

**RAPPORT
TECHNIQUE
TECHNICAL
REPORT**

**CEI
IEC**

TR 62096

Première édition
First edition
2002-09

**Centrales nucléaires –
Système de contrôle commande
et d'instrumentation –
Guide pour décider d'une modernisation**

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



Numéro de référence
Reference number
CEI/IEC/TR 62096:2002

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- Site web de la CEI (www.iec.ch)
- Catalogue des publications de la CEI

Le catalogue en ligne sur le site web de la CEI (http://www.iec.ch/searchpub/cur_fut.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- IEC Just Published

Ce résumé des dernières publications parues (http://www.iec.ch/online_news/justpub/jp_entry.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- Service clients

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- IEC Web Site (www.iec.ch)
- Catalogue of IEC publications

The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- IEC Just Published

This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- Customer Service Centre

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

**RAPPORT
TECHNIQUE
TECHNICAL
REPORT**

**CEI
IEC
TR 62096**

Première édition
First edition
2002-09

**Centrales nucléaires –
Système de contrôle commande
et d'instrumentation –
Guide pour décider d'une modernisation**

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

© IEC 2002 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

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 the publisher.

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

X

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

AVANT-PROPOS	6
INTRODUCTION	8
1 Domaine d'application et objet	10
2 Documents référencés dans le rapport technique.....	12
3 Termes et définitions	14
4 Abréviations.....	18
5 Motivation de la modernisation	18
5.1 Généralités	18
5.2 Facteurs de motivation d'ordre économique.....	18
5.3 Facteurs de motivation relatifs à la sûreté.....	22
5.4 Synthèse des motivations d'une modernisation.....	22
6 Présentation générale de la décision de modernisation.....	24
6.1 Cycle de vie du CC	24
6.2 Stratégie du CC long terme	28
6.3 Etudes de faisabilité	32
6.4 Spécifications pour l'appel d'offre et achat de systèmes élémentaires	48
7 Eléments de réflexion concernant la modernisation.....	52
7.1 Codes et normes réglementaires	52
7.2 Politique générale de l'entreprise et codes d'ingénierie.....	52
7.3 Besoins futurs du système de sûreté et de commande du procédé	52
7.4 Fiabilité du système de CC	56
7.5 Considérations économiques.....	58
7.6 Etude des risques et avantages	58
7.7 Classement de sûreté.....	60
7.8 Exigences relatives à la qualification d'équipement.....	60
7.9 Exigences de qualification de logiciels	62
7.10 Contraintes physiques	64
7.11 Aspects technologiques	64
7.12 Disponibilité de l'équipement (livraison et assistance technique)	68
7.13 Ergonomie	68
7.14 Analyse DPD	72
7.15 Séparation et protection contre les incendies et les inondations	74
7.16 Incertitude et calcul des points de consigne.....	74
7.17 Analyse du temps de réponse.....	76
7.18 Essais	76
7.19 Gestion de la documentation	76
7.20 Mise à niveau de la documentation technique de la centrale.....	78
7.21 Formation et qualification du personnel	80
7.22 Organisation du projet	82
7.23 Gestion de configuration.....	82
7.24 Interfaces vers les autres systèmes existants	82
7.25 Standardisation	82

CONTENTS

FOREWORD	7
INTRODUCTION	9
1 Scope and object	11
2 Reference documents	13
3 Terms and definitions	15
4 Abbreviations	19
5 Motivation for modernization	19
5.1 General	19
5.2 Economic motivating factors	19
5.3 Safety motivating factors	23
5.4 Summary of motivations for modernization	23
6 Modernization decision overview	25
6.1 I&C life cycle	25
6.2 Long-term I&C strategy	29
6.3 Feasibility studies	33
6.4 Tender specification and purchasing of the individual systems	49
7 Considerations for modernization	53
7.1 Regulatory codes and standards	53
7.2 Company policy and engineering standards	53
7.3 Safety and process control system future needs	53
7.4 I&C system reliability	57
7.5 Economic considerations	59
7.6 Risks and benefit study	59
7.7 Safety classification	61
7.8 Equipment qualification requirements	61
7.9 Software qualification requirements	63
7.10 Physical constraints	65
7.11 Technology considerations	65
7.12 Equipment availability (delivery and support)	69
7.13 Human factors	69
7.14 3D analysis	73
7.15 Separation and protection against fire and flooding	75
7.16 Uncertainty and set-point calculation	75
7.17 Response time analysis	77
7.18 Test procedures	77
7.19 Documentation management	77
7.20 Update of plant technical documentation	79
7.21 Training and staff qualification	81
7.22 Project organization	83
7.23 Configuration management	83
7.24 Interfaces to the other existing systems	83
7.25 Standardization	83

8	Réalisation.....	84
8.1	Introduction	84
8.2	Architecture cible.....	84
8.3	Ordre des étapes de mise à niveau.....	86
9	Recommandations	92
	Annexe A Bibliographie internationale.....	96
	Figure 1 – Structure de la CEI 62096	12
	Tableau 1 – Phases du cycle de vie du CC	26

IECNORM.COM: Click to view the full PDF of IEC TR 62096:2002

8	Implementation	85
8.1	Introduction	85
8.2	Target architecture	85
8.3	Sequence of upgrading steps.....	87
9	Recommendations	93
Annex A	Bibliography – International publications	97
Figure 1	– IEC 62096 Structure	13
Table 1	– I&C Life cycle phases	27

IECNORM.COM: Click to view the full PDF of IEC TR 62096:2002

Withd 2012

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES – SYSTÈME DE CONTRÔLE COMMANDE ET D'INSTRUMENTATION – GUIDE POUR DÉCIDER D'UNE MODERNISATION

AVANT-PROPOS

- 1) La CEI (Commission Électrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments du présent rapport technique 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 des réacteurs, du comité d'études 45 de la CEI: Instrumentation nucléaire.

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

Projet d'enquête	Rapport de vote
45A/429/CDV	45A/442/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 2005. A cette date, la publication sera

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
INSTRUMENTATION AND CONTROL –
GUIDANCE FOR THE DECISION ON MODERNIZATION**

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this technical report may be the subject of patent rights. The 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: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

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

Enquiry draft	Report on voting
45A/429/CDV	45A/442/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 2005. At this date, the publication will be

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

INTRODUCTION

Les procédures classiques d'analyse de sûreté d'une centrale, de son exploitation et de sa maintenance renseigneront 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 de CC 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 de CC moderne peuvent être évalués au cours de la modernisation.

IECNORM.COM: Click to view the full PDF of IEC TR 62096:2002

INTRODUCTION

Normal procedures for evaluation of plant safety, operations and maintenance will provide information about potential needs for renewal or upgrades. After many years of operation the 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 ageing of the equipment. During modernization, the benefits offered by modern I&C equipment can be evaluated.

IECNORM.COM: Click to view the full PDF of IEC TR 62096:2002

Withd 2020

CENTRALES NUCLÉAIRES – SYSTÈME DE CONTRÔLE COMMANDE ET D'INSTRUMENTATION – GUIDE POUR DÉCIDER D'UNE MODERNISATION

1 Domaine d'application et objet

Le but de ce rapport technique est d'aider les propriétaires de centrales nucléaires lors du processus décisionnel et pendant la préparation de la modernisation partielle ou totale du CC. Pour cela, il propose:

- un rappel des facteurs motivant une modernisation du CC,
- les principales options pour l'élaboration de différents scénarios de modernisation du CC,
- les critères économiques et techniques pour le choix d'une stratégie de CC 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 de CC,
- le contenu du cahier des charges 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 seront utilisés comme documents de haut niveau pour cela, alors que les publications de la CEI serviront 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 de CC 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.

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

1 Scope and object

The purpose of this technical report is 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 will be 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.

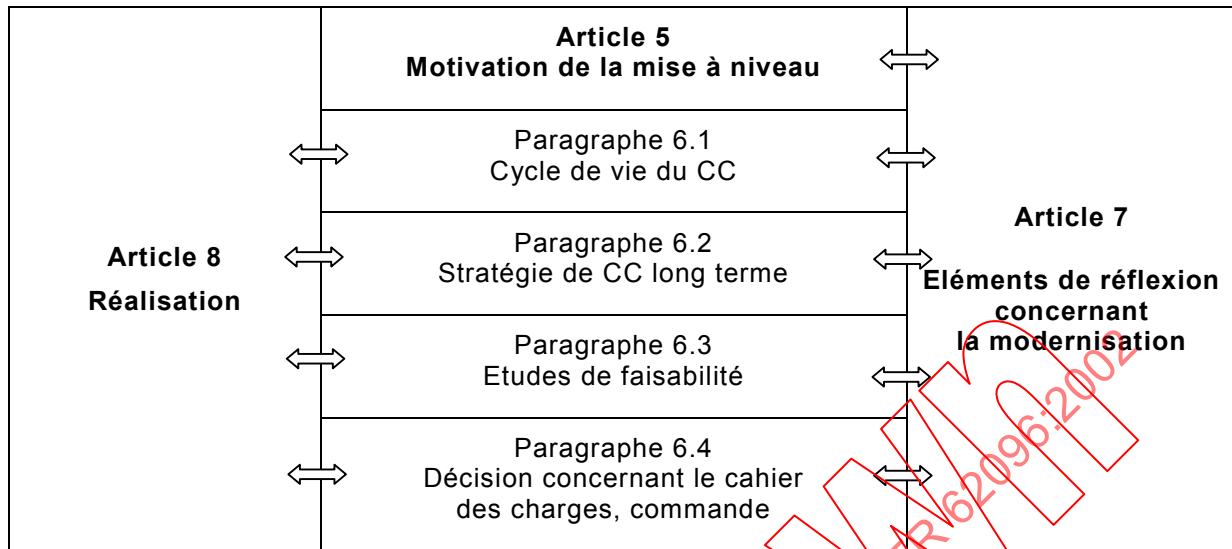


Figure 1 – Structure de la CEI 62096

IEC 2376/02

2 Documents de référence

CEI 60050(191):1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-3:1996, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 3: Evaluation du coût du cycle de vie*

CEI 60780:1998, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60880:1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*

CEI 60880-2:2000, *Logiciel pour les calculateurs de sûreté des centrales nucléaires – Partie 2: Défense contre les défaillances de cause commune provoquées par le logiciel, utilisation d'outils logiciels et de logiciels prédéveloppés*

CEI 60964:1989, *Conception des salles de commande des centrales nucléaires de puissance*

CEI 60980:1989, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 60987:1989, *Calculateurs programmés importants pour la sûreté des centrales nucléaires*

CEI 61000, *Compatibilité électromagnétique (CEM)*

CEI 61226:1993, *Centrales nucléaires – Systèmes d'instrumentation et contrôle commande importants pour la sûreté – Classification*

CEI 61513:2001, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

CEI 61772:1995, *Centrales nucléaires de puissance – Salle de commande principale – Application des unités de visualisation*

CEI 61839:2000, *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions*

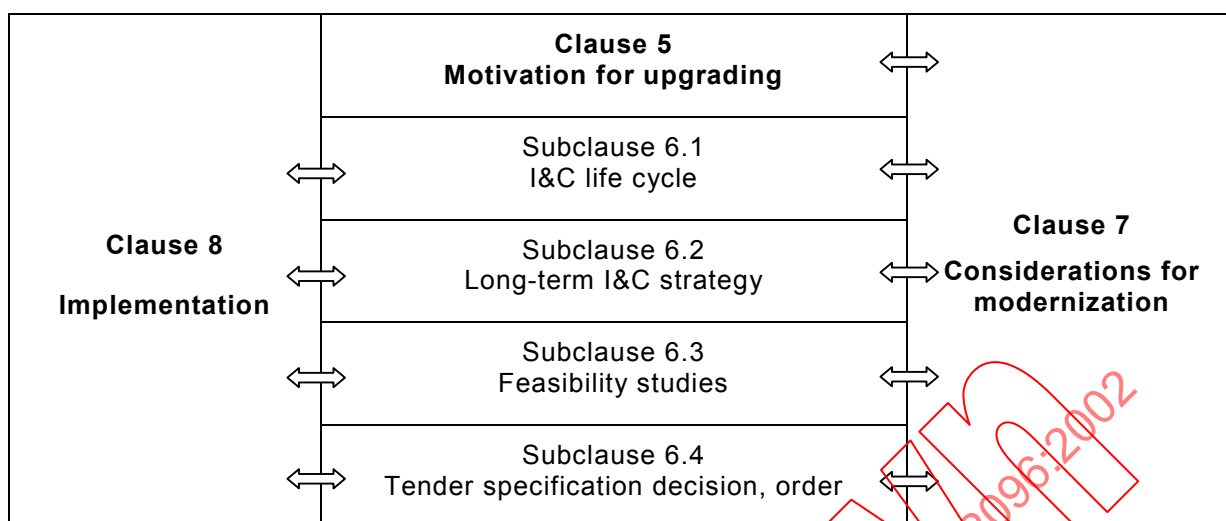


Figure 1 – IEC 62096 structure

IEC 2376/02

2 Reference documents

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

IEC 60300-3-3:1996, *Dependability management – Part 3: Application guide – Section 3: Life cycle costing*

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

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*

IEC 60880-2:2000, *Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software*

IEC 60964:1989, *Design for control rooms of nuclear power plants*

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

IEC 60987:1989, *Programmed digital computers important to safety for nuclear power stations*

IEC 61000, *Electromagnetic compatibility (EMC)*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

IEC 61513:2001, *Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems*

IEC 61772:1995, *Nuclear power plants – Main control-room – Application of visual display units (VDU)*

IEC 61839:2000, *Nuclear power plants – Design of control rooms – Functional analysis and assignment*

AIEA-50-SG-D11, 1988, *Principes généraux de sûreté dans la conception des centrales nucléaires*

AIEA-TECDOC-1016:1998, *Modernization of instrumentation and control in nuclear power plants*

AIEA-TECDOC-1066:1999, *Specification of requirements for upgrades using digital instrument and control systems*

AIEA-TECDOC-1147:2000, *Management of ageing of I&C equipment in NPP*

3 Termes et définitions

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

3.1

disponibilité

aptitude d'une entité 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]

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 la configuration

discipline appliquant des mesures techniques et administratives pour identifier et documenter les caractéristiques fonctionnelles et physiques d'un élément de configuration, contrôler les modifications apportées à ces caractéristiques, enregistrer et signaler le processus des modifications et le statut de réalisation et vérifier la conformité aux exigences spécifiées

[CEI 61513, définition 3.12]

3.3

système de CC

ensemble des matériels de commande automatique et manuelle, composé des systèmes d'instrumentation, de commandes et d'information

[CEI 60964]

3.4

IHM

interface entre l'équipe de conduite d'une part, les systèmes de contrôle-commande 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 61839, définition 3.3]

3.5

cycle de vie

intervalle de temps entre la conception d'un produit et sa mise au rebut

[CEI 60300-3-3, définition 3.1, modifiée]

3.6

coût du cycle de vie

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

[CEI 60300-3-3, définition 3.2]

IAEA - 50-SG-D11, 1988, *General design safety principles for nuclear power plants*

IAEA-TECDOC-1016:1998, *Modernization of instrumentation and control in nuclear power plants*

IAEA-TECDOC-1066:1999, *Specification of requirements for upgrades using digital instrument and control systems*

IAEA-TECDOC-1147:2000, *Management of ageing of I&C equipment in NPP*

3 Terms and definitions

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

3.1 availability

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

discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

[IEC 61513, definition 3.12]

3.3 I&C system

instrumentation and control system. A hardware implementation of automatic and manual controls, which consists of instrumentation, control and information systems

[IEC 60964]

3.4 HMI Human Machine Interface

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 61839, definition 3.3]

3.5 life cycle

time interval between a product's conception and its disposal

[IEC 60300-3-3, definition 3.1]

3.6 life cycle cost

cumulative cost of product over its life cycle

[IEC 60300-3-3, definition 3.2]

3.7

maintenabilité

pour une entité donnée, utilisée dans des conditions données d'utilisation, probabilité pour qu'une opération donnée de maintenance active puisse être effectuée pendant un intervalle de temps donné, lorsque la maintenance est assurée dans des conditions données avec l'utilisation de procédures et de moyens prescrits

[VEI 191-13-01]

NOTE Le terme «maintenabilité» est aussi employé pour désigner l'aptitude caractérisée par cette probabilité (voir 191-02-07).

3.8

modernisation

remplacement ou mise à niveau par des systèmes et composants plus récents

Remplacement est le terme à utiliser quand il n'y a pas de modification des exigences.

NOTE 1 Les termes améliorer, remettre en état, à niveau, rattraper, rénover sont similaires et souvent interchangeables. Seules les nuances diffèrent (AIEA-TECDOC-1066).

Mise à niveau est le terme à utiliser quand les exigences sont plus sévères. La mise à niveau comprend également la mise en œuvre de fonctionnalités supplémentaires.

NOTE 2 Les termes remplacer et renouveler sont similaires et souvent interchangeables.

Ces termes s'utilisent qu'il s'agisse d'un composant unique ou du CC complet.

(Cette définition s'appuie sur le texte de l'AIEA-TECDOC-1016, Page 1)

3.9

exigences

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 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 la fiabilité demandée par la conception du système

3.10

sûreté

protection de toute personne contre les risques radiologiques inacceptables

[guide AIEA No 50-SG-D11]

3.11

spécification

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

[CEI 60880-2, définition 3.21]

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 191-13-01]

NOTE The term “maintainability” is also used to denote the maintainability performance quantified by this probability (see 191-02-07).

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*.

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 is the term to be used when there is an *increase in requirements*. 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.

(The definition is based on IAEA-TECDOC-1016 Page 1 text)

3.9

requirements

safety requirements

requirements imposed by authorities on the safety of the NPP in terms of impact on individuals, society and environment during the NPP life cycle

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 fulfilment 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 fulfilment of the reliability demanded by the system design

3.10

safety

protection of all persons from undue radiological hazard

[IAEA safety guide No 50-SG-D11]

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 60880-2, definition 3.21]

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
CC	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
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 de CC 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 seront 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

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

5.2.1 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

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	Programmable Logic Controller
PSA	Probabilistic Safety Assessment
SAT	Site Acceptance Tests
SCC	Station Control Computer
SW V&V	Software Verification & Validation
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 will usually lead to increased functionality and performance improvements, but it is likely that most upgrades will be primarily motivated by problems with the old equipment rather than the perceived benefits of the new.

5.2 Economic motivating factors

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

5.2.1 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 will 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

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 réduira les dépenses de maintenance et peut donner le coût de cycle de vie le plus bas.

5.2.2 Revenu

Le revenu peut être augmenté des 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 permettra 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 de CC 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.

5.2.3 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, que 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.

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 support cost, and may give the lowest overall life cycle cost.

5.2.2 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 will result in better plant utilization. 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.

5.2.3 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 will decrease, 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 time scales 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 analog electronics. Technical education and training courses tend to concentrate on digital technology.

– Vieillessement

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 réduire 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 susceptibles aux effets de vieillissement (exemple: 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 ailleurs. Les exemples suivants traitent des questions de compatibilité:

- Modifications concernant le réacteur ou le matériel associé ayant pour conséquence des exigences de CC différentes;
- Modifications concernant d'autres équipements de CC utilisant des interfaces ou des protocoles de connexions plus récents.

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'avantage économique apparent. Néanmoins, cette décision est finalement d'ordre économique, ainsi il est recommandé que l'exploitant compare 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, il est recommandé d'intégrer une analyse coût/bénéfice où 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 du CC de l'article 6.

– Ageing

The ageing 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 ageing 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 ageing 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.

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. It is recommended where possible that the report include 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 life cycle description in clause 6 should be followed.

6 Présentation générale de la décision de modernisation

6.1 Cycle de vie du CC

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.

Cet article 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. Ce rapport technique traite des phases de cycle de vie demandant 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 de CC.

Cet article 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 du CC de la centrale (de 1 à 3, tableau 1). Les phases suivantes du cycle de vie sont décrites:

- 6.2 «Stratégie du CC long terme»,
- 6.3 «Etudes de faisabilité»,
- 6.4 «Spécifications pour l'appel d'offre et achat de systèmes élémentaires».

L'article 7 «Eléments de réflexion concernant la modernisation» et l'article 8 «Réalisation» présentent d'autres renseignements, à utiliser le cas échéant dans les paragraphes concernés.

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 life cycle is given in table 1.

Based on the input from clause 5 on motivation for modernization this clause 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 clause 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.

Tableau 1 – Phases du cycle de vie du CC

(Voir aussi Tableau XI de l'AIEA-TECDOC-1066)

Phases du cycle de vie du CC	
Stratégie générique de modernisation	Actions, plans et résultats associés
1 Stratégie du CC long terme Répondre aux besoins d'exploitation de la centrale	Evaluation de l'état des systèmes de CC 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 de CC – 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 de CC Spécification des exigences Offres des fournisseurs Commande au fournisseur
4 Spécification des systèmes individuels de CC	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 de CC individuels Réalisation et intégration système	Documentation détaillée sur la production et l'installation, ainsi que guides de maintenance et d'exploitation Système prêt 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 rapport 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
10 Exploitation et maintenance	Rapport permanent des défaillances de système Rapport des résultats des essais périodiques Mise à niveau du simulateur Formation des opérateurs

Table 1 – I&C life cycle phases

(see also Table XI of IAEA-TECDOC-1066)

I&C life cycle phases	
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
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

6.2 Stratégie du CC long terme

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

6.2.1 Evaluation préliminaire de l'état des systèmes de CC 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.

L'historique long terme d'exploitation et de maintenance des systèmes de CC élémentaires 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 de CC 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 de CC défaillants ou obsolètes;
- déclin progressif du niveau de compétence du personnel de la société exploitante et des fournisseurs concernant les systèmes de CC 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 de CC à considérer pour une éventuelle modernisation, et de la priorité relative des différents systèmes de CC.

De plus, il faut tenir compte du fait que dans le cas de défaillances de systèmes de CC 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 du CC; 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 Long-term I&C strategy

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 will affect the modernization programme. These strategic factors will influence the more detailed work of preliminary evaluations and will set the goals for detailed feasibility studies. The preliminary evaluation should suitably identify these factors.

6.2.1 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 has to 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 have to be compared with the budgetary framework which depends on the economics of the plant.

6.2.2 Priorités de renouvellement/mise à niveau des systèmes de CC

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

- élaboration des plans techniques pour l'installation, la mise en service et l'exploitation des systèmes de CC 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.

6.2.3 Conditions limites budgétaires

Le cadre budgétaire des renouvellements/mises à niveau du CC est défini par:

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

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

6.2.4 Evaluation des différents scénarii de modernisation

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

La stratégie du CC long terme doit s'appuyer 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,
- une modernisation en une seule étape.

6.2.2 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 as

- technical plans are produced for the installation, commissioning and operation of the I&C systems concerned,
- intermediate system configurations allowing 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.

6.2.3 Budget boundary conditions

The budgetary framework for I&C renewal and upgrading results from the 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.

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

6.2.4 Evaluation of different modernization scenarios

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 analog and relay based technology.

The long-term I&C strategy has to 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.

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 7.6).

Un ou deux scénarii optimaux ressortiront de cette évaluation. Ceux-ci constituent des choix possibles de stratégie du CC 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, les scénarii choisis devront être revus plus tard sur la base des offres formelles. Il est possible que quelques itérations soient nécessaires.

6.3 Etudes de faisabilité

Au cas où la stratégie du CC long terme démontre le besoin de renouveler ou de mettre à niveau technique une certaine étendue de systèmes de CC, 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* (6.3.1 à 6.3.4), 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* (6.3.5 à 6.3.10).

Il est recommandé que la stratégie du CC 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 inhérents 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.

6.3.1 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 de CC. 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.

Il est recommandé que la liste des objectifs inclue 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;

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 ageing and obsolescence;
- other aspects associated with the modernization (see 7.6).

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

6.3 Feasibility studies

In the case that the long-term I&C strategy demonstrates the need to renew or technically upgrade a certain scope of I&C systems, it is recommended to start *feasibility studies*.

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

- the *generic feasibility studies* (6.3.1 to 6.3.4) 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* (6.3.5 to 6.3.10).

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.

6.3.1 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;

- définir une disponibilité acceptable (fiabilité, maintenabilité et assistance technique) par rapport au coût du cycle de vie du CC;
- s'assurer de la compétence du personnel en ce qui concerne les équipements anciens actuellement en place.

Tout en se concentrant sur les systèmes de CC à moderniser, il convient d'analyser les conditions techniques des renouvellements/mises à niveau prévus:

- les caractéristiques essentielles et l'espace physique disponible et nécessaire pour les produits envisagés;
- la capacité disponible de l'alimentation électrique et des autres fluides;
- revues produits destinées à identifier des technologies de CC adaptées et des familles d'équipement/fournisseurs en ce qui concerne:
 - les interfaces pour les systèmes de CC existants qui seront conservés;
 - les exigences et les capacités du personnel d'exploitation et d'entretien;
 - les références selon le niveau d'autorisation réglementaire exigé;
 - l'IHM (voir 6.3.8 et 7.13);
 - 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 de CC est envisagé, il convient d'étudier les ressources humaines suivantes:

- 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.

6.3.2 Autorisation réglementaire

Les questions d'autorisation sont susceptibles d'avoir un impact majeur sur le projet de modernisation. Dans la plupart des pays, le demandeur d'autorisation doit informer 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 du CC 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 le plus tôt possible sont recommandées.

- 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 analyzed:

- key properties and physical space available and needed for possible products;
- the available capacity of electrical supplies and other services;
- product reviews, to identify suitable I&C technologies and equipment families/suppliers with respect to:
 - interfaces to the existing I&C systems which have to be maintained,
 - requirements and capability of service personnel,
 - references according to the required licensing level,
 - the HMI (see 6.3.8 and 7.13),
 - previous experience with similar modernization projects,
 - optimization 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.

6.3.2 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.

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

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

(Voir les références des articles A.2 et A.3 pour plus de détails sur ce qui peut être nécessaire pour l'étude de sûreté.)

Une fois le champs 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 valider au plus tôt l'ensemble complet de critères de conception du CC. L'analyse de sûreté existante devra éventuellement être mise à niveau. Il est recommandé d'examiner la sûreté et les marges de sécurité opérationnelles du système de CC 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 de CC numériques de sûreté;
- une expérience d'autorisation de solutions comparables mises en œuvre dans d'autres pays peut être partiellement transposée;
- les systèmes prévus ont déjà été conçus ou pré-qualifiés conformes aux normes usuelles et aux exigences en matière de sûreté;
- le système a déjà été évalué par un organisme de réglementation.

Quand une solution innovante est proposée, il convient que le producteur d'électricité s'attende à devoir soumettre des justifications spécifiques.

6.3.3 Coûts budgétaires préliminaires

Le fait que la définition de l'ensemble des systèmes de CC à renouveler ou à mettre à niveau soit compatible avec le cadre budgétaire est nécessaire pour garantir la réussite de la modernisation. Ceci passe généralement par un processus itératif. Il est utile d'intégrer un plafond financier préliminaire en entrée des études de faisabilité, puisque cette limite sera 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 que des simulateurs de formation ou la 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.

The safety case is the licensee's documented demonstration that

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

(See references in clauses A.2 and A.3 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 minimize 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;
- licensing experience of comparable applications in other countries may be transposed to a certain degree;
- the anticipated systems have already been designed or pre-qualified with the safety issues with respect to common standards and requirements;
- the system has already been assessed by a regulator.

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

6.3.3 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 will be a key factor for possible solutions. The budget should include allowances for any high-cost supplementary items 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.

Les frais habituels comprennent:

- frais de capitaux et d'équipement;
- frais détaillés d'ingénierie relatifs à la mise en œuvre du système de CC et à la reprise de l'existant (voir 6.3.5 et 7.20);
- frais de démontage, d'installation et de mise en service;
- frais d'exploitation et de maintenance du système modernisé;
- frais de documentation et de formation du personnel d'exploitation et de maintenance;
- coût du manque à gagner pendant la période d'indisponibilité pour modernisation du système de CC.

6.3.4 Stratégie de réalisation

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 du CC, et
- la définition de l'enchaînement des étapes du renouvellement/mise à niveau, et plus particulièrement la définition des interfaces avec le matériel restant.

6.3.4.1 Architecture globale du CC

La définition de l'architecture globale doit tenir compte de la conception générale révisée de la centrale et de l'ensemble des systèmes de CC, 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 de CC, ainsi que (dans une première étape) une répartition grossière du CC 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 de CC à des systèmes de CC 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.

6.3.4.2 Chronologie de la modernisation

Le second élément de la stratégie de réalisation est la séquence optimale de réalisation des différentes étapes de la modernisation du CC. 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:

Typical costs include:

- capital and equipment costs;
- re-engineering and detailed engineering implementation cost (see 6.3.5 and 7.20);
- 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.

6.3.4 Implementation strategy

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 ageing, 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.

6.3.4.1 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 sub-division 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.

6.3.4.2 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:

- possibilité d'identifier des sous-systèmes pouvant être séparés sans besoin d'interfaces intermédiaires;
- possibilité d'effectuer l'installation pendant le fonctionnement en puissance;
- possibilité de renouvellement coordonné avec une modernisation des systèmes mécaniques et électriques;
- main d'œuvre sur place;
- aspects économiques.

L'étude de faisabilité ne doit pas forcément 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 de CC sont connues. L'article 8 apporte des orientations supplémentaires pour ces deux phases.

6.3.5 Evaluation de la documentation conforme à l'exécution

Cette étape de la phase 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 et 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. Il convient que la revue s'assure aussi 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 conforme à l'exécution nécessaire 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.

Dans ce contexte, les principaux documents intéressants sont:

- les exigences de conception de système, informations sur l'équipement, expérience d'exploitation, notifications de modification technique passées;
- rapports de sûreté;
- spécifications de conception des fonctionnalités;
- schémas fonctionnels;
- points de consigne;
- précision;
- constantes de temps et temps de retard admissibles;
- paramètres procédé;
- algorithmes de traitement;
- 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.

- possibility to identify subsystems which can be separated without the need for intermediate interfaces;
- possibility to perform installations during power operation;
- possibility to co-ordinate in time the renewal with the modernization of mechanical or electrical systems;
- manpower on site;
- economics.

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 provides additional guidance for both phases.

6.3.5 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.

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;
- processing algorithms;
- 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.

6.3.6 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.

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

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 notamment 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 leur validité devra être justifiée.

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

- exigences générales;
- exigences fonctionnelles;
- exigences matérielles;
- domaine des fonctions et matériel;
- interfaces (signaux standards, types non standards, types d'interfaces série, etc.);
- exigences d'installation;
- divers.

Le contenu préconisé est développé en 7.3 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.

6.3.7 Affectation de fonctions

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

Les activités principales lors de cette étape de conception sont:

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

6.3.6 Basic requirement specification

Design basis events, i.e. postulated initiating events and also following event sequences should be considered when preparing the basic requirement specification.

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 have to 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 have to be justified.

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

- general requirements;
- functional requirements;
- equipment 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 7.3 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.

6.3.7 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 is sufficient to meet the requirements of 'defence in depth' or that the functions are graded as diverse with respect to a common plant safety objective,
- the assignments of tasks to operating and maintenance staff.

6.3.8 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 de CC. Dans les cas où l'affectation de fonctions ne correspond pas à la conception du CC 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 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 de CC, de communication, etc., puisque celles-ci sont impactées par la modernisation du CC.

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, etc. des instruments.

Il convient que l'approfondissement et la portée de l'analyse soient compatibles avec l'étendue de la modernisation du CC 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);
- du contenu, des formats et de la conception des affichages sur les unités de visualisation;
- du traitement de données pour l'affichage de l'état des systèmes;
- de l'adaptation 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.

6.3.8 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;
- 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 analyzed, and the analysis of different scenarios considered in the task analysis should be done with the help of safety and process engineers.

6.3.9 Acquisition 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 de CC, 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 de CC. L'utilisation d'un système de gestion de bases de données (SGBD) standard est recommandée. 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 de CC, y compris une 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 au constat fait à la centrale qui soit à la fois souple et sécurisée, appuyée par une assurance qualité efficace.

6.3.10 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 de CC soit conforme aux exigences suivantes:

- il convient que la spécification soit compréhensible par les ingénieurs de CC et de sûreté, ainsi que par les évaluateurs et les ingénieurs de 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. 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, ne pas oublier qu'une centrale typique a 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 demande 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 7.19).

6.3.9 Data collection

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 will require a flexible yet secure method of correction of errors found in the data, by comparison with the plant, and with suitable supporting QA.

6.3.10 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 life cycle.

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 operators. Presentations should include the current state of the plant, and also the ability to show historical traces. The design of these displays will require 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 7.19.

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

Les exigences pertinentes pour la réalisation du système de CC 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 de CC 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.

6.4.1 Spécifications des propriétés du système de CC pour les solutions candidates

Ce paragraphe décrit les exigences de base nécessaires à l'élaboration réussie des spécifications d'un système de CC. 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 de CC soit homologué ou homologuable afin d'assurer une robustesse convenable en ce qui concerne les séismes et les phénomènes naturels (CEI 60780, CEI 60980, CEI 60987, CEI 61000, CEI 61513);
- il convient que les logiciels possèdent une structure modulaire claire et un développement coordonné selon la CEI 60880 et son supplément ou d'autres normes logicielles applicables;
- il convient que le système de CC soit suffisamment souple et performant pour garantir la fonctionnalité requise ainsi que des temps de réponse satisfaisants;
- il convient que le comportement exigé du système de CC 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 de la maintenance des logiciels tout au long du cycle de vie, l'état de la technique courant consiste à mettre en œuvre un atelier logiciel capable de générer du code automatiquement. L'obtention de l'autorisation réglementaire pour des systèmes de CC 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.

6.4.2 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,

6.4 Tender specification and purchasing of the individual systems

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 will be 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.

6.4.1 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 60780, IEC 60980, IEC 60987, IEC 61000, IEC 61513);
- the software should have a clear modular structure with a coordinated development according to IEC 60880 and its supplement, 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 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.

6.4.2 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, it is recommended that common

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 demandé, 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 y a lieu 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.

6.4.3 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 pour les systèmes concernés. 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 la solution. Il est recommandé que le projet examine les preuves de la qualité des logiciels afin de s'assurer qu'aucun problème ne survienne 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. Il convient que des références concernant des installations antérieures soient fournies.

6.4.4 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. 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 avec les autres parties conservées de la centrale.

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

specifications are 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.

6.4.3 Tenders for each system

The potential suppliers will 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. 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.

6.4.4 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 contact 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 will then serve as a reference for proceeding with design, implementation and installation of the system.

7 Eléments de réflexion concernant la modernisation

Il convient que la modernisation du système de CC 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 dans les paragraphes suivants. Il convient de reprendre celles-ci dans le cahier des charges.

7.1 Codes et normes réglementaires

Le système de CC modernisé devra probablement satisfaire aux normes et codes réglementaires en vigueur. Les codes et normes à utiliser et l'indice de révision applicables doivent être convenus et 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 l'Annexe A.

7.2 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 de CC modernisé.

Le choix d'un système de CC 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 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 seules fonctions des systèmes de sûreté ou relatifs à la sûreté.

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

Il convient que les objectifs et exigences du système de CC 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:

a) 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 l'édition des codes et normes avec lesquelles le système de CC 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,

7 Considerations for modernization

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

7.1 Regulatory codes and standards

The modernized I&C system will probably have 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.

Annex A provides some useful references.

7.2 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 an NPP are the following:

- to limit the number of control system vendors to allow overall plant standardization on a cost-effective basic industrial system that would result in low O&M costs;
- 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.

7.3 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:

a) 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;

- fiabilité,
- maintenabilité,
- classement du code.

b) Exigences fonctionnelles

- 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 de CC (CEI 60964),
- 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.

c) 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 concernant la tolérance aux défaillances 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.

d) 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.

e) 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 entre le producteur d'électricité et le fournisseur, et entre fournisseurs.

- reliability;
- maintainability;
- code classification.

b) Functional 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);
- 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.

c) 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 failure tolerance and 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 (including accident conditions) and seismic;
- the quality assurance of software or programmable equipment;
- input and output signals.

d) 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.

e) 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 between the utility and supplier and between suppliers.

f) 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.

g) 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).

7.4 Fiabilité du système de CC

Il est recommandé de déterminer les objectifs de fiabilité pour chaque système ou composant constituant le système de CC mis à jour. Ces objectifs seront dérivés des exigences globales de performance du système, qui peuvent être imposés 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 de CC, 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 et 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'être restauré progressivement à la suite d'une éventuelle défaillance de CC.

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

f) Installation requirements

- limitations of power supplies;
- cabinet and cable tray space;
- sensor installation limitations;
- penetrations;
- ventilation.

g) Others

- design review requirements;
- V&V, qualification;
- information on available documents and re-engineering of documentation;
- the identification of required documentation, for example 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).

7.4 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.

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

7.5 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 pourrait facilement être installés dans l'emplacement de l'équipement existant.

Il convient également de considérer dans les considérations économiques le manque à gagner en termes de production perdue pendant la réalisation du système de CC modernisé, ainsi que le déclassement de la centrale entraîné par l'installation du système de CC 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 de CC 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, comme avec les systèmes actuels.

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 procédé 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, qui partageront 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'utilisées parfois 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, de rendre compte des moyens nécessaires.

7.6 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:

7.5 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 do maintenance and testing during plant operation instead of during outage periods with present systems.

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.

7.6 Risks and benefit study

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

- 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 de CC 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.

7.7 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 autres fonctions relatives à la sûreté.

Les dernières normes (exemple: CEI 61226) raffinent 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 (par exemple: API et systèmes IHM numériques).

Les derniers classements de sûreté montrent que la séparation des systèmes de CC 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 de CC d'exploiter les sous-classes 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.

7.8 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 de CC 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.

- 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, ageing;
- the influence of ageing 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.

7.7 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.

7.8 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 operations of other safety systems at any time during a DBA.

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, etc.).

Il est recommandé de déterminer les exigences de conception antisismique. L'équipement mis à niveau devra éventuellement se conformer aux dernières normes antisismiques. Il faut définir le niveau des exigences antisismiques 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 du personnel, outillages spéciaux, etc.) ancrés au sol afin d'éviter que des objets non fixés ne mettent en danger l'équipement homologué antisismique du local.

7.9 Exigences de qualification de logiciels

La modernisation des systèmes de CC de sûreté effectuée à l'aide de systèmes de CC 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 Annexe A.

- Il est recommandé d'utiliser un système de classement pour les fonctions de CC, afin de permettre la définition d'une échelle d'exigences pour différentes classes de systèmes et fonctions.
- Il est recommandé d'effectuer une analyse de défense en profondeur et de diversité afin d'identifier toute possibilité de DMC impliquant des logiciels et d'évaluer d'éventuelles parades.
- La conception du logiciel doit être soumise 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:

- 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.

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;
- ageing;
- 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 unanchored objects from jeopardizing the seismically qualified equipment in the same area.

7.9 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 modernized 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 Annex A.

- It is recommended to use a classification scheme for the I&C functions, allowing the definition of graded requirements for different classes of systems and functions.
- A 3D analysis is recommended, to identify the potential for software related common mode failures, and to evaluate potential countermeasures.
- Appropriate requirements have to 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:

- 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.

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 standards est à encourager autant que possible. Il est recommandé que les composants logiciel réutilisables (par exemple: 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.

7.10 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 des nouvelles technologies, par exemple: chemins de câbles spéciaux pour fibre optique, câbles de bus, et exigences séparation,
- charges au sol,
- capacités des systèmes auxiliaires; par exemple: 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 numérique doit remplacer un système raccordé en fil-à-fil, il sera nécessaire de faire de la place pour des chassis et des panneaux E/S. Le remplacement de composants isolés aura peu d'impact sur le câblage existant.

7.11 Aspects technologiques

Il est recommandé pour des systèmes de CC mis à niveau d'établir des exigences révisées ou nouvelles telles que:

- exigences pour systèmes auxiliaires,
- exigences sur les alimentations électriques,
- exigences supplémentaires issues de l'expérience opérationnelle,
- amélioration de l'aide à l'opérateur,
- exigences de transition.

Le matériel de CC 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 susceptible 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 radioactifs 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.

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 minimizes the project-specific licensing effort and risk.

7.10 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, for example special cable trays for fibre-optic cables, bus cables and requirements for separation;
- floor loading;
- auxiliary systems capacities, for example 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.

7.11 Technology considerations

The establishment of revised or new requirements is recommended for upgraded I&C system such as

- requirements for support systems;
- requirements for power supplies;
- further requirements based on operating experience;
- improvement of operator assistance;
- transitional requirements.

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 use of a shielded, low EMI level environment is recommended to house the new digital equipment. Electronic equipment is sensitive to radioactive radiation and should be suitably qualified for its proposed location, taking into account dose rates from normal operation and accident conditions.

Il convient de noter que de nos jours le cycle de vie du matériel de CC se réduit progressivement, suite à une évolution rapide de la technologie électronique, support du CC.

Les capteurs/transducteurs deviennent plus «intelligents», grâce à une conception faisant appel aux micro-contrôleurs embarqués. L'auto-étalonnage, les fonctions d'auto-test et le diagnostic intégré 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 procédé). Les circuits analogiques utilisés pour l'instrumentation discrète sont en voie d'obsolescence et sont remplacés par leur équivalent numérique, ce qui dans certains cas offre une plus grande précision, une performance et une fiabilité améliorées.

La révolution dans le monde de la conception numérique concerne également les dispositifs de commande finaux et de nombreuses vannes «intelligentes» sont déjà commercialisées.

Les boucles de commande analogique individuelles configurées avec des instruments analogiques discrets et des interconnexions en fil-à-fil sont de plus en plus dépassées 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 procédé 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 bien peut être mis en oeuvre par l'un des différents modules logiciels de commande.

Une fois qu'un signal de mesure d'un paramètre procédé 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 et 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 de la 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.

La décision de remplacer un système de CC à boucle de commande analogique discrète par un système à architecture numérique implique la résolution des points suivants:

- une approche raisonnable de la question de V&V, et des normes de recette du matériel fabriqué. Les normes CEI applicables se trouvent dans l'article A.1;
- l'étendue de la modernisation du CC 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;

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 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 analog measurements to a digital format from the front end, as close to the sensor/transducer (and process) as possible. Analog 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.

The revolution in digital design is also affecting final control elements, and many "smart" valves are already on the market.

Individual analog control loops configured from discrete analog 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 analog 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 DCS 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 analog 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 computerized safety systems, has led to the situation where significant amounts of time are required for SW V&V tasks, even in cases where program code changes are minimal, i.e. a set point change.

The decision to upgrade a discrete analog 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 clause A.1;
- the scope of the I&C modernization and the impact of having multiple architectures in the same plant. Digital equipment designed to replace analog-based equipment in discrete analog loops using the existing wiring should not be difficult. However, the replacement of complete analog loops with a digital control system will result in hardware and wiring differences;

- la compatibilité avec les SNCC de la centrale existants, l'interface/communications avec les nouveaux;
- la modernisation ultérieure, la migration vers de nouvelles générations de systèmes de commande et la protection contre l'obsolescence;
- la prise en compte du fait que l'équipement numérique ne se comporte pas toujours de la même manière que son équivalent analogique ou à base de relais.

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

Il convient d'établir un inventaire des équipements et du matériel pour le système de CC 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 restant 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.

7.13 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. L'article A.1 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, fenêtre de message, étiquetage, et fonctions des consoles,
- idem pour les postes de commande secondaires, en prenant en compte les différences fonctionnelles,
- IHM et son impact sur les procédures d'exploitation,

- 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 analog or relay based equivalent.

7.12 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 minimize the possibility, for example:

- 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.

7.13 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, for example IEC 61839. Other IEC standards supporting HMI-design can be found in clause A.1. 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, window annunciation, labelling, and console functions;
- secondary control area considerations similar to the main control room, but allowing for functional differences;
- HMI and its impact on operating procedures;

- 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 matérielle + logicielle. 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,
- 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 une étude ergonomique avant acceptation de la conception définitive. Il faudra 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 (clignotement, type de sirène, fonctions des boutons-poussoirs).

Les exigences antisismiques 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.

- 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 visualize 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 will have to 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 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.

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.

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.

7.14 Analyse DPD

Les mises à niveau récentes 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 et qui peuvent amener à des comportements imprévisibles. 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 pour 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 de CC 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 désormais 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 en ce qui concerne les programmes de modernisation numérique jusqu'à présent:

– 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 de CC

Certains organismes de réglementation ont accepté l'argument expliquant que la DMC n'entraîne que des problèmes passifs (dormants) au niveau du système de CC. D'autres demandent 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 demande souvent des modifications de conception afin de garantir un résultat acceptable.

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.

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.

7.14 3D analysis

Recent I&C upgrading usually replaces old analog equipment with new digital equipment due to the obsolescence of analog 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 analog 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 paragraphs 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.

– 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 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 exemple: différentes applications tournant sur la même plateforme produit ou système d'exploitation logiciel). D'autres demandent 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 de CC diversifiés accrédités.

Malgré ces différences, il a été prouvé lors de plusieurs projets de modernisation que le problème de la DMC peut être résolu, et ce de façon économique. 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.

7.15 Séparation et protection contre les incendies et les inondations

Il convient que chaque train d'équipement soit isolé physiquement et électriquement des autres trains afin d'empêcher les événements de mode commun et les défaillances de cause commune.

Il est recommandé afin de séparer les fonctions et de renforcer la robustesse, 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 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.

7.16 Incertitude et calcul des points de consigne

Les points de consigne des systèmes de CC 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 des incertitudes de différentes sortes concernant les composants de CC du système. Quand le nouvel équipement de CC 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 le nouveau système soit 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.

- 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 CMF 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.

7.15 Separation and protection against fire and flooding

Each equipment train should be physically and electrically separated from all other equipment trains to avoid common mode events or common cause failure.

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.

7.16 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.

7.17 Analyse du temps de réponse

Le temps de réponse du nouvel équipement utilisé pour la mise à niveau n'est pas toujours plus court que 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.

7.18 Essais

Avant la recette formelle, les sous-systèmes du système de CC seront intégrés et testés. Ceci peut comprendre des essais à boucle ouverte et fermée, des essais sur le terrain ou des essais 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 essai d'exploitation) apporteront 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 (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 bogues logicielles,
- 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. Les essais doivent être définis de façon détaillée à l'aide de procédures d'essai, 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.

Les procédures existantes relatives aux essais périodiques du système de CC, aux essais de temps de réponse, à la surveillance et à l'étalonnage devront être 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.

7.19 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 convient qu'il soit mis en place tôt dans le projet. Un tel système facilitera l'interface fournisseur/client pendant le projet et apportera dès le départ 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.

7.17 Response time analysis

The response time of new equipment used for upgrading is not always faster than 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.

7.18 Test procedures

Prior to formal acceptance tests, subsystems of the I&C system will be 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) will 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 (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 have to 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 will have to 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.

7.19 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 will make the supplier/customer interface easier during the project and give 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.

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 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 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 civils.

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 seront 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 de CC 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.

7.20 Mise à niveau de la documentation technique de la centrale

Les documents et schémas de conception existants ne reflètent pas forcément l'état réel de la centrale physique existante pour cause de modifications effectuées sur le terrain qui n'ont pas été documentées et 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 sera ensuite utilisée pour déterminer si la centrale physique est conforme aux prescriptions actuelles relatives aux systèmes de sûreté et aux systèmes procédé. Il convient de classer tout écart en tant que manque ou que déficience de conception.

Il est recommandé que la documentation mise à niveau 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 lorsqu'aucune documentation concernant la conception n'est disponible ou si la documentation existante est incomplète ou inexacte. Si c'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 de CC ainsi que son état.

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 would be 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 has to be finalized later, after the new I&C has been installed and commissioned. This effort should not be underestimated.

7.20 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 walkdown 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.