode Failure can be handled successfully and cost effectively. Critical to this success is that regulators be approached early in the modernization program, so that the design basis for coping with common mode failures is agreed to by all.

7.16 Separation and protection against fire and flooding

Where a system is important to safety, each redundant equipment channel should be physically and electrically separated from all other equipment channels to avoid common mode events or common cause failure. Full requirements are given in IEC 60709.

From a point of view of extra robustness and separation of functions, separate servers retrieving data from the same data highways should be used for each different function.

Block walls to stop the spread of fire and to limit the fire load of each area may be needed in the upgraded design. Station layout and equipment location should consider flooding.

Improved fire protection and flooding protection may give large improvements on PSA figures on CDF.

7.17 Uncertainty and set point calculation

The set-points of I&C systems are very important for efficient, reliable and safe operation of NPPs. The calculation methodology and the uncertainties of various kinds of I&C components in the system affect the results of the set-point calculation. When new I&C equipment is installed to replace the old one, a set-point calculation should be performed using the new equipment data and latest calculation methodology, which could differ from the previous one. The results of set-point calculations should be compared with the current safety and operational criteria in order to confirm that the new system meets the current operational and safety limits. If there are greater margins, the final set-points could be selected within the limits considering operational performance and safety analysis. IEC 61888 gives requirements for the determination and maintenance of trip set-points.

7.18 Response time analysis

The response time of new equipment used for upgrading may differ from that of old equipment. Therefore, it is required to show that the response time of new equipment meets the specified criteria in accordance with the licensing basis. Following installation, tests should be carried out to demonstrate that the actual response time is within the allowable limits.

7.19 Test procedures

Prior to formal acceptance tests, subsystems of the I&C system are integrated and tested. This may comprise open and closed loop tests, tests in a test field, or simulation tests. The test results, together with the data from commissioning and the agreed scope of acceptance tests (e.g. FAT, SAT, operation acceptance tests and test operation) provide evidence for the system's fulfilment of the design requirements. Particular interest should be paid to the interfaces between "old" and "new".

It may be necessary to impose additional requirements on these tests and the monitoring of system functions during plant operation, such as

- parallel operation,
- trial periods at limited power,
- specific tests and measurements of system performance characteristics (for example: processor load, bus load, fault behaviour compared to predicted/specified behaviour),
- follow-up of fault reports,
- frequency of design errors,
- frequency of software bugs,
- frequency of hardware failures and failure logs over extended periods as deemed appropriate to obtain confidence in the quality of the design process and the system itself.

The principles for these tests should be established early in the project. The tests should be defined in detail by appropriate test procedures, specifying test conditions, test scenarios, resulting documentation and acceptance criteria. The safety authorities will be interested in the documented analysis of the test procedures and the corresponding results and may also impose specific conditions.

Existing procedures for the I&C system for periodic tests, response time tests, surveillances and calibration procedures should be revised due to the new system's characteristics, such as a higher degree of self-monitoring, self-test features or reduced frequency for tests due to higher component reliability.

7.20 Documentation management

To support the operation and maintenance, as well as modernization projects a document management system should be used. Such a system is large and complex and therefore special resources should be set up to create the system. The document management system should be initiated early in the project, if not already available. Such a system makes the supplier/customer interface easier during the project and gives good support to operation and maintenance from the beginning.

The documentation for the modernized plant should meet the various requirements of personnel categories such as operators, operation management, maintenance, design engineers, safety review personnel and training of these personnel categories.

A plant management network normally has many servers that require input from design databases. For example, work order management requires a list of different items that may be worked on, their location, specifications, parts, drawings, etc. There would be considerable O&M time savings if the information were linked together in the databases created at the design stage so that it could be easily transferred in a format convenient for the different O&M servers without requiring extensive manual input. This applies not only to instrumentation and control, but also to electrical, mechanical and civil equipment and parts.

Cross-referenced documentation such as design manuals, reliability and safety analysis and the safety report should be put into the information system allowing changes and their impact to be easily integrated. Also, safety and licensing documents, training manuals, operating manuals, operating policies and principles, etc. may be integrated.

Although the operational documentation will be available from computer workstations, back-up hard copies are required for situations when the terminals, the network or the documentation servers are not available. Storage areas for the documentation, as well as for other required items (stationery, torches, keys, communication devices, etc.) should be provided in safely secured cabinets.

The limited time available for I&C replacement during a short outage may lead to a situation where changes in the design documentation of the new system and in the plant documentation impacted by late modifications/changes cannot be updated completely during the outage. So, updating of the marked-up documentation needs to be finalized later, after the new I&C has been installed and commissioned. This effort should not be underestimated.

7.21 Update of plant technical documentation

The existing design documents and drawings may not necessarily reflect the true status of the existing physical plant due to a failure to document and record changes made in the field. A system study and field walkdown may be required to identify the gaps between the physical plant and the existing design documents.

The results of the field walk down should be used to verify the existing design documentation, or plant design configuration. The verified design configuration is then used to determine if the physical plant meets the current safety systems and process systems requirements. Any discrepancies should be identified as design gaps or deficiencies.

The updated documentation should include functional and requirements specifications, system descriptions, lay-out drawings, detailed installation documents, test procedures, maintenance manuals and procedures.

Difficulties arise if no design documentation is available or if the existing documentation is incomplete or inaccurate. In such a case the only possibility is to generate as-built documentation by means of plant inspections, reviews of old project archives and discussions with the plant personnel. Basic documents should be issued or revised where needed. In some cases “fingerprints” on the plant can be used i.e. recordings from normal operation or disturbances. It is important to identify documents and make sure that all persons involved in the project understand the existing documentation of the I&C systems and its status.

7.22 Training and staff qualification

Training for plant staff in the features of the new I&C systems, the modified HMI, and possibly changed process behaviour and I&C functions should be planned in the overall schedule of the project.

Several categories of plant staff should be considered, the main ones being listed below.

- Staff of the I&C modernization project need an overview of the specific features and capabilities of the new I&C system, sufficiently early in the project. Typically, no detailed knowledge is required.
- I&C technicians and maintenance staff need training about detailed system to equip them to perform maintenance on the new system (e.g. replacement of components, tuning of parameters) and possibly also modifications of hardware (e.g. minor extensions) or application software (modification of interlocks, design of new operating displays).
- Operating staff require a basic understanding of I&C system properties, a detailed knowledge of the HMI functionality and of the new I&C functions implemented, as required for plant operation, and also to be capable of a basic response to I&C faults (e.g. decision on the need to dispatch I&C technicians).
- Engineers (design, safety) and possible future simulator instructors.
- Maintenance and installation staff participating in the installation of the modernised I&C.

Each category of staff needs specific training programs and training courses. Training objectives, required knowledge and scope should be identified and scheduled sufficiently early.

In addition to formal courses about the I&C systems properties and plant specific functions, training should also include practical experience, this means

- the use of training mock-ups for I&C maintenance,
- the participation of utility staff in I&C design, mounting and testing,
- where possible, to analyse the operators' capability to perform their job in the modernized control room, and to observe their response to typical equipment malfunctions, in order to obtain confidence in the new HMI's adequacy and to reveal design flaws. The training programme and assessment of the trainees may be verified by the safety authorities.

In case of major modifications of the HMI in the main control room, implementation of the new system in the plant should be preceded by implementation in the training simulator, in order to train the operating staff according to the characteristics of the new system under real-time conditions.

Training should be completed prior to implementation in the plant; this could therefore be a critical path activity.

The availability of competent training personnel should be ensured. Training documentation should be part of the plant technical documentation to ensure that it is automatically updated during the project and operation. Certain HMI aspects should be included in the training documentation. Where possible, the operators' ability to perform their job in the new control room (partly or completely renewed) should be tested.

7.23 Project organization

A successful I&C modernization project requires the interface between multiple departments. Therefore, it is recommended to have a dedicated project manager to co-ordinate the multiple disciplines involved. Since the installation is often required to be completed during plant outages, effective project management is essential. Because it may be difficult for the plant to set up a large and effective organization, the use of external resources should be considered for demanding projects.

The project may involve external organizations, such as an engineering company, equipment manufacturer/supplier, constructor or safety authority. The organisational aspects should cover proper division of responsibilities between these organisations. Depending on the size of the project, the proper organization should be established to perform the project efficiently.

7.24 Configuration management

Adequate configuration management should be observed for the existing/remaining I&C, and should be established for the new I&C parts. This should ensure that the plant is operated and maintained in accordance with the licensing basis. For this, a well-documented system should be put in place during the initial engineering stage. This should include

- all procedures and QA measures needed to obtain and maintain consistent documentation,
- identification of all configuration items,
- documentation of all items under configuration control so that consistency of the as-built configuration with the specified design can be checked at any time, and that replacement components and software can be unambiguously selected.

7.25 Interfaces to the other existing systems

In order to properly replace the old equipment with new equipment, the existing requirements for interfacing to other systems should be reviewed and the decision made on how current physical and functional interfacing requirements could be implemented. If possible, current requirements should be retained, otherwise new interfacing requirements should be set-up. This includes physical conditions, cabling system, signal types, actuation devices, communication network and supporting systems, including power supplies.

For the safety demonstration, it should be shown that all interfaces of safety and safety related systems have been accounted for, that they are compatible, that their behaviour is fully specified for all operating conditions, and that required independence criteria and fault scenarios with respect to the interfaces are met. This is particularly important in the case of partial modernization where new equipment meets old equipment and when using or adapting multi-purpose products.

7.26 Standardisation

In order to enhance operational convenience and safety, to reduce the costs of operator/staff training and reduce the number of spare parts, the concept of standardization should be planned into every possible aspect of works and products. The standardization could be assisted by the preparation of standardization guidelines or the application of common software tools for engineering and management to be applied on the upgrading. Other existing guidelines and tools should be surveyed and evaluated if they are applicable to the upgrading works.

Standardization should be established with due consideration for diversity issues, bearing in mind the possibility of introducing potentials for common cause failure.

8 Implementation

8.1 General remarks

For the preparation of an upgrading program, there are some key elements in the early development of the upgrading strategy, i.e.

- an upgrading strategy for the whole plant,
- an elaboration of the target (final) configuration of the I&C system to be achieved at the end of all upgrading steps, in the sense of a “vision”,
- an analysis of the sequence of upgrading steps to be performed.

This clause provides guidance for the elaboration of a “draft implementation strategy” (at a low level of detail), as needed in an early stage e.g. for a feasibility study, as well as the more detailed considerations required for the design of new individual I&C systems.

8.2 Target architecture

In the design of the overall I&C architecture, the total scope of I&C systems (those which will remain, as well as those which will be modernized) should be considered.

Essential inputs are:

- the as-built I&C architecture together with the categorization of safety functions,
- the subdivision of the existing plant into functional complexes which are subject to uniform requirements, such as common safety classification or common performance requirements,
- the subdivision of I&C systems according to different modernization priorities,
- the physical and other constraints imposed by the existing NPP buildings.

When comparing the safety classification of older plants against current standards it is noted that:

- the separation of I&C systems performing safety or safety-related functions is often incomplete, and functions which had initially no safety categorisation may need to be categorised,
- modern standards in some cases allow more sub-divisions of the safety classification scheme, offering possible cost advantages for the new I&C system.

Therefore, the categorisation of functions should be evaluated very carefully so as, on one side, to identify potential for safety enhancements and, on the other side, to benefit from the possibilities of more modern safety classification schemes.

The target architecture should reflect the initial planning with respect to:

- 1) the revised top level plant requirements, process systems, layout etc.,
- 2) the envisioned HMI:
 - screen-based or conventional control room,
 - quantity and characteristics of supplementary control points,
- 3) definition of functional complexes, grouping I&C functions with common characteristics, such as common safety classification, common performance requirements, or same modernization priority,
- 4) structure and characteristics of the new I&C equipment to be installed:
 - location of the existing equipment, and anticipated location of the new equipment such as cabinets, terminals, cabling,
 - structure and characteristics of the communication systems,
 - segmentation of surveillance functions within a division, e.g. instrumentation for main process parameters such as power, neutron monitoring and pressure monitoring should be implemented by separate equipment,
- 5) requirements for spatial separation and layout restrictions,
- 6) characteristics of the interfaces to remaining systems.

It should also be noted that the target structure may be a mixture of different technologies and different I&C generations, in spite of the objective to have the new system as homogeneous as possible. This is particularly valid in cases where:

- either upgrading and back fitting activities have already been performed with local, focused modifications, and where it is considered more economical to retain these systems, or
- where the existing I&C is composed of subsystems with very different lifetime characteristics, with obsolescence being a strong driving factor in some parts, and where other systems may be retained due to good long-term support, low failure rates and long expected lifetime.

8.3 Sequence of upgrading steps

8.3.1 General

The second element in the implementation strategy is the design of an optimal sequence of modernization steps or “work packages”.

There are basically three possibilities:

- upgrading in a single step, during a single extended outage,
- upgrading in a limited number of large steps, spread over several years, to be performed during normal (or slightly extended) outages,
- focused modifications, each with a very restricted scope.

The optimal solution in terms of size and order of the work packages should be found on the basis of the following considerations, to be assessed by the utility and the potential supplier.

It should be noted that licensing requirements include consideration of the operating conditions during the modernization work (replacement at power, replacement of safety equipment while the core is not unloaded, installation of temporary monitoring systems, etc.). Every temporary or intermediate configuration needs to be licensable. Also, the radiological

protection of the installation workforce during work in hazardous areas constitutes a safety concern, and requires a safety demonstration.

8.3.2 One large versus several small work packages

Generally speaking from technical and theoretical viewpoints, I&C replacement in a single step during an extended outage may be the most efficient solution, since it minimizes the creation of temporary interfaces, repeated mobilization of installation and commissioning teams, and repeated training of operating and maintenance staff for the modified equipment and HMI. It is also very convenient if larger enhancements of process systems or buildings are already planned, necessitating an extended outage. In this case, one-step I&C modernization could be fitted into this program.

However, these arguments should be balanced with other organizational and economic considerations, which may lead finally to a sequence of several smaller I&C work packages.

- Production losses due to the extended outage should be balanced against the benefits from a one-step-solution.
- Annual budgetary restrictions for I&C modifications might demand extension of the upgrading program over several years.
- The size of the work packages should be acceptable from an organizational point of view:
 - the amount of review of design documentation linked to a work package, V&V activities, and co-ordination with other plant related activities should be commensurate with the utility's resources;
 - the size of the work package should be compatible with the supplier's capacity to design, manufacture, install and commission the new equipment within the anticipated time frame;
 - splitting the whole scope into several work packages may give the opportunity to gain experience on less critical parts of the plant before the core systems are modernized;
 - requests from licensing authorities, or pending problems in an individual system may impose the need for modernization of isolated systems in the short term with insufficient time available to anticipate a one-step modernization.

8.3.3 Definition of work packages

If there are systems of limited size, with simple and clear interfaces to other I&C systems (e.g. data acquisition computers, special monitoring systems, etc.), these should be defined as isolated sub-work packages.

Optimal use of the available outage time typically requires installation of the new I&C equipment before removal of the obsolete equipment in the plant. This may be limited by the space available. Different solutions can be envisaged:

- it may be advantageous first to implement a small work package focused on the removal of larger items of obsolete equipment so as to gain more space for subsequent work packages;
- it may be advantageous to install new equipment in temporary locations (and to move it later to its final locations);
- it may be advantageous to install the new equipment in different locations than the obsolete one, either in new/additional buildings or enclosures or in locations which were initially not foreseen for I&C installations;
- a specific solution would be shifting functions from local control stations to screen-based operator working places in the main control room, thus gaining space for the installation of the next work package.

The space available for these different approaches may be decisive for the definition of the corresponding work package.

Interfacing existing equipment with newly introduced equipment may lead to complicated interfaces or the supply of custom built equipment, and may also require a re-qualification of the existing equipment due to the modifications. It may therefore be advantageous to extend the scope of the modernization so as to include non-obsolete equipment, with the intention of avoiding re-qualification, awkward interfaces and the supply of non-standard equipment.

When screen-based process control is introduced, the homogeneity of the HMI should be considered. The HMI for a defined individual operator task sequence should be kept as homogeneous as possible, i.e. either on the basis of conventional panels or on screen-based technology. Mixed solutions where a single operator task needs to be performed partially by screen, partially by conventional indicators and controls should be avoided. Where this cannot be respected because the boundaries within the I&C systems do not correspond to the boundaries of operator tasks, it might be necessary to consider the implementation of temporary interfaces of the new I&C to the conventional panels, or of the old I&C to the screen-based interface so as to maintain the consistency of the operator interface for a given task.

8.3.4 Parallel operation and replacing equipment at power

Parallel operation of old and new equipment should be considered; both open-loop and closed-loop-parallel operation could be considered. There are several possible motivations:

- parallel operation gives confidence in the correct operation and behaviour of the new I&C system. In case of open-loop operation, the correct response to plant events could be monitored, without any risk to spurious actuation,
- parallel operation separates the task of installation and commissioning of the new system from the task of disposal of the old system, allowing the latter to be carried out over a longer time thus keeping outages short. A necessary precondition is that sufficient space for installation of the new system is available.

A specific case where parallel operation is used to check the operation of the new equipment is replacement at power. This is, in case of minor modernizations and under some specific boundary conditions, an interesting option. It can be considered in cases where:

- the location of the equipment to be replaced is accessible during power operation,
- the scope of the equipment to be replaced is very limited (e.g. a single rack or drawer),
- the interface of the new equipment to the old one does not require modification of the remaining equipment,
- the new equipment is not needed during power operation, or redundant equipment is used so that one redundant channel can be replaced after the other without loss (the coincidence logic scheme may need to be temporarily reduced).

Such an approach may be interesting, e.g. in the case of replacement of neutron flux monitoring systems together with a new core. In this case, the channels of the new system can be aligned immediately against the existing old channels, without uncertainty about the “correct” flux level.

The following risks and advantages of this approach should be evaluated case by case:

- the high risk of impacting plant operation (trip by spurious actuation while coincidence logic is reduced) while manipulating the interfaces,
- the reduction of workload of I&C staff during outages,
- the possible shortening of outage times,
- the comparison of new and old equipment during parallel operation time.

8.3.5 Sequence of work packages

Subclause 8.1 recommends the establishment of priorities for the modernization of I&C systems. During the refinement of the implementation strategy, more detailed considerations

for the sequence of work packages are necessary. The most important criteria are listed in the following paragraphs.

Systems with imminent failures or increasing unavailability due to lack of spare parts, missing support, or unacceptably high failure rates should be modernized first, as well as systems needed to satisfy direct requirements of safety authorities.

Modifications with an important impact on the HMI (e.g. transition from conventional panels to screen-based operation) should be preceded by adequate time to allow for operator training and acceptance, and validation of the new concept in the simulator. If there is insufficient time for operator familiarisation, then systems without major modifications of the HMI should be modernized first. Where possible, the HMI platform to be used throughout the complete I&C modernization should be introduced from the start. Also, any systems which will not be represented in the training simulator could be modernized at an early stage since only reduced preparation time for the installation in the plant is needed.

It may be advantageous to start with auxiliary systems so that the utility and the supplier may gain experience on a first pilot project without critical impact on the overall plant processes. This could also be used to obtain acceptance by the operating staff in a non-critical part of the plant, and give a sound basis of acceptance and feedback of experience for the decision between screen-based or conventional HMI.

9 Recommendations

The report recommends a systematic approach including the following steps:

- consideration of the overall strategy of the utility, in forming the I&C modernization strategy itself,
- a preliminary evaluation to summarise the motives for modernization, giving the risks, costs and benefits,
- preparation of detailed feasibility studies, together with budget costs and a preliminary safety case,
- preparation of tender specification and a bidding process leading to order placement.

Guidance for following project activities are well described in other documents referenced in the bibliography.

Major upgrades to a nuclear power plant involve difficulties of the same level as building a new plant. It is therefore important:

- to set up a competent resource at the customer side,
- to choose competent suppliers with proven skills in nuclear power plant engineering and commissioning of their equipment.

The most important issue is then to work systematically as indicated in this report. Some of the most important issues found by experience are:

- to involve the licensing authorities in the earliest possible stage,
- to set up a scope that optimises the plant life cycle profit, define work package sizes and sequence carefully taking into account plant prerequisites, as well as the competence and workforce of the project organization,
- to secure plant documentation updates, including detailed information on the technical background to the design,
- to address the HMI of the programmable electronic technology from an early stage in the project,

- to review suppliers' evidence of software quality before ordering and choose products which give confidence for licensing later on.

Bibliography

International Electrotechnical Commission (IEC)

IEC 60671:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60780:1998, *Nuclear power plants – Electrical equipment of safety system – Qualification*

IEC 60960:1988, *Functional design criteria for a safety parameter display system for nuclear power stations*

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

IEC 60980:1989, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

IEC/TR 61000-1-5:2004, *Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems (only available in English)*

IEC 61225:2005, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for electrical supplies*

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions¹*

IEC 61227:2008, *Nuclear power plants – Control rooms – Operator controls*

IEC 61497:1998, *Nuclear power plants – Electrical interlocks for functions important to safety – Recommendations for design and implementation*

IEC 61500:2009, *Nuclear power plants – Instrumentation and control important to safety – Data communication¹*

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety – related systems – Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety – related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety – related systems – Part 4: Definitions and abbreviations*

IEC 61771:1995, *Nuclear power plants – Main control-room – Verification and validation of design*

¹ To be published.

IEC 61772:2009, *Nuclear power plants – Control rooms – Application of Visual Display Unit (VDUs)*²

IEC/TR 61838:2001, *Nuclear power plants – Instrumentation and control functions important to safety – Use of probabilistic safety assessment for the classification*

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62340:2007 *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

International Atomic Energy Agency (IAEA)

Reports prepared within the framework of the International Working Group on Nuclear Power Plant – Control and Instrumentation:

IAEA-TECDOC-668:October 1992, *The role of automation and humans in nuclear power plants*

IAEA-TECDOC-808:July 1995, *Computerisation of operation and maintenance for nuclear power plants* (only available in English)

IAEA-TECDOC-812:July 1995, *Control room systems design for nuclear power plants* (only available in English)

IAEA- TECDOC-912:October 1996, *Computerised support systems in nuclear power plants* (only available in English)

IAEA- TECDOC-952, *Advanced control systems to improve nuclear power plant reliability and efficiency* (only available in English)

IAEA-TECDOC-995:1998, *Selection, specification, design and use of various nuclear training simulators* (only available in English)

IAEA-TECDOC-1016:May 1998, *Modernization of instrumentation and control in nuclear power plants* (only available in English)

IAEA-TECDOC-1140:March 2000, *Effective handling of software anomalies in computer based systems at nuclear power plants* (only available in English)

IAEA-TECDOC-1327:2002, *Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants* (only available in English)

IAEA-TECDOC-1328:2002, *Solutions for cost effective assessment of software based instrumentation and control systems in nuclear power plants* (only available in English)

IAEA-TECDOC-1402:2004, *Management of life cycle and ageing at nuclear power plants: improved I&C maintenance* (only available in English)

IAEA-TRS-384:1999, *Verification and validation of software related to nuclear power plant instrumentation and control* (only available in English)

² To be published.

IAEA-TRS-387:1999, *Modern instrumentation and control for nuclear power plants: a guidebook* (only available in English)

IAEA-50-SG-D11:1986, *General design safety principles for nuclear power plants; A safety guide*

Reports prepared within the framework of the International Working Group on Nuclear Safety

SRS:1998 (No 6), *Safety issues for advanced protection, control and human-machine interface systems in operating nuclear power plants* (only available in English)

NS-R-1:September 2000, *Safety of nuclear plants: design* (only available in English)

NS-G-1.1:September 2000, *Software for computer based systems important to safety in nuclear power plants* (only available in English)

NS-G-1.3:March 2002, *Instrumentation and control systems important to safety in nuclear power plants* (only available in English)

NS-G-2.3:October 2001, *Modifications to nuclear power plants* (only available in English)

NS-R-2:2000, *Safety of nuclear power plants: operation* (only available in English)

GS-G-1.4:August 2002, *Documentation for use in regulating nuclear facilities* (only available in English)

GS-G-4.1:May 2004, *Format and content of the safety analysis report for nuclear power plants* (only available in English)

INSAG-12:1999, *Basic safety principles for nuclear power plants 75-INSAG-3 Rev.1*(only available in English)

INSAG-14:1999, *Safe management of the operating lifetimes of nuclear power plants* (only available in English)

UK Health and Safety Executive: Nov 1997, AECB Canada, DSIN/ISPN France, NII UK, USNRC USA, *Four party regulatory consensus report on the safety case for computer based systems in nuclear power plants* (only available in English)

European Commission Report EUR 19265: May 2000, *Common position of European nuclear regulators for the licensing of safety critical software for nuclear power reactors* (only available in English)

SOMMAIRE

AVANT-PROPOS	54
INTRODUCTION.....	56
1 Domaine d'application et objet.....	58
2 Références normatives.....	59
3 Termes et définitions	60
4 Abréviations	62
5 Motivation de la modernisation	63
5.1 Généralités.....	63
5.2 Facteurs de motivation d'ordre économique.....	63
5.2.1 Généralités.....	63
5.2.2 Réductions des coûts	63
5.2.3 Revenu.....	63
5.2.4 Modernisation motivée par des raisons économiques	64
5.3 Facteurs de motivation relatifs à la sûreté	65
5.4 Synthèse des motivations d'une modernisation	65
6 Présentation générale de la décision de modernisation	65
6.1 Cycle de vie de l'I&C	65
6.2 Stratégie de l'I&C long terme.....	67
6.2.1 Généralités.....	67
6.2.2 Evaluation préliminaire de l'état des systèmes d'I&C et des besoins futurs.....	67
6.2.3 Priorités de renouvellement/mise à niveau des systèmes d'I&C	68
6.2.4 Conditions limites budgétaires	68
6.2.5 Evaluation des différents scénarii de modernisation	68
6.3 Etudes de faisabilité.....	69
6.3.1 Généralités.....	69
6.3.2 Evaluation des conditions préalables et objectifs relatifs à la centrale	70
6.3.3 Autorisation réglementaire.....	70
6.3.4 Coûts budgétaires préliminaires	71
6.3.5 Stratégie de réalisation.....	72
6.3.6 Evaluation de la documentation conforme à l'exécution	73
6.3.7 Spécification d'exigences de base	74
6.3.8 Affectation de fonctions	75
6.3.9 Analyse des tâches et fonctions pour l'IHM.....	75
6.3.10 Gestion de données.....	76
6.3.11 Outils de conception	76
6.4 Spécifications pour l'appel d'offre et achat de systèmes élémentaires	77
6.4.1 Généralités.....	77
6.4.2 Spécifications des propriétés du système d'I&C pour les solutions candidates.....	77
6.4.3 Cahier des charges	78
6.4.4 Offres pour chaque système	78
6.4.5 Commande	79
7 Eléments de réflexion concernant la modernisation	79
7.1 Généralités.....	79
7.2 Aspects technologiques.....	79
7.3 Considérations économiques.....	80

7.4	Codes et normes réglementaires	81
7.5	Politique générale de l'entreprise et codes d'ingénierie	81
7.6	Besoins futurs du système de sûreté et de commande du procédé	82
7.7	Fiabilité du système d'I&C	84
7.8	Etude des risques et avantages.....	84
7.9	Classement de sûreté.....	84
7.10	Exigences relatives à la qualification d'équipement	85
7.11	Exigences de qualification de logiciels.....	85
7.12	Contraintes physiques	86
7.13	Disponibilité de l'équipement (livraison et assistance technique)	87
7.14	Ergonomie.....	87
7.15	Analyse de défense en profondeur et de diversité (analyse DPD).....	89
7.16	Séparation et protection contre les incendies et les inondations	90
7.17	Incertitude et calcul des points de consigne	90
7.18	Analyse du temps de réponse	91
7.19	Procédures d'essais	91
7.20	Gestion de la documentation	91
7.21	Mise à niveau de la documentation technique de la centrale	92
7.22	Formation et qualification du personnel	93
7.23	Organisation du projet.....	94
7.24	Gestion de configuration.....	94
7.25	Interfaces vers les autres systèmes existants.....	94
7.26	Standardisation	94
8	Réalisation	95
8.1	Remarques générales	95
8.2	Architecture cible	95
8.3	Ordre des étapes de mise à niveau	96
8.3.1	Généralités.....	96
8.3.2	Choix du nombre de lots de travaux.....	97
8.3.3	Définition des lots de travaux.....	97
8.3.4	Exploitation parallèle et remplacement de l'équipement en puissance	98
8.3.5	Ordre des lots de travaux	99
9	Recommandations.....	99
	Bibliographie.....	101
	Figure 1 – Structure de la CEI 62096	59
	Tableau 1 – Phases du cycle de vie de l'I&C.....	66

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTES POUR LA SÛRETÉ – GUIDE POUR DÉCIDER D'UNE MODERNISATION

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 n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
- 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 propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l'état de la technique.

La CEI 62096, qui est un rapport technique, 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.

Cette seconde édition annule et remplace la première édition publiée en 2002.

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

- mise à jour du format du document conformément aux directives ISO/CEI en vigueur portant sur la présentation,
- mise à jour des références en prenant en compte les normes publiées depuis la publication de la première édition,
- mise à jour de la terminologie,
- prise en compte d'un certain de nombre d'éclaircissements proposés par les Comités Nationaux.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
45A/711/DTR	45A/726/RVC

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

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 maintenance 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.

INTRODUCTION

a) Contexte technique, questions importantes et structure de ce rapport technique

Les procédures classiques d'analyse de sûreté d'une centrale, de son exploitation et de sa maintenance renseignent sur les éventuels besoins de remplacement ou de mise à niveau. Après de nombreuses années d'exploitation, les systèmes de contrôle commande (CC) ne sont peut être plus conformes aux exigences de sûreté courantes ou prévues prochainement. Ils peuvent aussi être obsolètes ou peu fiables, ou ne plus être aptes aux allongements de durée de vie. Dans ces conditions, la modernisation permet d'adapter les systèmes d'I&C afin de satisfaire aux exigences ou pour faire face aux problèmes et aux coûts relatifs à l'obsolescence ou au vieillissement du matériel. Les avantages offerts par un matériel d'I&C moderne peuvent être évalués au cours de la modernisation.

L'objectif du présent rapport technique est d'être utilisé par les exploitants de centrales nucléaires, les évaluateurs de système et par les régulateurs.

b) Position du présent rapport technique dans la collection de normes du SC 45A de la CEI

La CEI 62096 en tant que rapport technique est un document du SC 45A de la CEI de quatrième niveau qui s'attaque à la question de la modernisation.

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

c) Recommandations et limites relatives à l'application du présent rapport technique

Il n'existe aucune recommandation ou limitation particulière concernant l'utilisation du présent rapport technique.

d) Description de la structure de la collection des normes du SC 45A de la CEI et relations avec les documents 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 CEI 61513. Cette norme traite des exigences relatives aux systèmes d'I&C et équipements d'instrumentation utilisés pour accomplir les fonctions importantes de 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 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 CEI 61513, sont relatives à des matériels particuliers, à des méthodes techniques 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 publication fondamentale de base CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales des Parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la Partie 3 de la CEI 61508 pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA (maintenant remplacé par le document AIEA GS-R-3) 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 du SC 45A sont conformes à celles utilisées par l'AIEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – GUIDE POUR DÉCIDER D'UNE MODERNISATION

1 Domaine d'application et objet

Ce rapport technique est destiné à aider les propriétaires de centrales nucléaires lors du processus décisionnel et pendant la préparation de la modernisation partielle ou totale de l'I&C. Pour cela, il propose:

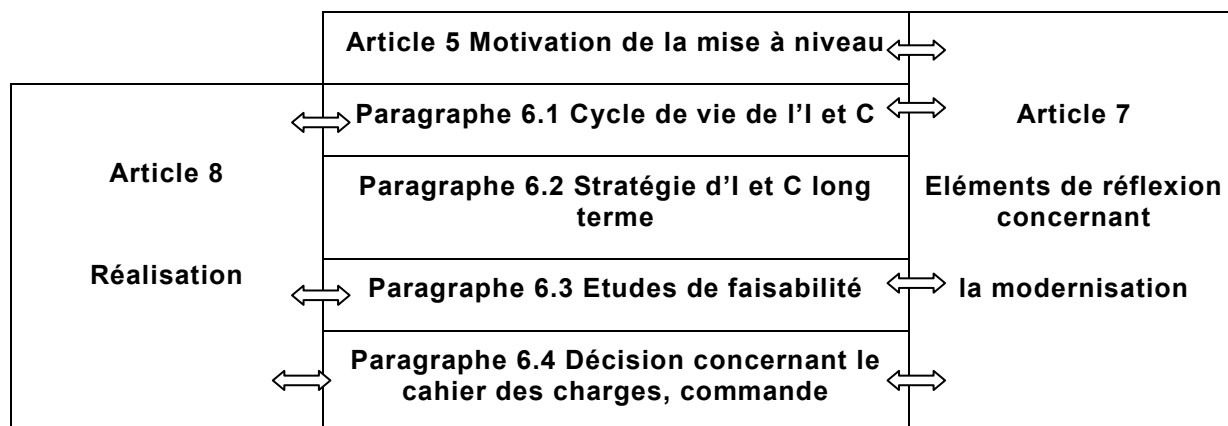
- un rappel des facteurs motivant une modernisation de l'I&C,
- les principales options pour l'élaboration de différents scénarios de modernisation de l'I&C,
- les critères économiques et techniques pour le choix d'une stratégie d'I&C à long terme,
- les principaux aspects à prendre en compte dans une étude de faisabilité technique détaillée.

De plus, ce rapport contient des recommandations détaillées et des conseils pratiques pour:

- l'analyse technique de l'état réel des systèmes d'I&C,
- le contenu du cahier des charges de l'I&C et la gestion de projet selon les recommandations contenues dans les rapports TECDOC 1016 et 1066 de l'AIEA,
- une réflexion sur la stratégie de modernisation.

Une attention particulière est portée à l'amélioration de l'IHM et de la sûreté du réacteur. Ce rapport ne fournit pas d'exigence de conception pour le CC. Nous supposons que les Codes et Guides de l'AIEA sont utilisés comme documents de haut niveau pour cela, alors que les publications de la CEI servent essentiellement à la conception des systèmes, ainsi qu'à la définition des exigences portant sur les équipements et sur certaines méthodes de travail. Les références des rapports de l'AIEA et certains autres documents contenant des renseignements plus détaillés sur des domaines spécifiques sont fournies.

La structure du rapport est donnée dans la Figure 1. Il est recommandé de respecter l'ordre suivant: résumer d'abord les motivations les plus évidentes (Article 5) puis monter un projet qui procède par étapes structurées et de plus en plus détaillées: Stratégie d'I&C long terme – Etudes de faisabilité – Cahier des charges pour l'appel d'offre et commande (Article 6). Les Articles 7 et 8 peuvent servir de liste de contrôle à chaque étape.



IEC 437/09

Figure 1 – Structure de la CEI 62096

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. 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 60050-191:1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-3:2004, *Gestion de la sûreté de fonctionnement – Partie 3-3: Guide d'application – Evaluation du coût du cycle de vie*

CEI 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

CEI 60880:2006, *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 61513, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

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

CEI 61888, *Centrales nucléaires de puissance – Instrumentation importante pour la sûreté – Détermination et maintenance des points de consigne*

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

CEI 62342:2007, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Gestion du vieillissement*

AIEA-TECDOC-1066:1999, *Specification of requirements for upgrades using digital instrument and control systems* (disponible en anglais seulement)

AIEA-TECDOC 1147:2000, *Management of aging of I&C equipment in nuclear power plants* (disponible en anglais seulement)

AIEA:2007, *Glossaire de sûreté de l'AIEA – Terminologie employée en sûreté nucléaire et radioprotection*

3 Termes et définitions

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

3.1

disponibilité

aptitude d'un élément à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée

[VEI 191-02-05, modifié]

NOTE Cette aptitude dépend d'un ensemble d'aspects: performance en matière de fiabilité, de maintenabilité et de support de maintenance.

3.2

gestion de configuration

processus consistant à identifier et à consigner les caractéristiques des structures, systèmes et composants (y compris des systèmes informatiques et des logiciels) d'une installation, et à s'assurer que les modifications de ces caractéristiques sont correctement élaborées, évaluées, approuvées, publiées, mises en œuvre, vérifiées, enregistrées et incorporées dans la documentation relative à cette installation

[Glossaire de sûreté de l'AIEA, 2007]

3.3

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»

[CEI 60964, 3.13]

3.4

système d'I&C

système exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même. Sa technologie est électrique et/ou électronique et/ou électronique programmable

Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées

[CEI 60964, 3.14]

3.5

cycle de vie

intervalle de temps entre la conception d'un produit et son démantèlement

[CEI 60300-3-3, 3.1]

3.6

coût du cycle de vie

coût cumulé d'un produit tout au long de son cycle de vie

[CEI 60300-3-3, 3.3]

3.7

maintenabilité

probabilité de mener à bien, pendant une période donnée, une action d'entretien sur un constituant ayant des conditions d'utilisation données, cet entretien étant effectué dans des conditions fixées et suivant des procédures et des moyens fixés

[VEI 191-02-07, modifié]

3.8

modernisation

remplacement ou remise à jour à l'aide de systèmes ou de composants plus récents. Remplacement est le terme à utiliser lorsque les exigences ne changent pas; remise à jour est le terme à utiliser lorsque le niveau d'exigences augmente.

NOTE 1 Les termes amélioration, remise en état ou à niveau, rénovation sont similaires et souvent interchangeables. Seules les nuances diffèrent (AIEA-TECDOC-1066).

NOTE 2 Les termes remplacer et renouveler sont similaires et interchangeables. Les termes sont utilisables du simple composant unique au système d'I&C complet.

[CEI 62342, 3.10]

3.9

sûreté nucléaire

obtention de conditions d'exploitation correctes, prévention des accidents ou atténuation de leurs conséquences, avec pour résultat la protection des travailleurs, du public et de l'environnement contre les risques radiologiques indus

NOTE Souvent abrégé en « sûreté » dans les normes des publications de l'Agence sur la sûreté nucléaire, en particulier lorsque d'autres types de sûreté (par exemple sûreté incendie, sûreté industrielle générale) sont examinées.

[Glossaire de sûreté de l'AIEA, 2007]

3.10

exigence

expression dans le contenu d'un document formulant les critères à respecter afin de prétendre à la conformité avec le document, et avec lesquels aucun écart n'est permis

[Directives ISO/CEI, partie 2, 2004, 3.12.1]

NOTE 1 Dans les documents du SC 45A de la CEI on distingue les types d'exigences suivant:

Exigences de sûreté – Exigences imposées par les autorités en matière de sûreté de la centrale nucléaire, en ce qui concerne l'impact sur les personnes, la société et l'environnement pendant le cycle de vie de la centrale nucléaire.

Exigences fonctionnelles et de performances – Les exigences fonctionnelles indiquent les réactions que doit adopter le système pour répondre à des conditions ou des signaux particuliers, et les exigences de performances définissent des caractéristiques telles que le temps de réponse et la précision.

Exigences opérationnelles – Exigences concernant l'aptitude et la capacité opérationnelles de la centrale imposées par le propriétaire.

Exigences de conception de la centrale – Exigences techniques portant sur la conception globale de la centrale afin de garantir le respect des exigences en matière de sûreté et les exigences opérationnelles de la centrale.

Exigences de conception du système – Exigences de conception de systèmes individuels permettant que la conception de la centrale complète satisfasse aux exigences de conception de la centrale.

Exigences de conception d'équipement – Exigences concernant un équipement individuel qui lui permettent de respecter les exigences de conception du système.

NOTE 2 Le Glossaire de sûreté de l'AIEA (2007) contient la définition suivante:

Prescrit, prescription – Prescrit par une législation ou une réglementation (nationale ou internationale) ou par des fondements ou des prescriptions de sûreté de l'AIEA.

Les prescriptions (exigences) visées par cette définition de l'AIEA sont celles correspondant à la définition d'exigences de sûreté du SC 45A de la CEI.

3.11

spécification

document qui spécifie de manière complète, précise et vérifiable les exigences, le comportement de la conception ou autres caractéristiques d'un système ou composant et, souvent, les procédures permettant de déterminer si ces dispositions ont été satisfaites

[CEI 60880, 3.39]

4 Abréviations

CAO	Conception Assistée par Ordinateur
FDC	Fréquence de Dégradation du Cœur
DMC	Défaillance de Mode Commun
ADR	Accident de Référence
SDC	Système Distribué de Commande
CEM	Compatibilité Electromagnétique
IEM	Interférence Electromagnétique
RU	Recette Usine
IHM	Interface Homme Machine
E/S	Entrée/Sortie
I&C	Instrumentation et Contrôle-Commande
APRP	Accident de Perte du Réfrigérant Primaire
MCO	Maintien en Conditions Opérationnelles
SPA	Surveillance Post-Accidentelle
API	Automate Programmable Industriel
EPS	Etudes Probabilistes de Sûreté
RS	Recette Site
SNCC	Système Numérique de Contrôle-Commande

V&V logiciel	Vérification et Validation du logiciel
VDU	Unité de visualisation
Analyse DPD	Analyse de Défense en Profondeur et de Diversité

5 Motivation de la modernisation

5.1 Généralités

Les facteurs motivant la modernisation peuvent être répartis en deux catégories selon leurs principaux avantages: économique et en termes de sûreté. Le remplacement d'un équipement d'I&C par un équivalent plus moderne entraîne généralement une amélioration fonctionnelle ainsi qu'une amélioration des performances, mais il est probable que la plupart des mises à niveau sont principalement motivées par des problèmes rencontrés par l'ancien équipement plutôt que par les avantages escomptés avec le nouveau.

5.2 Facteurs de motivation d'ordre économique

5.2.1 Généralités

Il convient d'optimiser le rendement économique en chiffrant le coût du cycle de vie, en prenant en compte non seulement les coûts les plus bas, mais aussi l'augmentation de la production.

5.2.2 Réductions des coûts

On peut obtenir des réductions de coûts dans les domaines suivants:

- Les coûts d'exploitation peuvent être réduits en améliorant l'efficacité, ce qui génère des économies de combustible, de consommation d'énergie, de consommables ou de besoins en main d'œuvre pour l'exploitation.
- Les frais de maintenance peuvent être réduits en allongeant les intervalles entre les entretiens et/ou en réduisant le temps et l'effort requis pour les tâches de maintenance. En améliorant la fiabilité de l'équipement, on peut réduire le coût des travaux de réparation et du stock de pièces de rechange. De plus, la réduction du nombre de familles d'équipement grâce à l'utilisation d'une plate-forme système unique permet de réduire le stock de pièces de rechange. Dans certains cas, une conception intégrant un niveau de redondance élevé peut permettre une maintenance préventive durant le fonctionnement normal.
- Les coûts administratifs peuvent être réduits en améliorant la façon dont les informations sont collectées, traitées, stockées et présentées.

Il convient de prendre en compte les réductions de coûts dans le cadre d'une démarche centrée sur la réduction au minimum du coût total du système pour son cycle de vie prévu. Notons qu'une modernisation qui met en œuvre un type de composant coûteux, mais très fiable augmente le coût d'approvisionnement mais réduit les dépenses de maintenance à long terme et peut donner le coût de cycle de vie le plus bas.

5.2.3 Revenu

Le revenu peut être augmenté avec les façons suivantes:

- Niveau de production plus élevé
L'amélioration des systèmes de contrôle et de protection peut donner une plus grande confiance en l'état de la centrale, permettant ainsi une réduction des marges de sûreté pour un niveau de sûreté donné et autorisant une puissance plus élevée.
- Disponibilité accrue

La réduction des temps d'arrêt pour réparations, maintenance de routine et rechargement en combustible, ainsi qu'une probabilité moins élevée d'arrêt d'urgence intempestif, permet une meilleure utilisation de la centrale. Pour cela, on peut améliorer la fiabilité et la stabilité, et recourir à des systèmes «intelligents» dotés de fonctions d'auto-vérification, de diagnostics et d'auto-étalonnage ; on peut améliorer le soutien à l'opérateur grâce aux fonctions d'I&C et à l'IHM. La mise à niveau des équipements obsolètes réduit la probabilité d'arrêt prolongé pour cause d'indisponibilité de pièces de rechange.

– Augmentation de la durée de vie de la centrale

Prolonger l'exploitation de la centrale au-delà de sa durée de vie économique prévue peut dégager des bénéfices considérables, au sens comptable, dans la mesure où les revenus ne seront plus amputés des charges de capital. Il est nécessaire de moderniser tout équipement ou système dont la durée de vie anticipée sera insuffisante par rapport au prolongement prévu de la durée de vie de la centrale.

5.2.4 Modernisation motivée par des raisons économiques

Une modernisation motivée par des raisons économiques peut être déclenchée par un ou plusieurs des facteurs suivants:

– Obsolescence

L'obsolescence de l'équipement intervient vers la fin du cycle de vie d'un produit. Quand une pièce n'est plus en production, le niveau de service fourni par son fabricant diminue et les pièces de rechange et consommables ne sont plus disponibles ou alors à un prix prohibitif. L'obsolescence concerne aussi les composants électroniques, où le cycle de vie peut ne durer que quelques années.

La première conséquence de l'obsolescence est d'augmenter les coûts et délais de maintenance et de réparation. A terme, l'équipement sera rendu hors service pour cause d'indisponibilité de pièces de rechange.

– Compétence du personnel

Au point précédent s'associe la difficulté de plus en plus grande de trouver du personnel de maintenance ayant la formation adéquate. Le personnel formé récemment ne possède pas le savoir-faire nécessaire en électronique analogique. L'enseignement et les formations techniques ont tendance à se concentrer sur la technologie numérique.

– Vieillesse

Les effets du vieillissement dont souffrent les composants et assemblages électroniques peuvent entraîner des problèmes de bruit, de dérive, de temps de réponse, de susceptibilité aux IEM et d'une manière générale de réduction de la fiabilité.

Exemples de dégradation dues au vieillissement:

- effets chimiques tels que l'oxydation ou la corrosion, entraînant des contacts haute résistance au niveau des connecteurs, commutateurs et soudures,
- dessèchement de condensateurs électrolytiques,
- perte d'isolation due à l'accumulation de contamination de surface (en particulier pour l'équipement haute tension),
- les câbles et autres composants à base de matériaux organiques sont soumis aux effets de vieillissement (ex: fragilisation) quand ils sont exposés à la chaleur, aux rayonnements, à l'oxygène, etc,
- effets mécaniques tels que l'usure, le grippage et la perte de rappel de ressort, susceptibles à terme d'entraîner la défaillance des mécanismes des commutateurs, condensateurs, relais, etc.

– Problèmes de compatibilité

Il est parfois nécessaire de mettre à niveau un équipement qui pourrait être jugé satisfaisant parce que des modifications ont été effectuées autre part. Les exemples suivants traitent des questions de compatibilité:

- modifications concernant le réacteur ou le matériel associé ayant pour conséquence des exigences d'I&C différentes,

- modifications concernant d'autres équipements d'I&C utilisant des interfaces ou des protocoles de connexions plus récents.
- Problèmes d'exploitation
La modernisation de l'instrumentation et du contrôle commande peut devenir nécessaire pour satisfaire des exigences liées à l'exploitation telles que le passage du mode de fonctionnement en base au mode de fonctionnement en suivi de charge.

5.3 Facteurs de motivation relatifs à la sûreté

Une mise à niveau de la sûreté peut s'avérer nécessaire afin de satisfaire aux exigences réglementaires. Une telle amélioration peut avoir un coût important sans offrir d'avantages économiques apparents. Néanmoins, cette décision est finalement d'ordre économique ; ainsi il est recommandé à l'exploitant de comparer le coût de la mise à niveau avec celui associé aux restrictions d'exploitation de la centrale.

Les mises à niveau destinées à améliorer la sûreté peuvent être motivées par les facteurs suivants:

- recommandations d'une revue de sûreté,
- changements des exigences d'autorisation réglementaire,
- déficiences mises à jour par un incident ou événement devant être déclaré,
- déficiences révélées par des essais.

5.4 Synthèse des motivations d'une modernisation

Il convient d'élaborer un rapport, résumant les différents aspects de la modernisation; ce rapport constitue un outil décisionnel pour les futures actions. Dans la mesure du possible, le rapport comprend une analyse coût/bénéfice quand chaque argument peut être quantifié. L'Article 7 peut servir de liste de contrôle des aspects les plus importants. Une fois la décision prise d'explorer et de définir une modernisation, il convient de respecter la description du cycle de vie de l'I&C de l'Article 6.

6 Présentation générale de la décision de modernisation

6.1 Cycle de vie de l'I&C

Il est recommandé d'établir un cycle de vie de référence pour le projet de modernisation. Un cycle de vie type est donné comme modèle dans le Tableau 1.

Ce paragraphe concerne le cycle de vie de modernisation, et se base sur les résultats de l'Article 5 traitant des motivations d'une modernisation. Ce rapport technique s'appuie sur l'AIEA-TECDOC-1066, qui s'adresse surtout aux fournisseurs potentiels de services pour les centrales nucléaires. Il traite uniquement des phases de cycle de vie exigeant une activité spécifique des exploitants de la centrale. Le Tableau 1 donne, en relation étroite avec l'AIEA-TECDOC-1066, une présentation générale du cycle de vie des systèmes d'I&C.

Ce paragraphe traite des phases déterminant la stratégie de modernisation et le processus d'appel d'offre jusqu'à la commande de l'équipement neuf ou des modifications nécessaires de l'I&C de la centrale (voir de 1 à 3 dans le Tableau 1). Les phases suivantes du cycle de vie sont décrites:

- 6.2 Stratégie de l'I&C long terme,
- 6.3 Etudes de faisabilité,
- 6.4 Appels d'offres et achat des systèmes élémentaires.

L'Article 7, Eléments de réflexion sur la modernisation, et l'Article 8, Réalisation, fournissent d'autres renseignements, à utiliser le cas échéant dans les paragraphes concernés.

Tableau 1 – Phases du cycle de vie de l'I&C
(Voir aussi Tableau XI de l'AIEA-TECDOC-1066)

Phases du cycle de vie de l'I&C	
Stratégie générique de modernisation	Actions, plans et résultats associés
1 Stratégie de l'I&C long terme Répondre aux besoins d'exploitation de la centrale	Evaluation de l'état des systèmes d'I&C Priorités de renouvellement/mise à niveau Conditions budgétaires limites Différents scénarios de modernisation
2 Etudes de faisabilité	A. Etudes de faisabilité générique - Conditions préalables et objectifs relatifs à la centrale - Autorisation réglementaire - Coûts budgétaires préliminaires - Stratégie de mise en œuvre - Architecture d'I&C - Chronologie de la modernisation par étape
	B. Etudes de faisabilité technique - Evaluation de la documentation conforme à exécution - Spécification des exigences de base - Affectation de fonctions - Analyse des tâches et fonctions pour IHM - Acquisition des données et objectifs de conception
Phases de modernisation des systèmes individuels	Actions associées
3 Cahier des charges et achat des systèmes individuels ou CC complet	Spécification des propriétés d'I&C Spécification des exigences Offres des fournisseurs Commande au fournisseur
4 Spécification des systèmes individuels d'I&C	Spécification et plans validés pour: Validation du système (RU et RS) Exploitation et maintenance du système Formation du personnel
5 Réalisation du système Conception détaillée des systèmes d'I&C individuels Réalisation et intégration système	Documentation détaillée sur la production et l'installation, ainsi que guides de maintenance et d'exploitation Système prêts pour les essais
6 Recette usine (RU)	Système prêt pour expédition sur site Procès-verbal de RU
Etapas sur site	
7 Installation et réglage des systèmes individuels	Démarrage du reporting des défaillances de système
8 Documents contractuels et de formation	Tous documents contractuels fournis
9 Recette sur site (RS) et mise en service en centrale	Système prêt à l'exploitation Procès-verbal de RS

CEI/TR 62096

Tableau 1 (suite)

Phases du cycle de vie de l'I&C	
10 Exploitation et maintenance	Reporting permanent des défaillances de système Reporting des résultats des essais périodiques Mise à niveau du simulateur Formation des opérateurs
11 Déclassement	Plans de déclassement Stratégies de remplacement Evacuation et stockage définitif des systèmes

6.2 Stratégie de l'I&C long terme

6.2.1 Généralités

Une stratégie de l'I&C long terme permet la planification de la maintenance long terme de toutes les fonctions d'I&C nécessaires à l'exploitation de la centrale. La stratégie globale, les objectifs, la situation financière et les plans d'exploitation de la société ont un effet sur le programme de modernisation. Ces facteurs stratégiques ont une influence sur le travail plus détaillé des évaluations préliminaires et définissent les objectifs des études de faisabilité détaillées. Il convient que l'évaluation préliminaire identifie correctement ces facteurs.

6.2.2 Evaluation préliminaire de l'état des systèmes d'I&C et des besoins futurs

Il convient d'effectuer une évaluation préliminaire du potentiel de modernisation. Il est recommandé de présenter dans celle-ci les motifs fondamentaux de la modernisation, les objectifs de ces travaux et leurs principales conséquences pour l'exploitation, la sûreté et l'efficacité, en expliquant les avantages et le coût budgétaire attendus.

L'historique long terme d'exploitation et de maintenance des systèmes d'I&C individuels fournit les données d'entrée essentielles de cette étape:

- les comptes-rendus de défaillance contiennent des renseignements détaillés sur les modes spécifiques de défaillance, les niveaux spécifiques de défaut et les taux de défaillance quantifiés,
- l'apparition des défauts d'I&C et de leurs conséquences potentielles respectives sur la production d'énergie,
- le nombre total d'heures ouvrables annuelles consacrées à la maintenance et aux réparations, ainsi qu'à l'approvisionnement des pièces de rechange et de remplacement, sert de base de référence économique démontrant la tendance vers une augmentation des difficultés à obtenir des pièces de rechange obsolètes ou à réparer des systèmes d'I&C défaillants ou obsolètes,
- déclin progressif du niveau de compétence du personnel de la société exploitante et des fournisseurs concernant les systèmes d'I&C en exploitation.

Un bilan des documents correspondant aux critères ci-dessus, associé au planning d'exploitation de la centrale, permettent de décider l'ensemble des systèmes d'I&C à considérer pour une éventuelle modernisation, et de la priorité relative des différents systèmes d'I&C.

De plus, il convient de tenir compte du fait que dans le cas de défaillances de systèmes d'I&C de sûreté ou liés à la sûreté, un rapport spécifique peut être exigé par les autorités réglementaires, même si ces défaillances n'ont pas directement ou indirectement entraîné de danger ou de risque.

Il convient de vérifier que le CC soit conforme aux prescriptions de sûreté en vigueur, ainsi qu'aux prescriptions futures attendues. Concernant la démarche à suivre à propos des futures prescriptions de sûreté, il est recommandé que celle-ci fasse l'objet de décisions stratégiques et de planification prises à un niveau hiérarchique élevé. Il convient de prendre en compte ces prescriptions de sûreté et toute revue de sûreté de la tranche ou d'une autre tranche du même palier, (telles que celles de l'AIEA) en entrée de l'évaluation préliminaire des exigences.

Il est recommandé d'évaluer du point de vue des opérateurs et de la direction opérationnelle la fonctionnalité de l'I&C; il convient de préciser les améliorations nécessaires dans la synthèse de l'évaluation.

Il doit être clair dès le départ que le processus menant à une décision définitive concernant l'étendue des modernisations nécessite une démarche itérative, puisque les coûts de tout projet de modernisation ne seront déterminés correctement qu'à la suite d'un processus de consultation et d'appel d'offre. Il convient ensuite de comparer ceux-ci au cadre budgétaire dépendant de la situation économique de la centrale.

6.2.3 Priorités de renouvellement/mise à niveau des systèmes d'I&C

L'évaluation de l'état des systèmes d'I&C donne aussi les premières indications concernant les priorités de renouvellement ou de mise à niveau des systèmes d'I&C individuels. Les systèmes d'I&C concernés sont généralement regroupés selon leur priorité (c'est-à-dire selon si leur renouvellement/mise à niveau dans les prochaines années est impératif(ve), conseillé(e) ou souhaité(e)). Cette activité constitue une part essentielle de l'étude globale de faisabilité. Les étapes détaillées de la mise à niveau de ces systèmes d'I&C résultent des études de faisabilité technique suivantes:

- élaboration des plans techniques pour l'installation, la mise en service et l'exploitation des systèmes d'I&C concernés,
- détermination des configurations intermédiaires de système permettant l'exploitation de la centrale et étant aptes à obtenir l'autorisation nécessaire,
- réduction des coûts d'installations temporaires de systèmes ou d'interfaces au minimum.

L'Article 7 contient un examen plus détaillé du *besoin* de modernisation alors que l'Article 8 fournit plus de renseignements concernant l'*optimisation* des différentes étapes de modernisation.

6.2.4 Conditions limites budgétaires

Le cadre budgétaire des renouvellements/mises à niveau de l'I&C est défini par:

- la durée d'exploitation supplémentaire prévue pour la centrale,
- l'étendue des systèmes d'I&C à haute priorité de renouvellement/mise à niveau (systèmes «impératifs»),
- le coût annuel de la maintenance des systèmes d'I&C existants.

6.2.5 Evaluation des différents scénarii de modernisation

La décision d'inclure également le renouvellement/mise à niveau des systèmes «conseillés» ou «souhaités» dépend des coûts marginaux liés à ces systèmes et des bénéfices additionnels que le renouvellement ou la mise à niveau apporterait.

A partir des évaluations élaborées dans les paragraphes précédents, il convient de définir les différentes options pour les futures structures et technologies d'I&C. Ces définitions peuvent inclure la structure de l'I&C, les structures de plate-forme, les systèmes répartis ou une combinaison de technologie numérique et analogique et par relais.

Il convient que la stratégie de l'I&C long terme s'appuie sur l'évaluation économique complète d'un certain nombre de cas de figure concernant différentes options. Celles-ci dépendent fortement de la durée de vie prévue pour la centrale.

Il est recommandé que l'évaluation étudie différentes perspectives de durée de vie (si applicable) pour les hypothèses suivantes:

- aucune modernisation,
- modernisation des seuls systèmes «impératifs»,
- modernisation des systèmes «impératifs», «conseillés» et «souhaités».

Il convient que l'évaluation considère aussi:

- la modernisation échelonnée des systèmes concernés, ou
- une modernisation en une seule étape.

Il convient que cette évaluation prenne en compte:

- les frais anticipés d'exploitation et de maintenance des systèmes conservés,
- les coûts de modernisation prévus,
- les frais anticipés d'exploitation et de maintenance des nouveaux systèmes,
- la durée de vie des nouveaux systèmes,
- l'évaluation économique des risques relatifs à la disponibilité de la centrale ou au retrait de l'autorisation réglementaire pour cause de défaillances dues au vieillissement et à l'obsolescence de l'équipement,
- les autres aspects associés à la modernisation (voir 7.8, Etudes des risques et avantages).

Un ou deux scénarii optimaux ressortiront de cette évaluation. Ceux-ci constituent des choix possibles de stratégie de l'I&C long terme. Il convient d'en faire une analyse plus approfondie dans les études de faisabilité ultérieures. Puisque les évaluations ne peuvent à ce stade qu'être faites sur la base des estimations préliminaires des frais de modernisation, il convient de revoir ultérieurement les scénarii choisis sur la base des appels d'offres formels. Il est possible que quelques itérations soient nécessaires.

6.3 Etudes de faisabilité

6.3.1 Généralités

Lorsque la stratégie de l'I&C long terme montre le besoin de renouveler ou de mettre à niveau technique une certaine étendue de systèmes d'I&C, il est recommandé de démarrer des *études de faisabilité*.

Il est préférable de structurer en deux parties le champ total des études de faisabilité:

- dans les études de faisabilité *génériques* (voir 6.3.2 – 6.3.5), il convient d'identifier les systèmes et l'échelle de temps à consacrer au renouvellement/mise à niveau,
- dans les études de faisabilité *ultérieures*, il convient de se concentrer d'abord sur les aspects techniques de la faisabilité (voir 6.3.6 – 6.3.11).

Il est recommandé que la stratégie de l'I&C long terme soit évaluée principalement par le personnel du producteur d'électricité, éventuellement appuyés par des experts-conseils. Une équipe technique relativement importante et compétente est nécessaire afin de faire face à la quantité de travail et au besoin d'informations détaillées inhérent aux études de faisabilité. Si l'exploitant de la centrale ne dispose pas d'une telle équipe, la tâche peut être évaluée par des fournisseurs potentiels travaillant en collaboration étroite avec le personnel du producteur d'électricité. Pour un résultat optimal des études de faisabilité, une équipe mixte comprenant des membres de la société d'électricité et d'un fournisseur potentiel est recommandée. Une

telle démarche comporte cependant le désavantage d'une dépendance envers un seul fournisseur, ce qui peut lier la société d'électricité à ce fournisseur et avoir un impact sur les coûts. Afin d'éviter un engagement précoce envers un fournisseur spécifique, il convient que la société envisage la possibilité de commander des études de faisabilité à deux fournisseurs ou plus en parallèle.

6.3.2 Evaluation des conditions préalables et objectifs relatifs à la centrale

L'objectif principal de cette activité est d'identifier et de caractériser les objectifs globaux du renouvellement ou de la mise à niveau du système d'I&C. C'est habituellement le producteur d'électricité qui est le mieux placé pour identifier ces objectifs, qui constituent les données d'entrée les plus importantes des études de faisabilité.

La liste des objectifs peut inclure les points suivants:

- maintenir ou augmenter la sûreté,
- maintenir ou augmenter la capacité de la centrale et/ou son facteur de charge,
- simplifier la maintenance de la centrale,
- définir une disponibilité acceptable (fiabilité, maintenabilité et assistance technique) par rapport au coût du cycle de vie de l'I&C,
- s'assurer de la compétence du personnel en ce qui concerne les équipements anciens actuellement en place.

Tout en se concentrant sur les systèmes d'I&C à moderniser, il convient d'analyser les conditions techniques des renouvellements/mises à niveau prévu(e)s:

- les caractéristiques essentielles et l'espace physique disponible et nécessaire pour les produits envisagés,
- la capacité disponible de l'alimentation électrique et des autres services, et
- les revues produits destinées à identifier des technologies d'I&C adaptées et des familles d'équipement/fournisseurs en ce qui concerne:
 - les interfaces pour les systèmes d'I&C existants qu'il convient de conserver,
 - les exigences et les capacités du personnel d'exploitation et d'entretien,
 - les références selon le niveau d'autorisation réglementaire exigé,
 - l'IHM (voir 6.3.9 et 7.14),
 - une expérience passée de projets de modernisation similaires,
 - l'optimisation de l'équilibre entre équipement neuf et ancien,
- les attentes concernant le futur approvisionnement en pièces de rechange,
- l'assistance technique par le fournisseur,
- l'état de la documentation conforme à l'exécution.

Quand un renouvellement/mise à niveau du système d'I&C est envisagé, les ressources humaines suivantes sont à étudier:

- disponibilité de personnel de conception qualifié pour les besoins en ingénierie du système modernisé,
- disponibilité de personnel qualifié pour installer et mettre en service le système modernisé,
- disponibilité de personnel qualifié pour exploiter et entretenir le système modernisé.

6.3.3 Autorisation réglementaire

Les questions d'autorisation peuvent d'avoir un impact majeur sur le projet de modernisation. Dans la plupart des pays, il convient que le demandeur d'autorisation informe les autorités de sûreté, préalablement à toute modification des systèmes et équipements classés comme

importants pour la sûreté (IPS). Des méthodes adéquates acceptées des autorités peuvent déjà exister. Néanmoins, les exigences réglementaires spécifiques à la modernisation de l'I&C peuvent très bien ne pas exister ou être encore en phase d'élaboration. Il convient de tenir au courant les organismes de réglementation dès le début de la planification du projet. Même si la portée de la modernisation ne concerne pas directement la sûreté, il est recommandé que la société recherche tout impact potentiel de la modernisation prévue sur la sûreté dans les domaines où des changements sont prévus.

Afin de définir toutes les questions d'autorisation à prendre en compte pour le projet de modernisation, la réalisation d'une étude préliminaire de sûreté et son acceptation par l'organisme de réglementation sont recommandées le plus tôt possible.

L'étude de sûreté constitue la preuve apportée par le demandeur d'autorisation que:

- la justesse et l'exhaustivité des spécifications générales sont justifiées par rapport aux fonctionnalités du système prévu,
- le système est développé conformément à une norme compatible avec l'importance de l'application pour la sûreté,
- le système livré est conforme en tous points à ses exigences de spécification,
- des moyens et dispositions suffisants sont définis afin de garantir les performances exigées du système tout au long de sa durée de vie,
- le système est adapté à la mission prévue.

(Voir bibliographie pour plus de détails sur ce qui peut être nécessaire pour l'étude de sûreté.)

Une fois le domaine d'application et la méthodologie définis, l'effort total requis pour satisfaire aux demandes du régulateur peut être déterminé, et il devrait être possible de minimiser ou d'éliminer les risques associés à la satisfaction de toute exigence émergente d'autorisation.

Il convient de définir et de valider le plus tôt possible un ensemble complet de critères de conception de l'I&C. L'analyse de sûreté de l'installation existante devra éventuellement être mise à niveau. Il est recommandé d'examiner la sûreté et les marges de sécurité opérationnelles du système d'I&C de la centrale qui ne sont pas explicitement traitées dans les documents existants, ainsi que de noter les résultats. Il sera peut être nécessaire de réviser l'EPS du système mis à niveau.

En préparant sa demande d'autorisation, il est recommandé que le producteur d'électricité prenne en compte l'expérience de l'autorité concernée en matière d'autorisation de systèmes de contrôle commande numérique de sûreté. L'effort requis pour la démonstration de sûreté peut varier selon que:

- l'autorité possède déjà une expérience de l'évaluation de systèmes d'I&C numériques de sûreté, ou
- une expérience d'autorisation de solutions comparables mises en œuvre dans d'autres pays peut être transposées jusqu'à un certain point,
- les systèmes prévus ont déjà été conçus ou pré-qualifiés conformes aux normes usuelles et aux exigences en matière de sûreté, ou
- le système a déjà été évalué par un organisme de réglementation.

Quand des solutions innovantes sont proposées, il convient que le producteur d'électricité s'attende à devoir soumettre des justifications spécifiques.

6.3.4 Coûts budgétaires préliminaires

Pour garantir la réussite de la modernisation, il est nécessaire que l'ensemble des systèmes d'I&C à renouveler ou à mettre à niveau soit défini conformément au cadre budgétaire. Ceci

passé généralement par un processus itératif. Il est utile d'intégrer un plafond financier préliminaire en entrée des études de faisabilité, puisque cette limite est un facteur déterminant dans le choix des solutions envisageables. Il est recommandé d'inclure dans le budget une provision pour tout élément supplémentaire coûteux tel qu'un simulateur de formation et un V&V logiciel.

Bien entendu, la préparation d'une offre contractuelle nécessite une liste détaillée des livrables et des services. Un des principaux objectifs des études de faisabilité est d'évaluer les coûts budgétaires afin de préparer le processus d'appel d'offre.

Les frais habituels comprennent:

- les frais de capitaux et d'équipement,
- les frais détaillés d'ingénierie relatifs à la mise en œuvre du système d'I&C et à la reprise de l'existant (voir 6.3.6 et 7.21),
- les frais de démontage, d'installation et de mise en service,
- les frais d'exploitation et de maintenance du système modernisé,
- les frais de documentation et de formation du personnel d'exploitation et de maintenance,
- le coût du manque à gagner pendant la période d'indisponibilité pour modernisation du système d'I&C.

6.3.5 Stratégie de réalisation

6.3.5.1 Généralités

Il convient que la stratégie de réalisation soit suffisamment détaillée pour que l'impact technique et économique d'approches alternatives puisse être analysé.

Il est recommandé que la stratégie intègre les exigences d'exploitation et de maintenabilité. Les CC pour le réacteur et pour la turbine peuvent nécessiter des stratégies différentes. Si une grande partie du câblage existant ne convient pas pour cause de vieillissement, de dégradations mécaniques, etc., il convient d'envisager d'importantes modifications de la conception et de la stratégie.

Les deux éléments principaux déterminant le choix de la stratégie de réalisation sont:

- la définition de l'architecture globale de l'I&C,
- la définition l'enchaînement des étapes du renouvellement/mise à niveau, et plus particulièrement la définition des interfaces avec le matériel restant, et la minimisation des arrêts de tranche.

6.3.5.2 Architecture globale de l'I&C

La définition de l'architecture globale doit tenir compte de la conception générale révisée de la centrale et de l'ensemble des systèmes d'I&C, systèmes existants qui resteront en service et systèmes qui seront modernisés. Les entrées de cette activité sont l'architecture conforme à l'exécution, associée au classement de sûreté des fonctions d'I&C, ainsi que (dans une première étape) une répartition grossière de l'I&C en ensembles fonctionnels et un classement selon leurs priorités de remplacement.

Ceci permet de décomposer le CC global en plusieurs ensembles, chacun ayant des caractéristiques particulières, et de pré-affecter les fonctions d'I&C à des systèmes d'I&C dans le but de s'assurer que chaque système:

- puisse offrir des performances matériel acceptables,
- soit soumis à des exigences de qualification et d'autorisation cohérentes.

Cette approche permet aussi de faire face aux exigences d'une approche «défense en profondeur» ou aux exigences de diversification par rapport à l'objectif commun de sûreté de la centrale.

6.3.5.3 Chronologie de la modernisation

Le second élément de la stratégie de réalisation est la séquence optimale de réalisation des différentes étapes de la modernisation de l'I&C. Elle doit prendre en compte les différentes priorités des systèmes à remplacer, ainsi que les conditions aux limites à considérer dans le projet. La décision de moderniser tous les systèmes d'un coup ou de scinder l'installation sur plusieurs arrêts de tranche en dépendra. Les critères types à prendre en compte sont les suivants:

- possibilité d'identifier des sous-systèmes pouvant être séparés sans besoin d'interfaces intermédiaires,
- possibilité d'effectuer des travaux de préparation ou l'installation pendant le fonctionnement en puissance,
- possibilité de renouvellement coordonné avec une modernisation de systèmes mécaniques ou électriques,
- main d'œuvre sur place,
- aspects économiques, y compris des considérations relatives à la trésorerie.

L'étude de faisabilité ne doit pas nécessairement faire ressortir une séquence optimale de réalisation; cependant, il convient qu'elle indique les différentes possibilités afin de permettre une première évaluation de leur impact technico-économique sur le projet global. L'ordre détaillé de réalisation ne doit être élaborée que plus tard, une fois que le fournisseur a été choisi et que les caractéristiques détaillées du nouveau système d'I&C sont connues. L'Article 8, Stratégies de réalisation, apporte des orientations supplémentaires pour ces deux phases.

6.3.6 Evaluation de la documentation conforme à l'exécution

Cette étape des études de faisabilité sert de préparation pour l'évaluation de la spécification des exigences et fournit aussi des données d'entrée pour l'appel d'offre.

Il est recommandé d'effectuer une revue de dimensionnement couvrant les exigences fonctionnelles, physiques et réglementaire. Il convient que toute modification ou écart par rapport à la base de calcul existante soit identifiée par rapport à la modernisation. Il est recommandé que la base de calcul soit identique à l'ancienne, à moins qu'une mise à niveau de la base de calcul soit nécessaire suite à de nouvelles exigences réglementaires, de nouvelles spécifications d'équipement ou de futurs besoins prévus par la société d'exploitation. Il convient aussi que la revue s'assure que la modernisation n'entraîne pas le déclassement de la base de calcul existante. Il convient de porter une attention particulière aux fonctions à sûreté intégrée.

Il est recommandé que la revue vérifie que toute la documentation nécessaire et conforme à l'exécution est disponible et exacte. Si ce n'est pas le cas, il est recommandé qu'elle fournisse les moyens et les actions nécessaires à la correction des manquements. Des inspections sur site peuvent permettre de faire des vérifications sur le terrain des documents, et révèlent souvent des caractéristiques importantes qui ne sont pas apparentes dans la documentation.

Dans ce contexte, les principaux documents intéressants sont:

- les exigences de conception de système, informations sur l'équipement, expérience d'exploitation passée, notifications de modification technique passées (modification),
- rapports de sûreté,
- spécifications de conception des fonctionnalités,
- schémas fonctionnels,

- points de consigne,
- précision,
- constantes de temps et temps de retard admissibles,
- paramètres procédé,
- liste des signaux (analogiques et contacts),
- algorithmes de traitement, avec les définitions et les schémas type logiques fonctionnels d'exploitation,
- exigences de qualification,
- schémas électriques des armoires et plannings de connexion,
- schémas de routage des câbles,
- spécifications de conception de l'IHM,
- plans d'agencement des indicateurs et commandes dans la salle de commande principale et le panneau de repli,
- spécifications de conception pour le système d'information procédé,
- procédures de conduite.

6.3.7 Spécification d'exigences de base

Il est recommandé de prendre en compte lors de la préparation de la spécification des exigences de base les événements de dimensionnement, c'est à dire les événements initiateurs hypothétiques, ainsi que les séquences d'événements qui en découlent. Il convient de prendre autant que possible en compte les accidents hors dimensionnement et les accidents graves.

Les exigences de base s'appuient d'abord sur les spécifications de la conception originale et sur la documentation conforme à l'exécution. Ensuite, il convient de prendre en compte les exigences et recommandations résultant des études citées plus haut.

Celles-ci traduisent en grande partie l'expérience de l'exploitation de la centrale depuis sa mise en service, mais aussi les avantages et fonctionnalités escomptés liés au nouveau CC, tels que le traitement des défaillances de signaux, la gestion des codes de qualité des signaux, le filtrage numérique, l'étalonnage à distance et les fonctions de diagnostic.

Lors des mises à niveau fonctionnelles prévues, il convient de s'assurer de la disponibilité de mesures et actionneurs adéquats.

En ce qui concerne le CC relatif à la sûreté, toute mise à niveau fonctionnelle ou fonctionnalité étendue sera intégrée dans la démonstration de sûreté et il convient de justifier leur validité.

Il est recommandé que la spécification des exigences de base contienne une information adéquate sur les sujets suivants:

- exigences générales,
- exigences fonctionnelles,
- exigences matérielles, y compris les exigences relatives sismiques et celles relatives à l'environnement,
- domaine des fonctions et matériel,
- interfaces (signaux standards, types non-standard, types d'interfaces série, etc.),
- exigences d'installation,
- divers.

Le contenu préconisé est développé en 7.5 et la CEI 61513 contient des conseils détaillés pour le développement de l'architecture du système et l'affectation de fonctions.

Une fiche de spécification type est fournie dans l'AIEA-TECDOC-1066.

6.3.8 Affectation de fonctions

A partir des résultats des étapes de conception précédentes, les fonctions identifiées sont affectées aux systèmes d'I&C, et leurs sous-fonctions sont affectées aux sous-systèmes dans l'architecture de l'I&C globale.

Les activités principales lors de cette étape de conception sont:

- de vérifier que le domaine fonctionnel de chaque sous-système est accompagné d'une performance correcte du matériel,
- de vérifier que l'affectation de fonctions aux systèmes d'I&C indépendant satisfait aux exigences de «défense en profondeur » ou que les fonctions sont diversifiées, par rapport à l'objectif global de sûreté de la centrale,
- l'affectation des tâches au personnel d'exploitation et de maintenance.

6.3.9 Analyse des tâches et fonctions pour l'IHM

La spécification des exigences de base conduit à l'affectation de fonctions aux opérateurs et aux systèmes d'I&C. Dans les cas où l'affectation de fonctions ne correspond pas à la conception de l'I&C existant, c'est à dire où il y a:

- modification du degré d'automatisation,
- introduction de systèmes supplémentaires,
- modifications du concept des essais périodiques et autres tâches de l'opérateur,
- migration du VDU vers une conduite informatisée,
- changement d'implantation du pupitre de conduite,

il convient d'effectuer une analyse des tâches afin de servir de base aux spécifications détaillées pour l'IHM. Il est recommandé que cette analyse prenne en compte non seulement les tâches de commande du procédé, mais aussi le rôle de l'opérateur dans les tâches de maintenance, d'entretien des systèmes d'I&C, de communication etc., puisque celles-ci sont impactées par la modernisation de l'I&C.

Il est recommandé ensuite que l'analyse des tâches permette la mise au point des exigences concernant:

- les informations disponibles aux opérateurs,
- les actions des opérateurs,
- la communication entre les membres de l'équipe,
- l'accessibilité, la visibilité, l'éloignement, la fréquence d'utilisation des instruments, etc..

Il convient que l'approfondissement et la portée de l'analyse soient compatibles avec l'étendue de la modernisation de l'I&C et avec le degré de similarité entre l'IHM existante et la nouvelle IHM. Dans le cas de modifications mineures, l'analyse pourrait se résumer à une évaluation du domaine à modifier et de l'absence d'impact négatif sur les fonctions non-modifiées. Une modification majeure, par contre, peut nécessiter une réévaluation complète des tâches de l'opérateur.

Cette analyse fournit une bonne base pour les spécifications de:

- la disposition des affichages de la salle de commande (pour la conception finale et les stades intermédiaires),

- le contenu, les formats et la conception des affichages sur les unités de visualisation,
- le traitement de données pour l'affichage de l'état des systèmes, y compris les systèmes complémentaires support des opérateurs,
- l'adaptation nécessaire des procédures d'exploitation existantes afin de convenir à l'IHM modifiée et aux nouvelles fonctions.

Il est recommandé que l'analyse des tâches serve à identifier les situations de travail comportant une charge de travail potentiellement importante et un risque d'erreur humaine, afin de les étudier plus en détail lors des études de cas de validation ultérieures. Celles-ci permettront de vérifier l'acceptabilité des charges de travail et l'adéquation de la conception finale de l'IHM.

Il est recommandé que des ingénieurs de sûreté et de méthodes participent à la sélection des situations d'exploitation à analyser, ainsi qu'à l'analyse des différents scénarios considérés par l'analyse des tâches.

6.3.10 Gestion de données

Afin de garantir la cohérence et la disponibilité de toutes les données de conception pour le cycle de vie complet d'un système d'I&C, il est essentiel, peu après le démarrage du projet, de planifier l'introduction et l'installation d'un système de base de données performant qui stocke toutes les données du projet concernant les capteurs, les actionneurs et autres dispositifs, les locaux de service, etc. Dans la mesure du possible, il est recommandé d'intégrer des aménagements permettant la réalisation ultérieure de liens automatisés vers les outils de conception. Il convient de prendre des dispositions afin d'assurer la cohérence des données partagées par plusieurs systèmes d'I&C. L'utilisation d'un système de gestion de bases de données (SGBD) standard est recommandé. Garantir la cohérence de la base de données dans la durée est un travail difficile et lourd.

Il convient que le système de base de données intègre le contrôle automatique de format pendant la saisie de données. Il faut savoir que l'installation complète d'un système d'I&C, y compris de la salle de commande, passe par l'identification, la saisie dans la base de données et le contrôle de plusieurs millions de données. Il s'avère fréquemment que la documentation de conception disponible sous forme de dessins et de listes d'instruments est périmée ou non satisfaisante. La validation sur site de ces données nécessite une méthode de correction des données erronées par rapport à celles constatées à la centrale qui soit à la fois souple et sécurisée, appuyée par une assurance qualité efficace.

6.3.11 Outils de conception

Il est recommandé que la méthodologie adoptée pour la rédaction de la documentation de conception pour le renouvellement/mise à niveau prévue du système d'I&C soit conforme aux exigences suivantes:

- il convient que la spécification soit compréhensible par les ingénieurs d'I&C et de sûreté, ainsi que par les évaluateurs et les ingénieurs fonctionnement,
- il convient que les formats de la spécification soient normalisés,
- il convient que les données de conception soient stockées dans un système de gestion de bases de données (avec AQ convenable) comportant une instance unique de chaque donnée et gérant toutes les phases du cycle de vie CC.

Il convient de préciser la convention utilisée pour l'affectation des noms des signaux internes, etc dans le système I&C. Il est recommandé que la méthodologie de conception aboutisse à une documentation claire et cohérente.

Si des affichages sur écran sont prévus pour l'IHM, il convient de noter qu'une centrale typique peut avoir besoin de plusieurs centaines d'affichages différents. Il est recommandé que la conception de ces affichages suive des pratiques ergonomiques, en particulier en suivant les normes de référence du projet relatives à la taille des caractères, la couleur, les

noms des systèmes élémentaires de la centrale, les types de mesures et les symboles utilisés pour désigner les différents équipements de la centrale tels que pompes et vannes. Il convient de s'assurer que le nombre de mesures affichées sur chaque écran est limité afin d'optimiser la clarté et faciliter la compréhension rapide par l'opérateur. Il est recommandé que les affichages montrent l'état courant de la centrale, avec la possibilité d'afficher des traces historiques. La conception de ces affichages peut être grandement facilitée par l'utilisation de bons outils, de préférence avec des fonctionnalités CAO et si possible des liens automatiques vers le système de gestion des bases de données pour les caractéristiques des signaux. Il convient d'entreprendre une étude ergonomique des modèles d'affichages. La CEI 61772 contient des conseils sur la conception des affichages.

Il convient d'utiliser les mêmes outils d'acquisition de données et de conception à la fois pour le projet et pour l'exploitation et la maintenance futures (voir aussi 7.20).

6.4 Spécifications pour l'appel d'offre et achat de systèmes élémentaires

6.4.1 Généralités

Les exigences pertinentes pour la réalisation du système d'I&C prévu sont documentées dans la phase de spécification des exigences de base du projet. Ces exigences doivent être décomposées et développées afin de former des exigences détaillées pour chaque système élémentaire faisant partie du projet global. Elles forment les spécifications des systèmes d'I&C et sont générées à partir des spécifications des exigences de base. Ces spécifications constituent le document de référence en entrée des offres des fournisseurs et des attributions de contrats qui s'ensuivent, de la conception détaillée, de la fabrication, de la production de logiciel et du travail d'installation. Il est important d'identifier clairement le périmètre d'intervention de chaque acteur du projet de modernisation, ainsi que le partage des responsabilités. Il convient de définir ces principes dans ces spécifications.

6.4.2 Spécifications des propriétés du système d'I&C pour les solutions candidates

Ce paragraphe décrit les exigences de base nécessaires à l'élaboration réussie des spécifications d'un système d'I&C. Les caractéristiques énumérées sont recommandées dans le but de faciliter l'obtention de l'autorisation réglementaire pour la réalisation des fonctions de catégorie A (CEI 61226). En ce qui concerne la réalisation de fonctions de catégorie moins élevée, on peut omettre ou diminuer les exigences de catégorie A selon la sûreté ou l'importance opérationnelle. Il est recommandé de traiter des points suivants dans les exigences:

- il convient que le matériel du système d'I&C soit homologué ou homologable afin d'assurer une robustesse convenable en ce qui concerne les séismes et l'environnement (CEI 60987, série CEI 61000, CEI 60780, CEI 60980, CEI 61513),
- le système doit être conforme aux exigences de redondance et de séparation de la CEI 60709,
- il convient que les logiciels possèdent une structure modulaire claire et un développement coordonné selon la CEI 60880 et la CEI 62138 ou d'autres normes logicielles applicables,
- il convient que le système d'I&C soit suffisamment souple et performant pour garantir la fonctionnalité requise, ainsi qu'un temps de réponse satisfaisant,
- il convient que le comportement exigé du système d'I&C soit indiqué et reflète son classement fonctionnel,
- il convient que le système possède une architecture ouverte, prise en charge par plusieurs fournisseurs.

Pour des raisons d'effort au niveau de la conception et la maintenance des logiciels tout au long du cycle de vie, l'état de l'art courant consiste à mettre en œuvre un atelier logiciel capable de générer du code automatiquement. L'obtention de l'autorisation réglementaire pour des systèmes numériques d'I&C peut être facilitée par:

- une procédure éprouvée de génération de code, s'appuyant sur des modules logiciels éprouvés,
- une représentation graphique des fonctions de l'application destinée à en faciliter la compréhension,
- l'intégration des contrôles formels afin de faciliter la vérification des résultats de conception,
- un langage informatisé standard pour la validation fonctionnelle, permettant ainsi l'utilisation directe du code généré dans le système cible,
- des outils validés, bien documentés et accessibles,
- une assistance à la gestion de configuration.

6.4.3 Cahier des charges

Il convient que la documentation des exigences détaillées de chaque système prenne la forme d'un cahier des charges pour le matériel, les logiciels, et les services requis. Quand plusieurs systèmes sont concernés, éventuellement fournis par des fournisseurs différents, il est préconisé de rédiger des spécifications communes concernant par exemple les tests de qualification en environnement, les normes de fabrication d'équipement ou les normes et exigences portant sur les logiciels; il est également recommandé de définir les services et interfaces du site.

Une condition préalable importante à l'édition des cahiers des charges et des appels d'offre est que le producteur d'électricité ou le commanditaire s'accorde sur une liste de fournisseurs potentiels convenables. Il est recommandé qu'ils possèdent une expérience de la classe d'équipement exigé, de la classe de travaux de modernisation, ainsi que du travail sur site, sachant que celui-ci peut être difficile d'accès.

Il convient que les offres comprennent la vérification de conformité aux exigences.

Il est recommandé de convenir de la méthode d'évaluation et des critères d'acceptation des offres avant d'envoyer le cahier des charges aux fournisseurs potentiels. Il est important que les fournisseurs sachent que l'évaluation sera exhaustive et équitable et qu'ils seront informés de leurs positions dans l'évaluation, car l'élaboration d'offres pour une centrale nucléaire nécessite un travail considérable.

6.4.4 Offres pour chaque système

Les fournisseurs potentiels doivent élaborer une conception préliminaire, en s'appuyant sur le cahier des charges qui leur est fourni. Celle-ci doit conduire à des offres commerciales et des propositions techniques adaptées aux systèmes concernés. S'il est exigé des soumissionnaires qu'ils incluent dans leurs offres des études de faisabilité, alors il convient que les termes de référence d'une telle étude soient clairs.

Une part importante du travail de modernisation peut s'avérer être la réutilisation de conceptions ou de logiciels existants, déjà fournis pour des applications similaires. Il est important que l'expérience opérationnelle et le contenu des conceptions et logiciels soient clairement décrits par le soumissionnaire et qu'il soit prêt à mettre à disposition toutes les informations, sous réserve de la signature d'accords de confidentialité adaptés, afin de permettre l'évaluation d'une telle réutilisation dans l'application. Il est recommandé que le projet examine les preuves de la qualité des logiciels afin de s'assurer qu'aucun problème ne surviendra plus tard pendant le processus d'autorisation réglementaire.

Il est recommandé que le fournisseur retenu donne des preuves de sa conformité aux exigences et de sa capacité à respecter le calendrier et les contraintes budgétaires. Des références concernant des installations antérieures seront fournies.

6.4.5 Commande

Une fois que les offres sont soumises et évaluées, et que l'acheteur et toute organisation commanditaire ont arrêté leur choix d'un commun accord, une commande formelle sera soumise au fournisseur retenu. Il convient qu'une partie de ce travail consiste à négocier de façon détaillée les options et autres considérations supplémentaires: accord sur tout élément non-conforme de l'offre, mise au point complète de tous les travaux (conception de câblage, analyse des tâches ou maquette d'écran d'affichage) que le producteur d'électricité souhaiterait éventuellement entreprendre lui-même, ainsi que les interfaces détaillées vers les parties restantes de la centrale.

Il est conseillé d'élaborer une nouvelle édition de tous les cahiers des charges contractuels, révisée de façon détaillée afin de traduire les accords convenus pendant la négociation du contrat, pour utilisation contractuelle ultérieure. Ce document peut s'appuyer sur le cahier des charges ou l'offre formelle. Il convient qu'il précise clairement l'interface entre le fournisseur et le client. Le document final sert ensuite de référence pour la conception, la réalisation et l'installation du système.

7 Eléments de réflexion concernant la modernisation

7.1 Généralités

Il convient que la modernisation du système d'I&C existant soit analysée d'un point de vue technico-économique au cours d'une phase préparatoire. Celle-ci comprend souvent une réflexion sur des questions examinées par la suite dans les différents paragraphes. Il convient de reprendre celles-ci dans le cahier des charges.

7.2 Aspects technologiques

Il convient de noter que de nos jours, le cycle de vie du matériel d'I&C se réduit progressivement, en raison d'une évolution rapide de la technologie électronique, support de l'I&C.

Les capteurs, transducteurs et unités de commande deviennent plus «intelligents», grâce à une conception faisant appel aux micro-contrôleurs embarqués. L'auto-étalonnage, les fonctions d'auto-test et les diagnostics intégrés sont désormais courants. La tendance est de convertir les mesures analogiques au format numérique à partir du frontal, aussi près que possible du capteur/transducteur (et du process). Les circuits analogiques utilisés pour l'instrumentation discrète deviennent petit à petit obsolètes et sont remplacés par leur équivalent numérique, ce qui dans certains cas offre une plus grande précision, une performance et une fiabilité améliorées.

Les boucles de commande analogique individuelles configurées avec des instruments analogiques discrets et des interconnexions en fil-à-fil petit à petit obsolètes et sont remplacées par une architecture de commande différente, basée sur des systèmes de commande numérique. Dans cette nouvelle architecture numérique, la boucle analogique physique, à l'exception du transducteur de signaux process et le dispositif de commande finale, est remplacée par un contrôleur numérique équivalent. La plate-forme pour cette architecture numérique peut être conçue autour d'un API ou d'un SDC. L'équivalent numérique de la boucle de commande peut éventuellement comporter un processeur dédié, ou peut être exécuté par l'un des différents modules de logiciels de commande.

Une fois qu'un signal de mesure d'un paramètre process entre dans le système de commande numérique par l'interface d'entrée, le transfert et le traitement du contenu du signal n'est plus effectué par matériel discret, ni par un câblage d'interconnexion. Les données sont transférées de façon numérique, par l'intermédiaire du réseau de communication (bus de données) et les algorithmes de commande sont exécutés par un logiciel. Les interconnexions fil-à-fil transfèrent le signal de commande au dispositif de commande final au niveau de l'interface de sortie du système de commande numérique.

Il convient de noter que grâce à la disponibilité de systèmes de commande numérique équipés de fonctions d'entrée-sortie à distance, on peut éliminer une bonne partie du faisceau principal qui était nécessaire pour les boucles de commande analogique discrètes classiques, en remplaçant ce câblage par des bus de données.

Le fait que tous les systèmes de commande numérique et l'instrumentation s'appuient sur l'exécution de programmes logiciels pour les calculs et la gestion de signaux de mesure et de commande met en avant la question du V&V logiciel. L'expérience actuelle de l'industrie nucléaire, basée sur l'interprétation par les organismes de réglementation des exigences V&V des systèmes informatiques de sûreté, fait qu'un temps significatif est nécessaire pour réaliser les tâches de V&V, même dans les cas où les modifications du code sont minimales, par exemple pour une modification de point de consigne.

Le matériel d'I&C choisi peut être sensible aux variations de température ambiante et il peut être nécessaire de placer cet équipement dans des locaux climatisés. Les systèmes de commande numériques peuvent également être sensibles aux IEM. Il est recommandé d'installer le nouvel équipement numérique dans un environnement blindé, garantissant un niveau d'IEM faible. Le matériel électronique est sensible aux rayonnements et il convient d'effectuer une qualification correspondant à son emplacement prévu, en prenant en compte les doses de rayonnement en exploitation normale et en conditions d'accident.

La décision de remplacer un système d'I&C à boucle de commande analogique discrète par un système à architecture numérique plus récent implique la résolution des points suivants:

- une approche raisonnable de la question de V&V, et l'acceptation des normes de recette du matériel fabriqué. Les normes CEI applicables se trouvent dans la bibliographie,
- l'étendue de la modernisation de l'I&C et les conséquences de l'existence de plusieurs architectures au sein de la même centrale. Concevoir du matériel numérique pour remplacer l'équipement analogique des boucles analogiques discrètes en utilisant le câblage existant ne devrait pas être difficile. Néanmoins, le remplacement de boucles analogiques complètes par un système de commande numérique entraînera des différences de matériel et de câblage,
- la compatibilité avec les SNCC de la centrale existante, l'interface/communications avec les nouveaux SNCC,
- la modernisation ultérieure, la migration vers de nouvelles générations de systèmes de commande et la protection contre l'obsolescence,
- il convient de noter que l'équipement numérique ne se comporte pas toujours de la même manière que son équivalent analogique ou à base de relais,
- la qualification du logiciel est un point important à prendre en compte avant de choisir un équipement numérique.

7.3 Considérations économiques

Il est possible de remplacer certaines parties des systèmes existants par des modules préfabriqués. L'intérêt des modules est de simplifier l'installation et de réduire les coûts, particulièrement pour les parties de systèmes de conception complexe ou installés dans un espace exigu. L'encombrement des modules serait comparable à celui de l'équipement système existant et ces derniers pourraient facilement être installés dans l'emplacement de l'équipement existant.

Il convient également de noter dans les considérations économiques le manque à gagner en termes de production perdue pendant la réalisation du système d'I&C modernisé, ainsi que le déclassement de la centrale entraîné par l'installation du système d'I&C modernisé.

On peut éviter des interruptions de service excessives en installant des parties du système pendant l'exploitation du réacteur dans la mesure du possible. La préfabrication des modules permet de réduire le temps passé et les expositions aux rayonnements pendant l'installation en centrale.

Si les composants du système d'I&C renouvelé ou mis à niveau sont situés dans l'enceinte de confinement, il convient de prendre en compte dans l'estimation des coûts, ceux d'évacuation des matières radioactives, de la main d'œuvre et des doses de rayonnement.

Il est possible de réduire les frais si le nouveau système permet d'effectuer des opérations de maintenance et des essais pendant l'exploitation de la centrale plutôt que pendant des périodes d'interruption.

Il est recommandé d'étudier les dernières découvertes en matière d'instrumentation, par exemple:

- Certains instruments intelligents permettent un auto-étalonnage ou un étalonnage à distance. Il convient d'étudier cette caractéristique pour les instruments nécessitant un étalonnage fréquent, surtout dans le cas des applications nécessitant un taux de disponibilité élevé ou une grande précision.
- Il existe des instruments capables de mesurer plusieurs paramètres à l'aide du même ensemble de capteurs: pression et température, ou débit, pression et température. Il convient d'évaluer l'intérêt économique de tels instruments. Cependant, il est important de prendre en compte la possibilité de perte simultanée de plusieurs paramètres process à cause de la défaillance d'un seul instrument.
- Il existe des émetteurs équipés de connexions au réseau local, permettant d'en interconnecter un nombre important, de façon à partager ensuite le même bus de données vers l'ordinateur de commande. Des économies peuvent être réalisées grâce aux besoins réduits de câblage et à la simplification des interfaces d'entrée des ordinateurs.
La possibilité d'une perte de données en cas de défaillance de bus de données est à prendre en compte.
- Un système de contrôle réparti offre une méthode rentable d'élimination des boucles de commande 100 % pneumatiques telles qu'elles sont parfois utilisées pour la régulation d'eau alimentaire.

Il convient de noter que le choix de produits innovants peut nécessiter une justification approfondie auprès des autorités réglementaires. Il convient dans ce cas rendre compte des moyens nécessaires.

7.4 Codes et normes réglementaires

Le système d'I&C modernisé doit probablement satisfaire aux normes et codes réglementaires en vigueur. Les codes et normes à utiliser et l'indice de révision applicables doivent être faire l'objet d'un accord et être endossés par les autorités avant la mise en œuvre de la conception technique et de l'approvisionnement de l'équipement. Ces codes et normes sont susceptibles de comprendre les guides et codes de sûreté de l'AIEA, les normes CEI et surtout tous codes et normes édités par l'organisme local de réglementation de la sûreté.

Les références utiles sont données dans la bibliographie.

7.5 Politique générale de l'entreprise et codes d'ingénierie

D'éventuelles modifications de la politique de la société et des codes techniques peuvent affecter la conception du système d'I&C modernisé.

Le choix d'un système d'I&C modernisé pour une tranche nucléaire doit tenir compte des critères importants ci-dessous:

- limiter le nombre de fournisseurs de système de commande afin de permettre une normalisation avec un système industriel de base efficace par rapport à son coût, conduisant à des coûts d'exploitation et de maintenance (MCO) réduits,
- choisir des fournisseurs dont il est connu qu'ils ont déjà mené à bien des projets,

- choisir une architecture ouverte prise en charge par plusieurs fournisseurs qui permette des opérations de modernisation au fur et à mesure de leur disponibilité, plutôt qu'une architecture propriétaire fermée provenant d'un seul fournisseur,
- envisager l'utilisation d'un système de commande normalisé partout dans la centrale, par exemple un SDC; sinon, il est recommandé de prévoir des normes d'interfaçage adaptées si plus d'un type de système de commande est retenu,
- limiter l'application de systèmes de contrôle de qualité nucléaire aux fonctions des systèmes de sûreté ou relatifs à la sûreté.

7.6 Besoins futurs du système de sûreté et de commande du procédé

Il convient que les objectifs et exigences du système d'I&C modernisé soient clairement définis. Il est recommandé que le cahier des charges de l'équipement soit élaboré à partir de ces exigences. Il convient que les besoins futurs soient pris en compte en portant une attention particulière aux contraintes de la conception.

Il convient de spécifier les exigences suivantes:

1) Exigences générales

- exigences de sûreté et opérationnelles révisées,
- exigences de conception de la centrale révisées,
- exigences de conception du système révisées,
- détermination de la révision ou de l'édition des codes et normes avec lesquelles le système d'I&C entier a été conçu. Il est recommandé que toute non-conformité aux codes et normes et les raisons de ces non-conformités soient documentées,
- niveau d'automatisation,
- exigences de fiabilité,
- exigences de maintenabilité,
- classement de sûreté.

2) Exigences fonctionnelles et de performances

- identification complète des fonctions à renouveler ou à mettre à niveau, ainsi que leur affectation à la sûreté ou à d'autres objectifs identifiés dans l'étude de faisabilité,
- identification des affectations fonctionnelles entre les opérateurs et le système d'I&C (CEI 60964 et CEI 61839),
- classement formel de sûreté des fonctions prévues et identification de leur relation par rapport à la sûreté ou autres objectifs, au critère de défaillance unique, à la mise en œuvre de la défense en profondeur et la diversité fonctionnelle,
- identification de l'interaction entre opérateur et système,
- le traitement permettant de déclencher les alarmes,
- logique de commande,
- précision,
- temps de réponse,
- répétitivité,
- définition du niveau d'automatisation du système mis à niveau, et des actions requises de l'opérateur en conditions normales et d'accident.

3) Exigences d'équipement

- identification de caractéristiques déterministes concernant la tolérance aux défaillances et les changements d'état, ainsi que les probabilités de défaillance et de déclenchement ou d'activation intempestive,
- étendue du traitement fonctionnel des signaux,

- identification d'exigences déterministes et la gestion de défaillances de cause commune, ainsi que les valeurs cibles probabilistes de disponibilité et fiabilité de la conception,
 - exigences techniques générales de l'équipement,
 - exigences de qualification pour IEM, aspects environnementaux (y compris conditions d'accident) et résistance aux séismes,
 - assurance qualité logiciel ou des équipements programmables,
 - signaux d'E/S.
- 4) Domaine des fonctions/équipements
- identification de l'utilisation des mesures existantes,
 - identification des besoins d'installation de nouveaux capteurs,
 - nécessité de validation en ligne des signaux d'entrée,
 - identification de signaux de commande pour activer les actionneurs,
 - retrait des équipements anciens qui ne sont plus nécessaires,
 - domaine des fonctions de simulation associées à moderniser.
- 5) Interfaces
- interfaces internes du système,
 - les interfaces avec d'autres systèmes support, tels que systèmes d'alimentation électrique, d'air instrumentation, de protection contre les incendies, de chauffage et de ventilation, qu'il convient de spécifier,
 - interface détaillée et étendue des responsabilités entre le producteur d'électricité et le fournisseur, et entre fournisseurs.
- 6) Exigences d'installation
- limitations de l'alimentation électrique,
 - capacités des armoires électriques et des chemins de câble,
 - limitations relatives à l'installation de capteurs,
 - pénétrations,
 - ventilation,
 - accès pour les travaux d'installation, y compris les travaux de préparation réalisables fonctionnement normal et les travaux qui peuvent seulement être réalisés en arrêts de tranche.
- 7) Divers
- exigences de la revue de conception,
 - V&V, qualification,
 - renseignements relatifs aux documents disponibles et refonte de la documentation,
 - identification de la documentation requise, par exemple: procès-verbaux de qualification et rapports d'analyse,
 - données concernant l'équipement, expérience opérationnelle,
 - contrôle qualité,
 - capacité d'auto-documentation,
 - méthodes de montage en usine et en centrale (visant la réduction de risques de défaillance systématique),
 - sécurisation (contrôle de configuration, méthodes de travail pour modifications de logiciel au cours du projet ou de l'exploitation, protection contre l'accès interne non-autorisé, protection contre une intrusion externe).

7.7 Fiabilité du système d'I&C

Il est recommandé de déterminer les objectifs de fiabilité pour chaque système ou composant constituant le système d'I&C mis à jour. Ces objectifs seront dérivés des exigences globales de performance du système, qui peuvent être imposées par l'évaluation globale du système de sûreté et par le facteur de productivité de la tranche.

Il convient d'envisager d'améliorer la fiabilité par la redondance des systèmes.

Il convient que les composants critiques soient de conception simple et éprouvée, afin de permettre une fiabilité maximale.

Il convient que le contrôle d'accès, ainsi qu'une gestion de changements soient mis en œuvre pour empêcher toute intrusion non-autorisée dans les zones hébergeant les bases de données et les programmes du système d'I&C, afin de garantir l'intégrité et la sécurité des données critiques.

Il convient que le CC soit conçu de façon à offrir une robustesse convenable, une tolérance aux défaillances, un fonctionnement assurant la défaillance non-dangereuse et une dégradation progressive. Il est recommandé de réduire la probabilité d'une perte totale de communication par les bus de données au strict minimum, ainsi que de prévoir des matériels redondants destinés à garantir une exploitation sûre de la centrale en cas de défaillance d'un des bus de données. Il convient que la conception permette au système d'I&C d'être restauré progressivement à la suite d'une éventuelle défaillance d'I&C.

Le vieillissement des composants peut entraîner une augmentation des défaillances de système. Il convient de penser à la maintenance préventive. Voir aussi le TECDOC-1147 de l'AIEA pour des conseils sur la gestion du vieillissement.

7.8 Etude des risques et avantages

Il convient de prendre en compte les facteurs suivants pour les calculs de motivation lors de l'étude des risques et avantages:

- les revenus générés par une production plus élevée, une disponibilité et une durée de vie accrues,
- la réduction des coûts de maintenance: maintenance pendant l'exploitation, allongement des intervalles de maintenance, maintenance orientée fiabilité et fiabilité améliorée,
- la possibilité de raccourcir les arrêts de tranche, ce qui aura comme conséquence d'augmenter la productivité de la centrale,
- la réduction des frais administratifs grâce à un traitement de données amélioré,
- le risque de délais au moment du redémarrage à la suite de l'arrêt pour modernisation,
- le maintien d'une exploitation sûre de la centrale pendant la modernisation du système d'I&C et l'indisponibilité éventuelle du système modernisé,
- tout risque associé au maintien de l'ancien système, par exemple pour cause d'obsolescence ou de vieillissement,
- l'influence de l'équipement vieillissant et la disponibilité de personnel capable d'entretenir l'équipement ancien,
- les risques d'incompétence du personnel vis à vis du nouveau système pour cause de formation insuffisante ou de manque d'expérience opérationnelle.

7.9 Classement de sûreté

Les classements de sûreté se sont développés dans la plupart des pays avec la mise au point de différents paliers de réacteurs. Dans les centrales plus récentes, les classes de sûreté ont été élaborées en intégrant les concepts de défense en profondeur, d'exploitation post-accidentelle et d'autres fonctions relatives à la sûreté.

Les dernières normes (ex: CEI 61226) affinent le classement de sûreté des fonctions et du matériel CC, en tenant compte des contraintes relatives à la qualification de sûreté de l'équipement CC de qualité industrielle (ex: API et systèmes IHM numériques).

Les derniers classements de sûreté montrent que la séparation des systèmes d'I&C effectuant des tâches relatives à la sûreté est souvent incomplète sur d'anciennes centrales, ce qui oblige à classer des fonctions qui n'ont aucun rapport direct avec la sûreté.

Il peut être financièrement avantageux pour la conception des nouveaux systèmes d'I&C d'exploiter les sous-classes les plus fines du classement de sûreté introduites par les dernières normes.

En cas d'application d'un nouveau système de classement dans le cadre d'un projet de modernisation, il convient de définir avec précision les domaines auxquels s'appliquent le nouveau système de classement, ainsi que les prescriptions qui y sont associées. Ceci peut amener à la coexistence de différents ensembles d'exigences pour les nouveaux et les anciens systèmes.

7.10 Exigences relatives à la qualification d'équipement

Il convient de déterminer les exigences relatives à la qualification de l'équipement pour le système et les composants actuels. Il est recommandé que l'étude comprenne les exigences concernant l'équipement et les environnements accidentels (conditions en salle) du système modernisé et de ses composants. Il convient de prendre en compte le coût de l'équipement et de la qualification, les difficultés techniques et le temps nécessaire pour homologuer les composants du système d'I&C modernisé. Les coûts ultérieurs du maintien de la qualification de l'équipement du système modernisé et de ses composants ne doivent pas être négligés.

Par exemple, il est recommandé d'éviter d'étendre jusque dans le bâtiment réacteur les bus de données transportant des signaux qui seraient nécessaires à la suite d'un APRP. Il convient que les signaux passant par ces bus ne soient pas altérés et n'empêchent, à aucun moment pendant un ADR, les autres systèmes de sûreté de fonctionner correctement. Il est recommandé que le matériel situé dans le bâtiment réacteur nécessite aussi peu d'entretien que possible en conditions normales d'exploitation.

Les types suivants de qualification d'équipement sont à considérer:

- APRP,
- vibration,
- CEM,
- vieillissement,
- qualification sismique,
- environnement (températures normales et extrêmes, humidité, rayonnements...).

Il est recommandé de déterminer les exigences de conception anti-sismique. L'équipement mis à niveau devra éventuellement se conformer aux dernières exigences anti-sismiques. Il faut définir le niveau des exigences anti-sismiques, ainsi que la fonction de sûreté de tous les dispositifs de sûreté pendant et après un événement sismique.

Il convient que la conception comprenne des meubles et armoires (pour le stockage de manuels, équipement de protection personnel, outillages spéciaux...) ancrés au sol afin d'éviter que des objets non-fixés ne mettent en danger l'équipement homologué anti-sismique du local.

7.11 Exigences de qualification de logiciels

La modernisation des systèmes d'I&C de sûreté effectuée à l'aide de systèmes d'I&C numériques fait habituellement appel à des fonctions logicielles.

Les systèmes à base logicielle sont plus complexes que les systèmes câblés qu'ils remplacent. Ceci a attiré l'attention sur les problèmes d'erreurs de spécification et de conception que les essais et les inspections n'ont pas entièrement mis à jour, entraînant la possibilité de défaillances systématiques.

Habituellement, les normes et bases de conception des systèmes fil-à-fil à moderniser ne s'attachent pas spécifiquement aux erreurs et à la qualification des logiciels. Néanmoins, en ce qui concerne la plupart des aspects relatifs à la qualification de systèmes à base logicielle, un consensus international s'est fait jour, se traduisant par un ensemble de normes internationales détaillant les exigences essentielles. Voir bibliographie.

- Il est recommandé d'utiliser un système de classement pour les fonctions d'I&C, afin de permettre la prise en compte de différentes catégories de fonctions et des systèmes d'I&C mettant en œuvre ces fonctions.
- Il est recommandé d'effectuer une analyse de défense en profondeur et de diversité (analyse DPD) afin d'identifier toute possibilité de DMC impliquant des logiciels et d'évaluer d'éventuelles parades.
- Il convient de soumettre la conception du logiciel à des exigences appropriées.

Puisqu'on ne peut pas garantir l'absence totale d'erreurs de logiciel, il convient d'insister sur la qualité du processus de conception en plus des exigences concernant les essais.

Les exigences de base sont définies ci-après.

- Il convient que la conception du logiciel soit supportée par la documentation suivante:
 - plan de sûreté logiciel,
 - plan AQ logiciel,
 - plan de vérification et validation du logiciel, y compris une V&V indépendante,
 - plan de gestion de configuration logiciel,
- Il convient que le logiciel soit conçu selon un plan de cycle de vie, avec une documentation et des phases de conception bien définies.

Un des principes de base de l'exécution des fonctions de sécurité est l'exécution cyclique du logiciel, indépendamment des conditions de la centrale. Un tel système, avec une charge constante au niveau du processeur et des bus, peut être vérifié relativement facilement.

D'un point de vue pratique, la réutilisation de logiciels standard est à encourager autant que possible. Il est recommandé que les composants logiciel réutilisables (par ex: noyau OS, bibliothèques et outils) aient subi une procédure d'autorisation générale ou aient été évalués au cours d'une procédure d'autorisation spécifique à la centrale.

Il est également recommandé que les logiciels applicatifs spécifiques à la centrale soient générés automatiquement par des générateurs de code à partir d'un cahier des charges formel. Ceci évite un codage manuel spécifique au projet, simplifie les processus de revue, vérification et validation et minimise l'effort et les risques spécifiques au projet lors de la demande d'autorisation réglementaire.

7.12 Contraintes physiques

Il est recommandé que le choix de l'emplacement du matériel du système modernisé tienne compte des éléments suivants:

- contraintes concernant les bâtiments,
- contraintes concernant les armoires,
- contraintes concernant les systèmes procédé,
- contraintes concernant les pénétrations existantes,

- limites de cheminement du câblage, y compris l'évaluation des besoins en nouvelles technologies, par exemple: chemins de câbles spéciaux pour fibres optiques, câbles de bus, et exigences séparation,
- charges au sol,
- capacités des systèmes auxiliaires, par ex: alimentations électriques, circuits de refroidissement, ventilation, détection et protection anti-incendie,
- limitations en termes de place et d'accès pour installation, exploitation et maintenance.

Suivant la portée des modifications, si un nouveau réseau de communications numériques doit remplacer un système raccordé en fil-à-fil, il sera nécessaire de faire de la place pour des racks et des panneaux E/S. Le remplacement de composants isolés aura peu d'impact sur le câblage existant.

7.13 Disponibilité de l'équipement (livraison et assistance technique)

Il convient de dresser un inventaire des équipements et du matériel pour le futur système d'I&C modernisé. Il est recommandé de faire ressortir les éléments ayant un long délai de livraison, les éléments coûteux et les fournisseurs potentiels.

Il convient d'étudier la disponibilité de pièces de rechange et d'assistance technologique pendant le reste de la vie de la centrale. Le soutien continu du fournisseur dans le futur est toujours un point important, quelle que soit la technologie utilisée. Généralement, en cas de conservation d'un équipement obsolète, l'assurance d'une future disponibilité ininterrompue de pièces de rechange est moins probable qu'en cas d'utilisation d'un équipement neuf.

La protection contre une future obsolescence, même dans le cas de nouvelles technologies, ne peut jamais être complètement garantie, mais il existe certaines stratégies permettant de minimiser la possibilité d'obsolescence, par exemple:

- utiliser un équipement conforme aux normes de l'industrie, provenant de fabricants bénéficiant d'un important parc de systèmes installés,
- utiliser des technologies éprouvées. La plupart des fabricants auront plusieurs installations dans lesquelles leurs systèmes sont en service depuis plusieurs années,
- se conformer aux tendances de l'industrie nucléaire. Voir ce que d'autres producteurs d'électricité ont essayé avec succès.

La mise en œuvre d'architectures ouvertes et de protocoles de communication standards peut réduire les effets de l'obsolescence dans la future vie de la centrale.

7.14 Ergonomie

Il convient d'incorporer une réflexion sur les aspects ergonomiques au processus de conception et au développement des procédures de maintenance et d'exploitation, afin d'améliorer la capacité du personnel à faire fonctionner la centrale de façon sûre en conditions normales, incidentelles et accidentelles.

Un plan d'ergonomie est habituellement exigé pour toute conception d'une nouvelle centrale nucléaire. Le plan identifie les problèmes ergonomiques et les intègre à la conception technique dès le début de la phase de conception. Il est recommandé d'identifier par des méthodes appropriées, par exemple: la CEI 61839, les exigences procédées pour le CC, y compris pour la salle de commande et autres locaux de commande dans la centrale. La bibliographie contient d'autres normes CEI encadrant la conception d'IHM. Le retour d'expérience du personnel d'exploitation et de maintenance a un rôle important dans la conception ergonomique du centre de commande, afin d'assurer une efficacité maximum et un stress minimum pendant le travail intellectuel et physique de l'opérateur. Voici quelques exemples de facteurs ergonomiques à prendre en compte:

- agencement des pupitres principaux de la salle de commande, message d'alarme, étiquetage et fonctions des consoles,

- idem pour les postes de commande supplémentaires, en prenant en compte les différences fonctionnelles,
- IHM et son impact sur les procédures d'exploitation,
- panneaux de zone et leur interface avec la salle de commande,
- acquisition et évaluation des données à l'aide des nouvelles consoles.

Les exigences concernant la SPA et l'ergonomie font partie d'une description plus globale des principes de conception, et peuvent conduire à des exigences concernant l'architecture du système de commande.

Le fabricant de systèmes de commande fournit souvent les interfaces homme machine dans une solution intégrée matériel + logiciel. Il convient de déterminer l'aptitude à gérer des interfaces personnalisées, s'il est nécessaire d'utiliser une IHM existante ou différente.

L'IHM remplit les fonctions distinctes suivantes:

- affichage de l'état du procédé,
- saisie manuelle et affichage de retour d'information,
- annonce d'alarmes,
- archivage de données d'état,
- filtrage des données.

Le système d'entrée manuelle et de retour d'information sert de:

- «fenêtre» permettant à l'opérateur de visualiser l'exploitation de la centrale,
- et interface par le biais de laquelle l'opérateur peut saisir des commandes de changement d'état ou de points de consigne pour le système de commande numérique.

Il est probable que les instruments des consoles et leur agencement seront modifiés de façon significative, nécessitant ainsi une étude ergonomique avant acceptation de la conception définitive. Il convient d'effectuer une analyse fonctionnelle des tâches de l'opérateur. Beaucoup de tâches autrefois effectuées debout derrière un panneau de commande peuvent être effectuées assis à une station de travail opérateur. Il est recommandé que les moyens permettant à l'opérateur en chef et au chef de quart de surveiller l'état de la centrale, ainsi que l'activité courante des opérateurs dans la salle de commande, soient fournis d'une façon qui élimine les interférences entre les tâches de chacun.

Dans le cas d'une modernisation partielle ou par phases, il est recommandé que les nouveaux éléments soient compatibles avec l'agencement et les principes de conception existants.

Dans le cas d'une modernisation complète, le nouvel agencement de la console de la salle de commande peut avoir une apparence très différente. Il convient de réviser les anciens guides de conception de la salle des commandes. Par exemple, il faut revoir les principes de «dark panel» (écran noir) ainsi que les critères de mise en évidence des dispositifs de SPA. Il est recommandé de réviser également les critères de conception des annonces d'alarme (clignotement, type de sirène, fonctions des boutons-poussoirs).

Les exigences anti-sismiques de la salle de commande principale: éclairage, climatisation et purification de l'air, réduction du bruit, contrôle d'accès etc. font partie des domaines susceptibles de nécessiter une mise à niveau afin d'offrir aux opérateurs un environnement adapté en conditions normales ou d'accident.

L'utilisation d'un système de commande numérique augmente la facilité de production d'alarmes. Il convient de développer des critères adaptés de conditionnement des alarmes, afin de limiter le nombre gênant d'alarmes. Une fonction séparée d'archivage des états peut éliminer une grande partie des alarmes gênantes associées à l'exploitation normale de

l'installation: changement d'état de disjoncteur, changement de position de vanne, etc. Dans ces cas, il est recommandé que l'alarme ne soit déclenchée que si le changement d'état attendu ne se produit pas. L'information concernant le changement d'état sera consignée dans l'enregistreur automatique. En ce qui concerne les signaux d'alarme redondants ou triplés, le serveur d'alarme pourrait annoncer le premier signal d'alarme arrivé. Quand le deuxième ou troisième signal d'alarme est détecté, le message d'alarme confirmerait le moment où le signal était arrivé. L'enregistreur automatique fournirait une liste détaillée des alarmes. Il convient de mettre en place une politique de filtrage d'alarme claire afin de supprimer les alarmes les moins importantes, conformément aux exigences de la CEI 62241.

Il est recommandé que les opérateurs expérimentés et les chefs de quart, ainsi que les ingénieurs de maintenance participent tôt au développement des critères relatifs aux affichages écran pour l'IHM du poste de travail et de maintenance. Les opérateurs et les concepteurs ont tendance à avoir une vision très différente des systèmes. Souvent, ce que le concepteur trouve important ne l'est pas du point de vue de l'opérateur. Les concepteurs ont besoin des conseils d'opérateurs expérimentés afin de comprendre leurs préoccupations et de fournir en salle de commande les informations qui correspondent bien à leurs besoins.

7.15 Analyse de défense en profondeur et de diversité (analyse DPD)

Les mises à niveau récentes de l'I&C consistent habituellement à remplacer le vieil équipement analogique par un nouvel équipement numérique pour cause d'obsolescence des composants analogiques. L'équipement numérique exécute des programmes informatiques afin de satisfaire aux exigences fonctionnelles. Les fournisseurs d'équipement numérique ont tenté de convaincre les organismes de réglementation que ces systèmes informatiques modernes n'introduisent pas de défaillances qui n'étaient pas déjà prises en compte dans la conception de leurs prédécesseurs analogiques. Néanmoins, dans le cas de systèmes électroniques programmables, le logiciel est intrinsèquement vulnérable aux erreurs logicielles, ce qui peut conduire à un comportement imprévisible. Une intégrité imparfaite du matériel et une sensibilité excessive aux conditions ambiantes figurent parmi les raisons mises en avant pour expliquer les DMC. Les organismes de réglementation demandent qu'une DMC ayant lieu simultanément dans tous les systèmes/divisions soit prise en compte dans les accidents de dimensionnement de la centrale. Au cas où un équipement numérique est retenu dans un système de protection, il convient de vérifier que la DMC dans les systèmes de protection n'augmente pas la fréquence de fusion du cœur. Ceci s'appelle communément une analyse DPD. Il est recommandé que l'analyse DPD montre que le système d'I&C entier possède une capacité de défense en profondeur suffisante et plusieurs moyens divers d'accomplir des fonctions de sûreté destinées à limiter les conséquences d'accident et les régimes transitoires en cas de défaillance commune du logiciel de protection du système.

Bien que la plupart des organismes de réglementation demandent une analyse DPD démontrant l'aptitude à faire face aux DMC, il existe toujours dans le secteur des variations importantes en ce qui concerne les conditions aux limites initiales, les stratégies de réponse acceptables et les critères d'acceptation de cette analyse. Les paragraphes suivants décrivent certaines des différences principales jusqu'à présent en ce qui concerne les programmes de modernisation numérique:

– Accidents qu'il convient d'associer à la DMC

Certains organismes de réglementation demandent que tous les accidents soient pris en compte. D'autres ont accepté des arguments probabilistes qui éliminent certains accidents de l'analyse en raison d'une faible probabilité de la DMC associée à la faible probabilité de l'accident. Habituellement, faire face à des accidents peu probables avec une DMC demande plus de fonctionnalité dans les systèmes diversifiés accrédités.

– Effet d'une DMC sur la réponse des systèmes d'I&C

Certains organismes de réglementation ont accepté l'argument expliquant que la DMC n'entraîne que des problèmes passifs (dormants) au niveau du système d'I&C. D'autres exigent une étude des DMC conduisant à des défaillances actives susceptibles d'avoir un impact négatif sur les autres systèmes de défense de la centrale. L'examen de ces interactions potentielles, y compris leurs relations dans le temps peut s'avérer très

complexe et exige souvent des modifications de conception afin de garantir un résultat acceptable.

– Systèmes pouvant être accrédités dans l'analyse

Certains organismes de réglementation acceptent d'accréditer tout système élémentaire/équipement diversifié (c'est-à-dire qui n'est pas sensible à la même DMC). D'autres limitent les systèmes pouvant être accrédités à ceux possédant seulement une qualification de sûreté acceptable. Ceci peut soulever la question du niveau de la qualification des systèmes diversifiés accrédités.

– Portée de la diversification pour accréditation

Dans certains cas, les organismes de réglementation ont accepté le fait que la diversité fonctionnelle suffit (par ex: différentes applications tournant sur la même plate-forme produit ou système d'exploitation logiciel). D'autres exigent une diversité à tous les niveaux du système/produit afin de permettre l'accréditation du système dans l'analyse DPD.

– Contraintes temporelles relatives aux activités des opérateurs

En établissant des méthodes permettant de faire face à une DMC en conditions d'accident, les organismes de réglementation ont accepté d'accréditer toute action de l'opérateur pouvant être justifiée selon les principes admis d'ergonomie. D'autres ont limité les temps de réponse de l'opérateur afin qu'ils correspondent aux contraintes des analyses de sûreté actuelles. Limiter le temps dont dispose l'opérateur pour effectuer une action peut conduire à un besoin accru d'automatisation dans les systèmes d'I&C diversifiés accrédités.

Malgré ces différences, il a été prouvé lors de plusieurs projets de modernisation de centrales que le problème de la DMC peut être résolu, et ce de façon économique et réussie. Un facteur de succès important consiste à contacter les organismes de réglementation tôt dans le programme de modernisation dans l'optique de déterminer d'un commun accord la base de calcul pour faire face aux cas de DMC.

7.16 Séparation et protection contre les incendies et les inondations

Lorsqu'un système est important pour la sûreté, il convient que chaque voie matériel soit isolée physiquement et électriquement des autres voies afin d'empêcher tous les événements de mode commun ou les défaillances de cause commune. Un ensemble complet d'exigences est fourni par la CEI 60709.

Afin de séparer les fonctions et de renforcer la robustesse, il est recommandé d'utiliser pour chaque fonction des serveurs distincts pour récupérer les données sur les mêmes bus de données.

Des murs coupe-feu peuvent être nécessaires dans la conception mise à niveau, afin d'empêcher la propagation du feu et de limiter la charge calorifique de chaque zone. L'implantation de la centrale et l'emplacement de l'équipement doit prendre en compte le risque d'inondation.

Un renforcement de la protection anti-incendie et anti-inondation peut se traduire par une très nette amélioration des chiffres EPS relatifs à la FDC.

7.17 Incertitude et calcul des points de consigne

Les points de consigne des systèmes d'I&C sont cruciaux pour une exploitation efficace, fiable et sûre d'une centrale nucléaire. Le résultat du calcul du point de consigne dépend de la méthodologie de calcul et les incertitudes de différentes sortes concernant les composants d'I&C du système. Quand le nouvel équipement d'I&C est installé à la place de l'ancien, il convient de calculer les points de consigne en utilisant les données du nouvel équipement et la méthodologie de calcul la plus récente, qui peut être différente de celle utilisée précédemment. Il convient de comparer ces résultats aux critères actuels de sûreté et d'exploitation afin de confirmer que ce nouveau système est conforme aux limites de sûreté et

d'exploitation en vigueur. Si les marges sont plus importantes, les points de consignes définitifs peuvent être choisis dans les limites en tenant compte des performances d'exploitation et de l'analyse de sûreté. La CEI 61888 fournit les exigences concernant la détermination et la maintenance des points de consigne.

7.18 Analyse du temps de réponse

Le temps de réponse du nouvel équipement utilisé pour la mise à niveau peut être différent de celui de l'ancien équipement. Il faut donc démontrer que le temps de réponse du nouvel équipement est conforme aux critères spécifiés pour l'obtention de l'autorisation réglementaire. Après l'installation, il convient de procéder à des essais afin de démontrer que le temps de réponse réel ne dépasse pas les limites permises.

7.19 Procédures d'essais

Avant la recette formelle, les sous-systèmes du système d'I&C sont intégrés et testés. Ceci peut comprendre des essais à boucle ouverte et fermée, des tests sur le terrain ou des tests de simulation. Les résultats ainsi que les données obtenues pendant la mise en service et le type de la recette (par exemple: RU, RS, recette et test d'exploitation) apportent les preuves que le système est conforme au cahier des charges. Il convient de porter une attention particulière aux interfaces entre le vieux et le neuf.

Il peut être nécessaire d'imposer des exigences supplémentaires pour ces essais, ainsi que des fonctions de surveillance du système pendant l'exploitation de la centrale, par exemple:

- exploitation parallèle,
- périodes d'épreuve à puissance limitée,
- essais spécifiques et mesures des caractéristiques de performance du système (par exemple: charges processeur et bus, comparaison du comportement en cas de défaut réel par rapport au comportement prévu/spécifié),
- suivi des rapports de défaut,
- fréquence des erreurs de conception,
- fréquence des bugs logiciels,
- fréquence des défaillances de matériel et archivage long terme de journaux de défaillances si besoin, afin de prendre confiance en la qualité du processus de conception et en le système lui-même.

Il est recommandé d'établir les principes de ces essais dès le début du projet. Il convient que les essais soient définis de façon détaillée à l'aide de procédures d'essai appropriées, en spécifiant les conditions d'essai, les scénarios, la documentation associée et les critères d'acceptation. Les organismes de sûreté s'intéresseront à l'analyse documentée des procédures d'essai et aux résultats correspondants. Ils peuvent aussi imposer des conditions spécifiques.

Il convient que les procédures existantes relatives aux essais périodiques du système d'I&C, aux essais de temps de réponse, aux procédures de surveillance et d'étalonnage soient révisées pour tenir compte des caractéristiques du nouveau système, comme un plus haut niveau d'auto-surveillance, des fonctions d'auto-test ou une fréquence d'essais réduite grâce à une plus grande fiabilité des composants.

7.20 Gestion de la documentation

Il est recommandé d'utiliser un système de gestion des documents afin d'aider à l'exploitation, à la maintenance ainsi qu'aux projets de modernisation. Un tel système est large et complexe et par conséquent il convient d'y consacrer des moyens spécifiques pour le créer. Si le système de gestion des documents n'est pas déjà disponible, il doit être mis en place tôt dans le projet. Un tel système facilite l'interface fournisseur/client pendant le projet et apporte dès le début un soutien précieux pour l'exploitation et la maintenance.

Il convient que la documentation de la centrale modernisée soit conforme aux différentes exigences relatives aux catégories de personnel: opérateurs; responsables d'exploitation, ingénieurs conception et maintenance, personnel de revue de sûreté, ainsi qu'aux formations de ces différentes catégories.

Un réseau de gestion de centrale comporte habituellement plusieurs serveurs nécessitant des entrées provenant de bases de données de conception. Par exemple, la gestion des ordres de travail nécessite une liste des différents éléments pouvant faire l'objet d'une intervention, leurs emplacements, spécifications, pièces, schémas, etc. On dégagerait des économies de temps d'exploitation et de maintenance importantes si ces informations pouvaient être reliées ensemble dans une base de données créée pendant la phase de conception pour qu'elles puissent être transférées facilement dans un format pratique pour les différents serveurs d'exploitation et de maintenance, sans nécessiter de saisies manuelles extensives. Ceci est valable non seulement pour le contrôle-commande mais également pour l'équipement et les pièces électriques, mécaniques et civiles.

Il convient d'entrer dans le système d'information les documents à références croisées: manuels de conception, analyses de fiabilité et de sûreté et le rapport de sûreté, afin de permettre l'intégration facile des modifications et de leurs impacts. De même, les documents concernant la sûreté et l'autorisation réglementaire, les manuels de formation, d'exploitation, les politiques et principes d'exploitation, etc., peuvent être intégrés.

Bien que la documentation d'exploitation soit disponible sur les postes de travail informatiques, des copies de secours sont nécessaires en prévision de situations où les terminaux, le réseau ou les serveurs de documentation ne seraient pas disponibles. Il est recommandé de fournir des zones de stockage pour la documentation, ainsi que d'autres éléments nécessaires (papeterie, torches, clés, moyens de communication, etc.) dans des armoires sûres.

Le temps disponible limité pour un remplacement d'I&C pendant un arrêt d'exploitation court peut mener à une situation où des modifications de la documentation de conception du nouveau système et de la documentation de la centrale touchée par des modifications de dernière minute ne peuvent pas être complètement intégrées pendant l'arrêt. Par conséquent, la mise à niveau de la documentation à corriger doit être réalisée plus tard, après l'installation et la mise en service du nouveau CC. Il convient de ne pas sous-estimer cet effort.

7.21 Mise à niveau de la documentation technique de la centrale

Les documents et schémas de conception existants peuvent ne pas forcément refléter l'état réel de la centrale physique existante pour cause de modifications effectuées sur le terrain non documentées, ni notées. Une étude du système et une tournée d'inspection peuvent s'avérer nécessaires afin de repérer les écarts entre l'état réel de la centrale et les documents de conception existants.

Il est recommandé d'utiliser les résultats de la tournée d'inspection pour vérifier la documentation de conception existante ou la configuration conceptuelle de la centrale. La configuration conceptuelle vérifiée est ensuite utilisée pour déterminer si la centrale physique est conforme aux exigences actuelles relatives aux systèmes de sûreté et aux systèmes process. Il convient de classer tout écart en tant que manque ou déficience de conception.

Il est recommandé que la documentation mise à jour comprenne les cahiers des charges fonctionnels et autres, les descriptions des systèmes, les schémas d'implantation, les documents détaillés d'installation, les procédures d'essai, les manuels et procédures de maintenance.

Des problèmes se posent lorsque aucune documentation concernant la conception n'est disponible ou si la documentation existante est incomplète ou inexacte. Si tel est le cas, la seule solution consiste à générer une documentation conforme à l'exécution à l'aide de visites de centrale, de la revue des archives de projets passés et de discussions avec le personnel

de la centrale. Il convient que les documents de base soient édités ou révisés selon les cas. Dans certains cas, des «empreintes digitales» de la centrale peuvent être utilisées, par exemple des enregistrements en fonctionnement normal ou pendant des perturbations. Il est important d'identifier les documents et de s'assurer que toutes les personnes concernées par le projet comprennent la documentation existante des systèmes d'I&C, ainsi que son état.

7.22 Formation et qualification du personnel

Il convient de prévoir dans le planning global du projet la formation du personnel de la centrale en matière des fonctions des nouveaux systèmes d'I&C, l'IHM modifiée, et éventuellement aussi les changements de comportement procédé et des fonctions d'I&C.

Il convient prendre en compte plusieurs catégories de personnel de la centrale, dont les principales sont listées ci-dessous.

- Le personnel participant au projet de modernisation CC ont besoin d'une vision générale des fonctions et capacités spécifiques du nouveau système d'I&C, assez tôt dans le projet. Généralement, une connaissance détaillée n'est pas nécessaire.
- Les techniciens d'I&C et le personnel de maintenance ont besoin d'une formation approfondie sur le système, afin de les préparer à la maintenance du nouveau système (par ex: remplacement de composants, réglage des paramètres) et éventuellement aux modifications de matériel (par ex: extensions mineures) ou de logiciel applicatif (modification des verrouillages, conception de nouveaux affichages d'exploitation).
- Le personnel d'exploitation a besoin d'une connaissance rudimentaire des propriétés du système d'I&C, d'une connaissance détaillée des fonctionnalités de l'IHM et des nouvelles fonctions d'I&C mises en œuvre, selon les besoins de l'exploitation de la centrale; cette catégorie de personnel doit également être capable d'une première réaction aux défaillances de l'I&C (par ex: décision d'envoyer des techniciens d'I&C).
- Ingénieurs (conception, sûreté), et éventuellement futurs instructeurs sur simulateur.
- Personnel de maintenance et d'installation participant à l'installation de l'I&C modernisé.

A chaque catégorie de personnel correspond un programme de formation et des stages spécifiques. Il convient que les objectifs de formation, les connaissances nécessaires et l'étendue de la formation soient définis et planifiés suffisamment tôt.

En plus des cours théoriques sur les propriétés des systèmes d'I&C et les fonctions spécifiques de la centrale, il convient que la formation comprenne également des travaux pratiques, c'est-à-dire:

- l'utilisation de maquette de formation pour la maintenance de l'I&C,
- la participation du personnel du producteur d'électricité à la conception de l'I&C, ainsi qu'au montage et aux tests,
- dans la mesure du possible, l'analyse de la capacité des opérateurs à effectuer leur travail dans la salle de commande modernisée, et à observer leurs réponses aux défauts de fonctionnement typiques, afin de prendre confiance en la bonne adaptation de la nouvelle IHM et de mettre à jour d'éventuels défauts de conception. Le programme de formation et l'évaluation des stagiaires peuvent être vérifiés par les autorités de sûreté.

En cas de modification majeure de l'IHM de la salle de commande principale, il est recommandé que la mise en œuvre à la centrale du nouveau système soit précédée par la mise en œuvre dans le simulateur de formation, afin de former le personnel d'exploitation aux caractéristiques du nouveau système dans des conditions de fonctionnement en temps réel.

Il convient que la formation soit achevée avant la mise en œuvre en centrale; il se peut donc que la formation soit une activité de chemin critique.

Il est recommandé de s'assurer de la disponibilité de formateurs compétents. Il convient que les documents de formation fassent partie de la documentation technique de la centrale afin

de garantir sa mise à jour systématique pendant le projet et en exploitation normale. Il convient que certains aspects de l'IHM soient inclus dans la documentation de formation. Dans la mesure du possible, il convient que la capacité des opérateurs à effectuer leur travail dans la nouvelle salle de commande (partiellement ou entièrement renouvelée) soit contrôlée.

7.23 Organisation du projet

Un projet de modernisation d'I&C réussi nécessite une interface entre plusieurs services. Il est donc recommandé de nommer un chef de projet responsable de la coordination des différents métiers. Etant donné que l'installation doit souvent être effectuée pendant des arrêts d'exploitation, une gestion de projet efficace est indispensable. Comme la mise en place d'une organisation importante et efficace peut être difficile, il convient de prendre en considération l'appel à des ressources externes pour des projets exigeants.

Le projet peut nécessiter des interventions de tiers, tels que sociétés d'ingénierie, fournisseurs/fabricants de matériel, constructeurs ou organismes de sûreté. Il convient que l'organisation comprenne une répartition intelligente des responsabilités entre les différents acteurs. En fonction de la taille du projet, il est recommandé de mettre en place une organisation permettant de mener à bien le projet.

7.24 Gestion de configuration

Il convient de respecter une gestion de configuration convenable en ce qui concerne le CC existant/restant et d'en établir une pour les nouvelles parties de l'I&C. Ceci devrait garantir que la centrale est exploitée et entretenue selon les critères d'autorisation. Pour cela, il convient de mettre en place au cours de la phase d'ingénierie initiale un système bien documenté qui comprenne:

- toutes les procédures et mesures d'assurance qualité nécessaires à la mise en place et au maintien d'une documentation cohérente,
- l'identification de tout élément de configuration,
- la documentation de tous les éléments soumis au contrôle de configuration afin de pouvoir vérifier à tout moment que la configuration conforme à l'exécution correspond bien à la conception spécifiée, et de pouvoir choisir sans ambiguïté les composants et logiciels de substitution.

7.25 Interfaces vers les autres systèmes existants

Afin de remplacer correctement l'ancien matériel par du matériel neuf, il convient de revoir les exigences existantes concernant l'interfaçage vers les autres systèmes et de décider de la façon de satisfaire aux exigences d'interfaçage physiques et fonctionnelles. Si possible, il convient de conserver les exigences actuelles, sinon, de mettre en place de nouvelles exigences d'interfaçage. Ceci comprend les conditions physiques, le système de câblage, les types de signaux, les dispositifs actionneurs, le réseau de communication et les systèmes auxiliaires, y compris l'alimentation électrique.

Pour la démonstration de sûreté, il convient de montrer que toutes les interfaces des systèmes de sûreté ou relatifs à la sûreté ont été prises en compte, qu'elles sont compatibles, que leur comportement est entièrement spécifié pour toutes les conditions d'exploitation, et que les critères d'indépendance requis et les scénarios de défaut concernant les interfaces sont respectés. Ce point revêt une importance particulière lors d'une modernisation partielle mettant en relation matériel neuf et ancien, et en cas d'adaptation de produits multi-usage.

7.26 Standardisation

Afin d'améliorer la sûreté et la facilité d'exploitation, de réduire les coûts de formation des opérateurs et autre personnel et de diminuer le nombre de pièces de rechange, il convient de prévoir la standardisation des produits et travaux à chaque fois que cela est possible. La standardisation peut être facilitée par la préparation de recommandations de standardisation ou par l'application à la mise à jour d'outils logiciels courants d'ingénierie et de gestion. Il

convient de rechercher et évaluer d'autres outils et recommandations existants pouvant être appliqués aux travaux de mise à niveau.

Il convient que la mise en œuvre de la standardisation prenne en compte les problèmes de diversification, en gardant à l'esprit qu'elle peut potentiellement introduire des modes de défaillance communs.

8 Réalisation

8.1 Remarques générales

Voici quelques éléments essentiels du développement initial de la stratégie de mise à niveau nécessaire pour la préparation du programme de mise à niveau:

- une stratégie de mise à niveau pour toute la centrale,
- une élaboration de la configuration cible (finale) du système d'I&C à avoir réalisé à la fin des étapes de mise à niveau, dans le sens d'une «vision»,
- une analyse de la séquence d'étapes de mise à niveau à effectuer.

Cet article contient des conseils pour l'élaboration d'un «projet de stratégie de réalisation» (peu détaillé), nécessaire dès les phases initiales pour l'étude de faisabilité par exemple, ainsi que les points plus détaillés nécessaires à la conception de nouveaux systèmes d'I&C élémentaires.

8.2 Architecture cible

Il convient de prendre en compte pour la conception de l'architecture CC globale, l'étendue totale des systèmes d'I&C (ceux qui resteront, ainsi que ceux qui seront modernisés).

Les données d'entrée essentielles sont:

- l'architecture conforme à l'exécution, ainsi que la catégorisation des fonctions de sûreté de l'I&C,
- la décomposition de la centrale actuelle en ensembles fonctionnels soumis à des exigences uniformes, telles qu'un classement de sûreté commun ou des exigences de performance communes,
- la décomposition des systèmes d'I&C selon les différentes priorités de modernisation,
- les contraintes physiques et autres imposées par les bâtiments existants de la centrale.

L'analyse du classement de sûreté de vieilles centrales par rapport aux normes actuelles fait ressortir que:

- la séparation des systèmes d'I&C remplissant des fonctions de sûreté ou relatives à la sûreté est souvent incomplète, et les fonctions initialement sans catégorisation de sûreté vont peut-être devoir être catégorisées,
- les normes modernes permettent dans certains cas plus de sous-classes dans le classement de sûreté, ce qui peut offrir des avantages économiques au nouveau système d'I&C.

Il convient donc d'évaluer avec soin la catégorisation des fonctions afin d'identifier des améliorations potentielles de la sûreté et de bénéficier des avantages d'un classement plus moderne.

Il est recommandé que l'architecture cible corresponde au programme initial en ce qui concerne:

- 1) les exigences de premier niveau révisées pour la centrale, les systèmes procédé, l'implantation, etc.,

- 2) l'IHM envisagée:
 - salle de commande classique ou informatisée,
 - nombre et caractéristiques des postes de commande supplémentaires,
- 3) définition des ensembles fonctionnels, regroupant les fonctions d'I&C ayant des caractéristiques en commun (ex: classement de sûreté identique, exigences de performance identiques, même priorité de modernisation...),
- 4) structure et caractéristiques du nouvel équipement I&C à installer:
 - emplacement de l'équipement existant, et emplacement prévu pour le nouvel équipement: armoires, terminaux, câblage, etc.,
 - structure et caractéristiques des systèmes de communication,
 - segmentation des fonctions de surveillance à l'intérieur d'une division, par exemple, l'instrumentation des principaux paramètres procédé comme la puissance, la surveillance neutronique et de la pression doit être mise en œuvre par le biais d'équipements distincts,
- 5) exigences pour la séparation spatiale et contraintes d'implantation,
- 6) caractéristiques des interfaces des systèmes conservés.

Il convient aussi de noter que la structure cible peut être un mélange de différentes technologies et générations d'I&C, malgré l'objectif de réalisation d'un nouveau système aussi homogène que possible. Ceci est notamment valable dans les circonstances suivantes:

- des activités de mise à niveau ou d'amélioration ont déjà été effectuées avec des modifications locales et spécifiques et on estime plus économique de conserver ces systèmes, ou
- le CC existant est composé de sous-systèmes possédant des caractéristiques de durée de vie très différentes, l'obsolescence étant un facteur de motivation important pour certaines pièces tandis que d'autres systèmes se conservent grâce à un bon service soutien long terme du fournisseur, un taux de défaillance bas et une longue durée de vie.

8.3 Ordre des étapes de mise à niveau

8.3.1 Généralités

Le deuxième élément de la stratégie de réalisation est la mise au point d'une chronologie optimale des étapes de modernisation, appelés «lots de travaux».

Trois possibilités existent:

- mise à niveau en une seule étape, pendant un arrêt unique de longue durée,
- mise à niveau au cours d'un nombre limité de grandes étapes, étalées sur plusieurs années, à effectuer pendant les arrêts normaux (ou légèrement prolongés),
- une série de modifications spécifiques, chacune ayant un domaine très restreint.

Il convient de déterminer la solution optimale concernant la taille et l'ordre des lots de travaux en s'appuyant sur les considérations suivantes, à évaluer par le producteur d'électricité et le fournisseur potentiel.

Il convient de noter que les exigences réglementaires comprennent une étude des conditions d'exploitation pendant les travaux de modernisation (remplacement avec la tranche en puissance, remplacement de l'équipement de sûreté pendant que le cœur n'est pas déchargé, installation de systèmes de surveillance temporaires...). Chaque configuration temporaire ou intermédiaire doit pouvoir être autorisée. De plus, la radioprotection des travailleurs pendant les travaux dans les zones dangereuses constitue une responsabilité relative à la sûreté et nécessite une démonstration de sûreté.

8.3.2 Choix du nombre de lots de travaux

En général, d'un point de vue technique et théorique, le remplacement de l'I&C en une seule étape pendant un arrêt prolongé peut être la solution la plus efficace, puisqu'elle minimise la création d'interfaces temporaires, la mobilisation répétée d'équipes d'installation et de mise en service, et la formation répétée du personnel d'exploitation et de maintenance en ce qui concerne l'équipement modifié et l'IHM. Cette solution est aussi très pratique si des améliorations de plus grande envergure des systèmes procédé ou des bâtiments sont déjà prévues et nécessitent un arrêt prolongé. Dans ce cas, une modernisation de l'I&C en une seule étape pourrait être intégrée à ce programme.

Néanmoins, il convient de contrebalancer ces arguments avec d'autres considérations économiques et organisationnelles, ce qui peut finalement mener à une série de plusieurs lots de travaux CC plus courts.

- Il convient de comparer les pertes de production provoquées par un arrêt prolongé aux bénéfices d'une solution en une étape.
- Des restrictions budgétaires annuelles pour les modifications CC conduiront éventuellement à un étalement du programme de mise à niveau sur plusieurs années.
- Il est recommandé que la taille des lots soit acceptable d'un point de vue organisationnel:
 - il convient que le producteur dispose des moyens nécessaires pour la revue de la documentation de conception concernant un lot de travail, les activités de V&V et la coordination avec d'autres activités relatives à la centrale;
 - il convient que la taille de chaque lot soit compatible avec la capacité du fournisseur à concevoir, fabriquer, installer et mettre en service le nouvel équipement dans les délais prévus;
 - la décomposition du total en plusieurs lots de travaux peut donner la possibilité d'acquérir de l'expérience en commençant par les parties moins importantes de la centrale, avant de moderniser les systèmes du cœur;
 - les demandes émanant des organismes réglementaires, ou les problèmes existants dans un système élémentaire peuvent imposer la modernisation de systèmes isolés à court terme, sans offrir le temps nécessaire à la préparation d'une modernisation en une seule étape.

8.3.3 Définition des lots de travaux

Si il existe des systèmes de taille réduite, possédant des interfaces simples et claires vers d'autres systèmes d'I&C (ex: ordinateurs d'acquisition de données, systèmes de surveillance spéciaux, etc.), il convient de définir ceux-ci en tant que sous lots indépendants.

L'utilisation optimale du temps d'arrêt disponible passe habituellement par l'installation du nouvel équipement CC avant la suppression de l'équipement obsolète dans la centrale. Cette solution peut être limitée par des problèmes de place disponible. On peut envisager plusieurs solutions:

- il peut être avantageux de réaliser d'abord un petit lot de travaux centrés sur la suppression des équipements obsolètes encombrants afin de gagner de la place pour les lots suivants;
- il peut être avantageux d'installer un nouvel équipement à un emplacement temporaire dans un premier temps, et de le transporter à son emplacement final plus tard;
- il peut être avantageux d'installer le nouvel équipement à un endroit différent de l'ancien, ou bien dans des bâtiments neufs/supplémentaires ou dans des enceintes ou emplacements qui n'étaient pas initialement prévus pour des installations d'I&C;
- une solution spécifique serait de déplacer les fonctions des postes de commande locaux vers des postes de travail informatisés dans la salle de commande principale, afin de gagner de la place pour l'installation du prochain lot de travaux.

L'espace disponible pour ces différentes approches peut être décisif dans la définition des lots de travaux correspondants.

L'interfaçage de l'équipement existant avec l'équipement nouvellement installé peut donner lieu à des interfaces compliquées ou à la réalisation d'équipements dédiés, et peut aussi nécessiter une nouvelle qualification de l'équipement existant en raison des modifications. Dans un tel contexte, il peut être avantageux d'augmenter l'étendue de la modernisation afin d'y inclure des équipements non-obsolètes, dans le but d'éviter une nouvelle démarche de qualification, des interfaces peu pratiques et la fourniture de matériel non-standard.

En cas d'installation d'un système de commande procédé informatisé, il convient de s'assurer de l'homogénéité de l'IHM. Il convient de garder l'IHM aussi homogène que possible pour les différentes opérations d'une tâche opérateur donnée, c'est-à-dire soit à base de pupitres classiques, soit à base d'écrans. Il faut éviter les solutions mixtes, où une seule tâche opérateur doit être effectuée en partie à l'écran, en partie par commandes et indicateurs classiques. Quand ce n'est pas possible parce que les limites des différents systèmes d'I&C ne correspondent pas aux limites des tâches opérateur, il peut être nécessaire d'envisager la réalisation d'interfaces temporaires entre le nouveau CC et les panneaux classiques, ou entre l'ancien CC et l'IHM à base d'écrans, afin de maintenir la cohérence de l'interface opérateur pour une tâche donnée.

8.3.4 Exploitation parallèle et remplacement de l'équipement en puissance

Il convient d'envisager l'exploitation en parallèle de l'ancien et du nouvel équipement. Une solution d'exploitation en parallèle en boucle ouverte ou en boucle fermée pourrait convenir. Il y a plusieurs motivations possibles:

- une exploitation parallèle permet de vérifier le bon fonctionnement et le comportement correct du nouveau système d'I&C. Dans le cas d'une exploitation en boucle ouverte, on peut contrôler les réactions correctes aux incidents de la tranche, sans risque d'activation intempestive,
- une exploitation parallèle sépare l'installation et la mise en service du nouveau système de la suppression de l'ancien, permettant ainsi à cette dernière tâche de s'effectuer sur une période plus longue, et garder les temps d'arrêts courts. La disponibilité d'un espace suffisant constitue une condition préalable à l'installation du nouveau système.

Le remplacement en puissance est un cas spécifique où l'exploitation parallèle est utilisée afin de vérifier le bon fonctionnement de l'équipement. C'est une option intéressante dans le cas de modernisations mineures et avec certaines conditions limites spécifiques. Cette solution est à envisager au cas où:

- l'emplacement de l'équipement à remplacer est accessible pendant l'exploitation en puissance,
- le domaine de l'équipement à remplacer est très limité (ex: une baie ou un tiroir unique),
- l'interface entre le nouvel équipement et l'ancien ne nécessite pas la modification de l'ancien équipement,
- le nouvel équipement n'est pas nécessaire pendant l'exploitation en puissance, ou un équipement redondant est utilisé afin de permettre le remplacement d'une des voies redondantes, après une autre, sans perte (il peut être nécessaire de réduire temporairement le schéma de logique de coïncidence).

Une telle approche peut être intéressante, par exemple dans le cas du remplacement des systèmes de contrôle du flux neutronique et du cœur. Dans ce cas, les voies du nouveau système peuvent être alignées immédiatement par rapport aux anciennes voies, sans incertitude concernant le niveau de flux «correct».

Il convient d'étudier les risques et inconvénients de cette approche au cas par cas:

- le risque élevé d'un impact sur l'exploitation de la centrale (déclenchement par activation intempestive pendant la période de réduction du schéma logique de coïncidence) lors de la manipulation des interfaces,
- la réduction de la charge de travail du personnel d'I&C pendant les arrêts,
- l'éventuel raccourcissement des temps d'arrêt,
- la comparaison des équipements ancien et nouveau pendant l'exploitation parallèle.

8.3.5 Ordre des lots de travaux

Le Paragraphe 8.1 recommande la mise en place de priorités concernant la modernisation des systèmes d'I&C. Pendant la mise au point de la stratégie de réalisation, il est nécessaire de réfléchir plus en détail à l'ordre des lots de travaux. Les critères les plus importants sont énumérés ci-dessous.

Il convient que les systèmes proches de la défaillance, ainsi que ceux devenant de moins en moins disponibles pour cause de manque de pièces de rechange ou de prise en charge ou ceux ayant un taux de défaillance important, soient modernisés en premier, ainsi que les systèmes permettant de satisfaire directement aux prescriptions des autorités de sûreté.

Il est recommandé que les modifications ayant un impact important sur l'IHM (ex: migration d'une conduite d'exploitation conventionnelles à une conduite informatisée) soient précédées d'un laps de temps suffisant pour permettre la formation des opérateurs et la recette, ainsi que la validation du nouveau concept dans le simulateur. Si il n'y a pas suffisamment de temps pour permettre aux opérateurs de s'adapter, il vaut mieux moderniser d'abord les systèmes ne nécessitant pas de modification majeure de l'IHM. Dans la mesure du possible, introduire dès le début la plate-forme IHM à utiliser tout au long de la modernisation de l'I&C. Par ailleurs, tout système non représenté dans le simulateur de formation peut être modernisé au début du projet, puisque le temps de préparation nécessaire à l'installation dans la centrale est réduit au minimum.

Il peut être avantageux de commencer par les systèmes auxiliaires afin que le producteur d'électricité et le fournisseur puissent acquérir de l'expérience d'un premier projet pilote n'ayant pas d'impact critique sur l'ensemble du procédé de la centrale. Une telle démarche peut également être employée afin d'obtenir l'acceptation par le personnel d'exploitation dans une partie non critique de la centrale, et d'établir une bonne base de retour d'expérience et d'adhésion lors du choix d'une IHM classique ou à base d'écrans.

9 Recommandations

Le rapport recommande une approche systématique comprenant les étapes suivantes:

- prise en compte de la stratégie globale du producteur d'électricité pendant la mise au point de la stratégie de modernisation de l'I&C,
- évaluation préliminaire proposant un bilan des raisons de la modernisation, rappelant les risques, coûts et bénéfices,
- préparation d'études de faisabilité détaillées, avec coûts budgétaires et une étude de sûreté préliminaire,
- préparation du cahier des charges et appel d'offres débouchant sur la commande.

Des conseils concernant les activités ultérieures du projet sont décrits en détail dans d'autres documents référencés dans la bibliographie.

Les mises à niveau majeures d'une centrale nucléaire soulèvent des problèmes du même ordre que la construction d'une nouvelle centrale. Il est donc important de:

- mettre en place des moyens compétents côté client,

- choisir des fournisseurs compétents, possédant un savoir-faire éprouvé en ingénierie des centrales nucléaires et en mise en service de leur équipement.

Ensuite, le plus important est de travailler de façon systématique, comme il est indiqué dans le présent rapport. L'expérience fait ressortir les points importants suivants:

- impliquer les autorités réglementaires aussi tôt que possible,
- mettre au point un domaine d'application qui optimise les profits du cycle de vie de la tranche; définir les tailles et l'ordre des différents lots avec soin, en prenant en compte les prérequis de la centrale, ainsi que la compétence et la main d'œuvre de l'organisation chargée du projet,
- obtenir les mises à jour de la documentation de la centrale, y compris des informations détaillées sur le contexte technique de la conception,
- s'occuper de l'IHM pour la technologie électronique programmable dès le début du projet,
- étudier les preuves apportées par les fournisseurs pour justifier de la qualité des logiciels avant de commander; choisir des produits dont on est confiant qu'ils conviendront à l'autorisation ultérieure.

Bibliographie

Commission Electrotechnique Internationale (CEI)

CEI 60671:2007, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60780:1998, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60960:1988, *Critères fonctionnels de conception pour un système de visualisation des paramètres de sûreté pour les centrales nucléaires*

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 60980:1989, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

CEI/TR 61000-1-5:2004, *Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems* (disponible seulement en anglais)

CEI 61225:2005, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences pour les alimentations électriques*

CEI 61226:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande¹*

CEI 61227:2008, *Centrales nucléaires de puissance – Salles de commande – Commandes opérateurs*

CEI 61497:1998, *Centrales nucléaires – Verrouillages électriques relatifs aux fonctions importantes pour la sûreté – Recommandations pour la conception et la mise en œuvre*

CEI 61500:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle commande importants pour la sûreté – Communication de données¹*

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2:2000, *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

¹ A publier.

CEI 61771:1995, *Centrales nucléaires de puissance – Salle de commande principale – Vérification et validation de la conception*

CEI 61772:2009, *Centrales nucléaires de puissance – Salles de commande – Utilisation des unités de visualisation²*

CEI/TR 61838:2001, *Centrales nucléaires – Fonctions d'instrumentation et de contrôle-commande importants pour la sûreté – Utilisation des évaluations probabilistes de sûreté pour le classement*

CEI 62138:2004, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

CEI 62340:2007, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences permettant de faire face aux défaillances de cause commune (DCC)*

Agence Internationale de l'Energie Atomique (AIEA)

Rapports préparés dans le cadre du groupe de travail international de l'AIEA sur le contrôle commande des centrales nucléaires

AIEA-TECDOC-668:octobre 1992, *The role of automation and humans in nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-808:juillet 1995, *Computerisation of operation and maintenance for nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-812:juillet 1995, *Control room systems design for nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-912:octobre 1996, *Computerised support systems in nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-952, *Advanced control systems to improve nuclear power plant reliability and efficiency* (disponible seulement en anglais)

AIEA-TECDOC-995:1998, *Selection, specification, design and use of various nuclear training simulators* (disponible seulement en anglais)

AIEA-TECDOC-1016:mai 1998, *Modernization of instrumentation and control in nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-1140:mars 2000, *Effective handling of software anomalies in computer based systems at nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-1327:2002, *Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants* (disponible seulement en anglais)

AIEA-TECDOC-1328:2002, *Solutions for cost effective assessment of software based instrumentation and control systems in nuclear power plants* (disponible seulement en anglais)

² A publier.

AIEA-TECDOC-1402:2004, *Management of life cycle and ageing at nuclear power plants: improved I&C maintenance* (disponible seulement en anglais)

AIEA-TRS-384:1999, *Verification and validation of software related to nuclear power plant instrumentation and control* (disponible seulement en anglais)

AIEA-TRS-387:1999, *Modern instrumentation and control for nuclear power plants: a guidebook* (disponible seulement en anglais)

AIEA-50-SG-D11:1986 *Principes généraux de sûreté dans la conception des centrales nucléaires ; Guide de sûreté*

Rapports préparés dans le cadre du groupe de travail international de l'AIEA sur la sûreté nucléaire

SRS:1998 (No 6), *Safety issues for advanced protection, control and human-machine interface systems in operating nuclear power plants* (disponible seulement en anglais)

NS-R-1: septembre 2000, *Safety of nuclear plants: design* (disponible seulement en anglais)

NS-G-1.1:septembre 2000, *Software for computer based systems important to safety in nuclear power plants* (disponible seulement en anglais)

NS-G-1.3:mars 2002, *Instrumentation and control systems important to safety in nuclear power plants* (disponible seulement en anglais)

NS-G-2.3:octobre 2001, *Modifications to nuclear power plants* (disponible seulement en anglais)

NS-R-2:2000, *Safety of nuclear power plants: operation* (disponible seulement en anglais)

GS-G-1.4:août 2002, *Documentation for use in regulating nuclear facilities* (disponible seulement en anglais)

GS-G-4.1:mai 2004, *Format and content of the safety analysis report for nuclear power plants* (disponible seulement en anglais)

INSAG-12:1999, *Basic safety principles for nuclear power plants 75-INSAG-3 Rev.1* (disponible seulement en anglais)

INSAG-14:1999, *Safe management of the operating lifetimes of nuclear power plants* (disponible seulement en anglais)

UK Health and Safety Executive: novembre 1997, AECB Canada, DSIN/ISPN France, NII UK, USNRC USA, *Four party regulatory consensus report on the safety case for computer based systems in nuclear power plants* (disponible seulement en anglais)

Rapport de la Commission Européenne EUR 19265: mai 2000, *Common position of European nuclear regulators for the licensing of safety critical software for nuclear power reactors.* (disponible seulement en anglais)

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