IEC 60965

Edition 3.0 2016-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Control rooms – Supplementary control room for reactor shutdown without access to the main control room

Centrales nucléaires de puissance – Salles de commande – Salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale

IEC 60965:2016-02(en-fr)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

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

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

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

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

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

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

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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

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

IEC 60965

Edition 3.0 2016-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Control rooms – Supplementary control room for reactor shutdown without access to the main control room

Centrales nucléaires de puissance – Salles de commande – Salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-3203-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – CONTROL ROOMS – SUPPLEMENTARY CONTROL ROOM FOR REACTOR SHUTDOWN WITHOUT ACCESS TO THE MAIN CONTROL ROOM

FOREWORD

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

International Standard IEC 60965 has been prepared by subcommittee 45A: Instrumentation, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2009. This edition constitutes a technical revision.

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

a) requirements associated with regular testing of the supplementary control room (SCR);
b) requirements to assess the time available during which the reactor will be safe but unattended, in order to move from the main control room (MCR) to the SCR and for the SCR to become operational;
c) reference to SSR-2/1 which includes the following new requirements:

1) the SCR should be functionally (as well as physically and electrically) separate from the MCR,
2) consideration shall be given to the provision of shielding against radioactivity on the access paths to the SCR;

d) reference to DS431, the revision of NS-G-1.3, including the following new requirements:
1) to implement at least two diverse methods for communication with a set of predefined locations,
2) to implement features to support monitoring of trends in key plant parameters;

e) requirements for the role, functional capability and robustness of the SCR in design extension conditions;

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

FDIS	Report on voting
45A/1060/FDIS	45A/1078/RVD

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

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

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

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

INTRODUCTION

a) Technical background, main issues and organization of the standard

IEC 60965:1989 was developed to provide requirements relevant to the design of NPP supplementary control points for reactor shutdown without access to the main control room. The first edition of IEC 60965 has been used extensively within the nuclear industry. It was however recognized in 2007 that technical developments especially those which were based on software technology should be incorporated. It was also recognized that the relationships with the standard for the main control room (i.e. IEC 60964) and the derivative standards to that standard (i.e. IEC 61227, IEC 61771, IEC 61772, IEC 61839, and IEC 62241) should be clarified and conditioned. In 2009 the second edition of IEC 60965 was published.

In June 2013, during the Moscow meeting, WG A8 experts recommended a limited revision be launched to take into account the lessons learned from TEPCO Fukushima Daiichi accident and some comments formulated during the circulation of the FDIS of the published second edition. In the course of development of this revision, the title of the standard was amended to refer to Supplementary Control 'Room' for consistency with IAEA SSR-2/1.

This IEC standard specifically focuses on the functional design process of the supplementary control room of an NPP. It is intended that the standard be used by NPP designers, design authorities, vendors, utilities, and by licensors.

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

IEC 60965 is the third level IEC SC 45A document tackling the issue of the design of a supplementary control room.

IEC 60965 is to be read in association with IEC 60964 for the design of the main control room (including the derivative standards mentioned above) which is the appropriate IEC SC 45A document providing guidance on operator controls, verification and validation of design, application of visual display units, functional analysis and assignment, and alarm functions and presentation.

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

c) Recommendations and limitations regarding the application of this Standard

The purpose of this standard is to provide functional design requirements to be used in the design of the supplementary control room of a nuclear power plant to meet safety requirements.

This standard is intended for application to a supplementary control room whose conceptual design is initiated after the publication of this standard. The recommendations of the standard may be used for refits, upgrades and modifications.

Aspects for which special recommendations have been provided in this Standard, in accordance with IAEA safety standards, are:

– definition of the MCR and plant design bases for which the supplementary control room are to be used;
– access by station staff to the supplementary control room in such emergencies;
– assurance for the station staff that the environment in the supplementary control room is safe when it is to be used;
– provision of information in the supplementary control room on the state of the reactor critical functions;
– transfer of control and indication functions from the main control room to the supplementary control room in emergencies;
– independence and separation of the cabling used by the supplementary control room from that used by the main control room;
– assurance that a safe state has been reached using the supplementary control room;

– communication facilities between the supplementary control room and to the station management.

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

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

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

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

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

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

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers to ISO as well as to IAEA GS-R-3, IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements SSR-2/1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

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

NUCLEAR POWER PLANTS – CONTROL ROOMS – SUPPLEMENTARY CONTROL ROOM FOR REACTOR SHUTDOWN WITHOUT ACCESS TO THE MAIN CONTROL ROOM

1 Scope

This International Standard establishes requirements for the Supplementary Control Room provided to enable the operating staff of nuclear power plants to shut down the reactor, where previously operating, and maintain the plant in a safe shut-down state in the event that control of the safety functions can no longer be exercised from the Main Control Room, due to unavailability of the Main Control Room or its facilities. The design has to ensure that the Supplementary Control Room is protected against the hazards, including any localised extreme hazards, leading to the unavailability of the Main Control Room.

The standard also establishes requirements for the selection of functions, the design and organisation of the human-machine interface, and the procedures which shall be used systematically to verify and validate the functional design of the supplementary control room.

It is assumed that supplementary control room provided for shutdown operations from outside the main control room would be unattended during normal plant conditions other than for periodic testing. The requirements reflect the application of human engineering principles as they apply to the human-machine interface during such periodic testing and during abnormal plant conditions.

This standard does not cover special emergency response facilities (e.g. a technical support centre) or facilities provided for radioactive waste handling. Detailed equipment design is also outside the scope of the standard.

This standard follows the principles of IAEA Specific Safety Requirements SSR-2/1 and IAEA Safety Guide NS-G-1.3.

The purpose of this standard is to provide functional design requirements to be used in the design of the supplementary control room of a nuclear power plant to meet safety requirements.

This standard is intended for application to a supplementary control room whose conceptual design is initiated after the publication of this standard. If it is desired to apply it to existing plants or designs, special care must be taken to ensure a consistent design basis. This relates, for example, to factors such as the consistency between the supplementary control room and the main control room, the ergonomic approach, the automation level and the information technology, and the extent of modifications to be implemented in I&C systems.

2 Normative references

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

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

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

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

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

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

IEC 62646, *Nuclear power plants – Control rooms – Computer based procedures*

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

ISO 11064-1, *Ergonomic design of control centres – Part 1: Principles for the design of control centres*

ISO 11064-3, *Ergonomic design of control centres – Part 3: Control room layout*

ISO 11064-6, *Ergonomic design of control centres – Part 6: Environmental requirements for control centres*

IAEA SSR-2/1:2012, *Safety of nuclear power plants: Design*

IAEA NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants (to be replaced by SSG-39)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. For other terms, refer to the general terminology defined in IEC 60964, IEC 61513 and in the IAEA NUSS programme, such as Safety Guide NS-G-1.3 or the safety glossary.

3.1
control room staff
group of plant personnel stationed in the control room, which is responsible for achieving the plant operational goals by controlling plant through the human-machine interface. Typically, the control room staff consists of supervisory operators, and operators who actually monitor plant and plant conditions and manipulate controls, but may also include those staff members and experts who are authorised to be present in the control room, e.g. during long lasting event sequences

[SOURCE: IEC 60964:2009, 3.4]

3.2
design extension conditions
postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions include conditions in events without significant fuel degradation and conditions with core melting

[SOURCE: IAEA SSR-2/1:2012, definitions revised as DS462]

3.3
local control points
local control facilities
points (or facilities) located outside the control room where local operators perform control activities

[SOURCE: IEC 60964:2009, 3.17]

3.4
local operators
operating staff that perform tasks outside the control room

[SOURCE: IEC 60964:2009, 3.18]

3.5
operating staff
plant personnel working on shift to operate the plant. The operating staff includes the control room staff, maintenance engineers, etc.

[SOURCE: IEC 60964:2009, 3.20]

3.6
supplementary control room
location from which limited plant control and/or monitoring can be carried out to accomplish the safety functions identified by the safety analysis as required in the event of a loss of ability to perform those functions from the Main Control Room

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

4 Abbreviations

CBP Computer-Based Procedure
I&C Instrumentation and Control
LCP Local Control Point
MCR Main Control Room
NPP Nuclear Power Plant
PIE Postulated Initiating Event
SCR Supplementary Control Room
V&V Verification and Validation

5 Design principles

5.1 General

Requirement 66 of IAEA SSR-2/1 states: “Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.”

NOTE 1 The reference to “control room” is interpreted in this standard as “main control room (MCR)”.

NOTE 2 Functional separation means that the function of the SCR can be performed despite postulated malfunctions in the MCR.

NOTE 3 Complete functional separation of paths from human-machine interface control points out to end devices may be difficult to achieve for all I&C functions, especially for example when a shared actuator requires a common priority logic controller to select between MCR and SCR control. Any such common equipment is acceptable if adequate redundant, backup, or field equipment exists that can achieve the required actuation function and is sufficiently separated from common hazards to minimize the risk that the function may be completely disabled.

Subclauses 6.15 to 6.30 of IAEA NS-G-1.3 provide guidance on the requirements for supplementary control rooms, including requirements associated with the following:

- definition of the plant design bases that require use of the SCR (6.17, 6.19, 6.20);
- location and configuration of the SCR to promote prompt mobilisation (6.29);
- qualified access path to the SCR, with hazard indication and suitable countermeasures along this path (6.27, 6.28);
- prevention of unauthorised access to or use of the SCR (6.21);
- safety functions of the MCR and SCR not affected by the same PIE, and independence of the circuits associated with the SCR from those of the MCR (6.20, 6.23);
- priority of control between the MCR and SCR, and transfer of control from the MCR to the SCR (6.18, 6.20, 6.24);
- manual control in the SCR accomplished by simple actions (clause 6.22);
- displays and controls in the SCR similar to those in the MCR, to the extent possible (6.22);
- consideration of the difference of purpose between the MCR and the SCR (6.25);
- if long-term use is envisaged, suitable facilities for habitability and workspace for tasks (6.30).

5.2 Main objectives

The IAEA requirements for the design of the SCR given in 5.1, paragraph 1, shall be met as detailed in this standard.

The SCR shall be provided with the means to trip the reactor and bring the plant to a safe state and maintain it in that state without access to the MCR. However, the SCR is not required to perform all the other plant control and monitoring functions which are typically performed in the MCR. According to the type of NPP and the detailed safety arguments, provisions to cope with a predefined set of PIE could be integrated in the SCR.

The SCR is required when the ability to perform safety functions in the MCR is lost. Possible causes include a control room fire, the entry of excess smoke or a dangerous atmosphere to the MCR, severe damage to the MCR or its cables such that safety functions cannot be performed, major damage to the control room area, or major failure of control room facilities.

The design basis PIE and sequences of events for which use of the SCR is necessary shall be identified. This shall include identification and justification of the assumed conditions throughout the plant and the corresponding durations for which the SCR may be required.

Since events leading to the unavailability of the MCR are very infrequent, it is anticipated that the plant safety analysis will demonstrate that such events can only coincide with another independent event in the plant at an acceptably low frequency; in particular, it is anticipated that the primary coolant circuit will be intact. However, due account shall be taken of any plant fault that may occur as a consequence of reactor trip and of any plant faults at shutdown that are of sufficient frequency to coincide with use of the SCR. In particular, the design of the SCR shall take account of the possible long-term unavailability of the MCR due to fire or other reasons.

The criteria for use of the SCR shall be clearly stated in the plant operating procedures.

It shall be possible to determine the complete safety state of the plant from outside the MCR. This should preferably be from the SCR. The SCR should therefore enable the monitoring of the state of the relevant plant systems and key plant parameters. All information presented should comply with the ergonomic principles presented in the relevant parts of ISO 11064.

For the purpose of efficient monitoring and later analysis of the events, key plant parameters should be recorded to allow display of trends and later access for offline analysis. Automatic recording is recommended. If the MCR and SCR are assumed not to be staffed for an extended period of time, automatic recording shall be provided.

From an operational viewpoint (e.g. to simplify operation and avoid misunderstanding), it is preferable to have only one supplementary control room. Care shall be taken, however, to meet safety requirements, particularly requirements for redundancy and independence. If two or more supplementary control points are provided for an existing plant, each supplementary control point should display all information needed to perform the operator tasks.

Computer-based information displays in the SCR should provide the same functionality for the presentation of information important to safety as the corresponding displays in the MCR. The content of the displays for a given plant state and for given operator tasks should be the same as in the MCR.

There shall be adequate time to reach the SCR before necessary actions are required as well as sufficient equipment to provide necessary communication between all operating staff involved in these actions and with on-site and off-site locations. Communication requirements are given in 7.7.

The layout of the instrumentation and the mode of presentation at the SCR shall provide the operating staff with adequate information to assess the plant state and to supervise the shutdown (and subsequent hold down) of the reactor, the long-term cooling of the reactor core and confinement of all radioactive substances.

The plant systems that can be controlled from the SCR may be limited to those providing the safety functions.

The SCR shall provide sufficient control over the safety functions to reach and maintain a safe state, for the defined set of PIEs and conditions for which the MCR cannot be used. The supervision and control provided at the SCR shall include the state of the safety functions concerned and control of their initiation and termination, and the state of the related fundamental safety functions (see IAEA SSR-2/1:2012, Requirement 4).

Facilities for site security monitoring, plant access control and fire alarms which are normally provided in the MCR shall also be provided in an independent location. This independent location may be the SCR or may be a location that would not be affected by the same event that causes the SCR to be used. Where the latter applies, the facilities location shall have a hazard withstand capability equivalent to that of the SCR.

The design of SCR shall be consistent with the MCR design. The identification and design process for the relevant controls and indications needed for the SCR shall follow the requirements of IEC 60964, as summarised in Clause 6 of this standard.

5.3 Safety principles

5.3.1 Design basis and design extension conditions

The design basis of an NPP normally specifies the internal and external hazards to be taken into account. The design shall ensure that such events are not able to make those functions of the MCR and SCR (and local control points) required for safe shutdown, monitoring to ensure safe shutdown and critical functions control and monitoring, unusable or ineffective simultaneously.

If the design basis is extended to address extreme hazards or low probability failure combinations, the design should ensure that the MCR and SCR will not fail together even under such circumstances. The implementation of the transfer of control to the SCR shall take due account of the practical constraints arising from the design basis or design extension assumptions for use of the SCR.

The above requirement for non-susceptibility of the MCR and SCR to the same design basis or design extension condition shall be extended to their respective supporting functions, systems and equipment.

5.3.2 Functionality and qualification

The functions of the SCR shall be classified in accordance with IEC 61226, with due account being taken of the criteria described in 5.2 for the use of the SCR.

Equipment and systems shall be designed with a degree of redundancy in accordance with their safety classification. Account shall also be taken of the need for functional isolation and physical separation where safety and non-safety systems and redundant systems are brought into close proximity (see IEC 60709).

The SCR equipment shall be suitable for the environmental conditions applicable to its intended use. The equipment shall be qualified for the design basis PIE and relevant sequence of events in accordance with its safety classification. Supplementary tests or analyses may be necessary to provide assurance of adequate reliability and robustness to withstand the stresses from design extension conditions.

5.3.3 Accessibility and operator transfer time

Taking into account the postulated causes of unavailability of the MCR functions, the SCR functions shall be so designed (and, if necessary, the SCR so located) that, even under emergency conditions, the SCR is accessible by safe routes. See 7.3 for further details.

The design shall allow adequate time for control room staff to reach the SCR after the MCR becomes unavailable. The actions and duration of unattended automatic operation of the safety functions, after initiation at the MCR, in order to maintain plant safety up to the time when the SCR becomes operational, should be shown to be satisfactory for this transfer. This shall include time for access control and time to assess the plant state at the SCR. Annex A addresses the aspects that are to be considered for theoretical assessment of the safe transfer time window.

5.3.4 Control transfer, control prioritisation and security

Facilities to disable MCR control and transfer control to the SCR shall be provided. These facilities shall be classified according to the highest category of safety functions for which control from the MCR could be disabled. They shall be demonstrated as highly reliable and, if required, demonstrated to comply with the single failure criterion. Possible failures in SCR security and the influence of SCR cybersecurity flaws on I&C security shall be analysed and taken into account.

NOTE The above excludes any requirement to disable the MCR manual ‘reactor trip’ function.

The control transfer facilities shall disable the MCR controls in order to ensure that a fire or damage affecting the MCR cannot cause spurious control actions. The facilities shall also be such as to avoid or minimize transients of the controlled variables during the transfer of control, in both directions: from MCR to SCR and from SCR to MCR.

The control transfer facilities may be on the route from the MCR to the SCR, or at the SCR, or in the MCR itself if analysis shows that this cannot lead to failure to accomplish the control transfer or failure of control from the SCR. Where the facilities are located in the MCR, additional means that do not involve the MCR should also be provided.

The SCR should include a means to identify the control status of the SCR and of the MCR controls (i.e. whether “enabled” or “disabled”).

I&C systems shall be so designed to prevent both the MCR and SCR from taking control of plant systems simultaneously.

I&C systems shall be so designed that there is an acceptably low probability of false signals from the MCR elements of the systems affecting plant safety. I&C systems shall be so designed that there is an acceptably low probability of false signals from the SCR elements of the systems interfering with the supervision and control of plant from the MCR under normal or abnormal conditions. Examples of design techniques to achieve these objectives are the use of: transfer switches, coded signals, optical isolation links.

A malfunction of the equipment controlling the transfer of control from the MCR to the SCR could lead to unintended isolation of the MCR. Therefore, the failure modes of the equipment that implements the control transfer function shall be analysed and shown to be acceptable. This analysis shall consider all PIEs for which operation from the MCR is credited.

When an SCR is in use, actions taken from it shall have priority over any other manual control actions, except when control has to be taken at a local control point.

The design of the SCR shall include provisions to prevent unauthorised access or use. The means of control transfer shall also include provisions to prevent unauthorised transfer of control from the MCR to the SCR and vice versa. Access to the SCR, and any attempt at control transfer to the SCR, shall be indicated by the provision of alarms in the MCR.

Where an SCR is unattended during normal plant operation, the SCR shall be regularly verified to ensure that the assigned level of security is being met.

All the procedures used during MCR software modification shall be also applied to the modification of SCR software.

5.3.5 Operational considerations

The SCR shall be designed to minimise operator errors.

The design shall include the provision of written instructions in the SCR for operation of:

- plant systems and control devices;
- information and recording systems;
- communication equipment;
- any other equipment to be operated from the SCR.

The operating procedures for actions to be taken from the SCR (e.g. plant cooldown) shall be simple and clear. They shall be based on the same principles and the way of presentation as the MCR operating procedures, and shall deviate only where differences are imposed by the local control facilities and by the available control means and systems. Additional training should be provided whenever an SCR operating procedure deviates from the equivalent MCR operating procedure.

Even if computer-based procedures (CBP) are implemented for the SCR, paper-based procedures shall be available. This allows failure of the CBP equipment to be mitigated and combinations of activities in the SCR and local actions to be more easily managed. For guidance on the design of CBP, see IEC 62646.

The designer shall specify the regular testing and inspection of the SCR equipment required to meet the design and safety principles. Requirements for regular testing and inspection are given in 7.9.

The design shall permit regular training and practice in the use of the SCR without affecting plant availability.

5.4 Human factors engineering principles

In order to provide an optimal assignment of functions which ensures maximum utilisation of operator and system capabilities and to achieve the maximum plant safety, the design shall pay particular attention to the human factors engineering principles and human characteristics of personnel under emergency conditions, especially for immediate actions, i.e. actions to be performed within a short time after mobilisation in the SCR.

If the safety analysis shows that long-term occupation of the SCR may be necessary, means shall be provided to ensure habitability (for example ventilation). Such provisions may not need to meet the same requirements as specified for the MCR.

The human-machine interface in the SCR shall follow the same design rules as that for the MCR, particularly in relation to the human-machine interface design for the monitoring of the key plant parameters, and should comply with the ergonomic principles as presented in ISO 11064.

Where multiple supplementary control points and/or LCP are necessary for an existing plant, clear guidance shall be developed for the use, staffing and co-ordination of activities involving these facilities. In addition, human factors analysis shall be undertaken to demonstrate that the required tasks can be achieved reliably and within the timescale assumed in the safety analysis.

If more than one supplementary control point is necessary for an existing plant, for redundancy and separation alone (for example for two similar plant trains, separated by a principal fire barrier), they should have matching layouts, with clear identification of the plant items concerned, and should not be mirrored (see IEC 60964).

6 Design process

A system approach shall be used for developing the SCR specification. This process should parallel the design process for the MCR and should use similar procedures, criteria and methods. More specifically, the following elements shall be applied to the SCR design (and documentation) objectives and principles.

a) Define the design basis and design extension scenarios, their goals and failure criteria (see 5.2).

b) Develop the plant specific SCR functions consistent with the overall design basis.

c) Assign basic functions to operating staff or I&C systems and allocate them to operating locations.

d) Classify the SCR functions with respect to their importance to safety, and define the corresponding design and qualification requirements.

e) Design the plant specific SCR consistent with the general principles given in Clause 5 of IEC 60964:2009.

f) Conduct a design concept verification (i.e. control room staff, SCR training and procedures) and validation of the entire system (see Clause 8).

g) Finalise the SCR design specification based on the above (see Clause 7).

h) Complete the detailed design and conduct a final verification and validation on plant after completion (see Clause 8).

The process described above should establish the list of systems to be controlled from the SCR, and their configuration, and the list of plant parameters to be monitored from the SCR.

7 Functional design

7.1 General

Because of the low frequency of use and the relatively small number of tasks which need to be performed in the SCR, the design shall aim to achieve a minimum extent of equipment, high reliability of functions and a configuration for easy and quick understanding.

7.2 Human factors

Anthropometric considerations, population stereotypes, intensity of audible signals, visual and viewing angles as well as preference for analogue or digital indications shall be chosen consistently with those for the MCR, and should comply with the ergonomic principles as presented in ISO 11064.

An adequate level of illumination shall be provided to ensure that visibility is sufficient for task performance on a continuous basis without undue fatigue and should comply with the requirements of ISO 11064-6.

The auditory environment shall enable clear verbal communication to be held and should comply with the requirements of ISO 11064-6.

If working areas are provided for use over an extended time, means for adequate seated operation, writing and document reference and document lay down should be provided.

If computer based information or control is used in the SCR, these shall function in a manner closely matching and preferably in an identical way to that of similar controls and indications in the MCR. Reliability and environmental considerations may require different equipment, but corresponding and compatible operating sequences to those in the MCR shall be used.

7.3 Location and access route

The SCR shall be located and the protection shall be designed so that no sequence of events of any PIE can simultaneously affect the functions of both the SCR and the MCR. This should include consideration of events that might affect them either directly or by affecting the service systems that support the SCR and MCR, respectively.

NOTE The practical implementation of the above functional location requirement is for the SCR area to be physically and electrically separated from the MCR area.

Adequate separation of cables of the MCR and SCR shall be achieved as part of functional (physical and electrical) separation. The signalling on cables to/from the field equipment should be sent to/from the SCR, not via the MCR, and vice versus. The ventilation systems shall also be considered as part of the functional separation and independence requirements for the MCR and SCR.

Fire is an important hazard following which use of the SCR may be required, and an assessment of the fire protection of the SCR and the human routes to them should be made and should show accessibility to the SCR location. Similar assessments of all service systems, with special reference to heating, ventilation and air conditioning systems, access routes and cables, should be made for other design basis and design extension conditions for which the SCR is to be used. The assessment of the cable routes should demonstrate independence of the SCR cables from the MCR cables.

It shall be possible to reach the SCR easily, safely and within the time allowed, notwithstanding the need for access control. This shall be possible both from the MCR upon

its evacuation and by routes avoiding the MCR and avoiding any other areas potentially affected by hazards following which use of the SCR is required. Consideration should also be given to the need for protection against radiation along these access routes.

An indication of the potential hazards (e.g. fire) and suitable countermeasures (e.g. breathing equipment) should be provided along the access route from the MCR to the SCR. Before an SCR is to be accessed, it shall be possible for the operating staff to be assured that the environment is safe for their access.

In order to alert all operating staff, particular those who were off site when the MCR was abandoned, it shall be clearly indicated that the MCR is unavailable and shall not be accessed for control purposes until it is available again.

7.4 SCR environment

The environmental conditions in the SCR shall meet the requirements derived from the safety analysis for normal and emergency conditions and shall take into account National rules, including the security plan in the respective country. Except where shown to be unnecessary by analysis, protection against radiation shall be provided for the SCR and its access points. This shall include consideration of access from off-site as well as from the MCR.

For the design basis conditions requiring use of the SCR, the environmental conditions shown by the safety analysis for the intended location of an SCR shall not exceed those for normal unprotected human access. Where an SCR may be required for use in a design extension condition, involving the national security plan, the location should be shown to be suitable for normal human access in those conditions. Notwithstanding this, radiation monitoring shall be provided for the SCR.

A battery powered emergency lighting system shall be continuously available in the SCR even upon failure of the normal lighting system or its power supply. The emergency system should provide sufficient illumination for task performance on the basis of a limited operational period, which should be shown to meet the requirements of the plant emergency plan.

Provisions shall be made for the use of portable batteries, brought from off-site, to restore supplies to the lighting and to any other facilities needed for continued use of the SCR in the event of long-term failure of the normal power supply system.

Power supplies for the equipment in the SCR and the lighting shall be designed in line with the safety class and the scenarios for the use of the SCR. This will typically comprise supply by an emergency uninterruptible power supply.

Depending on the scenarios for the use of the SCR, additional provisions should be made for connection to an external supplementary power supply. This may include the use of portable charging equipment and the running of cables, local supplies of tools that may be needed for connection of the supplementary power supply and assurance of compatibility of connections for this purpose.

The considerations for the supplementary power supply for the control rooms (MCR, SCR) shall be in line with the provisions for the supplementary power supply for the plant equipment (valves, motors, etc.) necessary for station blackout scenarios.

7.5 Space and configuration

The SCR shall have sufficient space for:

- all necessary information and control equipment in a well-structured arrangement;
- writing and laying down documents and procedures;
- storage of documents and procedures;

- communication equipment.

Spare space shall be included for additions and modifications.

The SCR configuration shall enable prompt mobilisation by the operating staff upon their arrival at the SCR. ISO 11064-1 offers guidance on process and ISO 11064-3 offers guidance on room layout principles.

7.6 Information and control equipment

All information, displays, recording and control equipment shall be arranged and structured according to their functions and priority in order to minimise the possibility of human errors and shall operate in the same way as the related MCR interface.

Mimic diagrams may be used to improve the presentation of information.

The presentation of controls, indications and mimic diagrams selected for the SCR shall follow the same layout and design principles as applied for the MCR.

Coding, labelling and grouping principles shall be consistent with those for the MCR.

Displays and controls shall be provided for safety functions as defined in 5.2. These displays and controls shall be provided with a degree of redundancy in accordance with their safety classification and design requirements.

Where for an existing plant a single supplementary control point does not provide the redundancy needed within itself, and that redundancy is not otherwise provided by an alternative supplementary control point, use of a local control point can, for some plant designs, provide the necessary indication or control to mitigate a failure of the supplementary control point functionality. For exceptional conditions, if this is required by the safety arguments, this should be considered as an engineering solution rather than extending the supplementary control point facilities. For such exceptional conditions, accessibility to the LCP and time restraints for access to the LCP shall be shown to be acceptable.

7.7 Communication systems

SCR communication should be provided with station management and the technical support centre, if there is one. There shall be normal internal plant telephone communication and other communication facilities, such as for paging, as required by the plant emergency plan. Assured communication facilities shall be provided between the SCR and local control points. If more than one supplementary control point is necessary for an existing plant, communication between these supplementary control points shall be provided.

Redundant communication equipment using different transmission routes shall be available for operational purposes, management of the shutdown procedures and to communicate with the emergency response centres or their equivalent. Such redundant equipment shall be available for communication between the SCR and/or local control points.

In addition to the above, diverse means shall be provided for communication between the SCR and specific locations as required by the plant emergency plan. These diverse communication means should be:

- designed such that only one communication means may be affected by the same failure, hazard or PIE, and
- capable of operating independently of the on-site and off-site power systems.

The normal plant communication equipment may be used for communication with the MCR for training, testing or other purposes.

7.8 Other equipment

Other equipment which should be either located in the SCR or readily accessible from the SCR includes:

- medical equipment for first aid;
- equipment to be used during local emergency situations, as required by the plant emergency plan;
- documentation on the plant emergency plan;
- portable lighting, radiation detectors and fire fighting equipment;
- protective clothing and breathing air sets.

The plant operating utility should develop operating principles to be followed when the MCR conditions require the use of the SCR, concerning access control, site security and actions in response to fires. If not provided elsewhere, the SCR design shall include any facilities for these functions, such that they can continue during the period that the MCR cannot be used.

7.9 Testing and inspection

Regular testing shall be undertaken of the functions related to use of the SCR. This shall include testing of the following:

a) emergency lighting along the operator transfer routes from the MCR to the SCR and from off-site to the SCR;
b) SCR access control and associated security functions;
c) MCR to SCR control transfer function;
d) SCR manual control for reactor shutdown;
e) SCR manual control for maintenance of a safe state;
f) SCR monitoring functions, including for simulated representative scenarios;
g) SCR communication functions;
h) SCR other service functions (e.g. ventilation, lighting, power supplies (including the emergency installation of portable batteries)).

The frequency of testing shall fully support the assumptions of the safety analysis.

The testing arrangements shall be shown to not adversely affect plant safety or availability.

In addition to the above, routine inspections should be undertaken of the following:

- the absence of obstacles preventing safe transfer along the routes from the MCR to the SCR and from off-site to the SCR;
- the general condition and state of readiness of the SCR and its facilities.

Wherever appropriate, operational staff shall be involved in the testing and inspection activities and their feedback taken into account.

8 System verification and validation

The system verification and validation process for the SCR is closely related to the MCR verification and validation process. The human-machine functional assignment shall be done for the SCR and MCR at the same time.

NOTE IEC 61513 gives general requirements for V&V of I&C systems. This standard only addresses additional V&V requirements specific to the SCR.

Due to the requirement for simplification of tasks and therefore also of information and actions, the V&V of the SCR may be made simpler than that for the MCR. The V&V of the SCR should be planned, with suitable criteria, based on the requirements of IEC 60964 and IEC 61771.

During the final review, it shall be verified that the events which could lead to loss of the MCR safety functions have no effect on the SCR or its functions. During the on-site commissioning tests, the availability and reliability of the SCR shall be verified.

Annex A
(informative)

Assessment of safe transfer time window

It is stated in 5.3.3 that “the design shall allow adequate time for control room staff to reach the SCR after the MCR becomes unavailable”.

This annex addresses the factors that may be considered in order to demonstrate this, which are as follows:

a) assumptions regarding credible ‘loss of MCR’ scenarios – e.g. the cause and form of the ‘loss of MCR’, the impact on the control room staff (i.e. whether or not they are available to transfer to the SCR) and the ambient conditions in the vicinity of the MCR and on the routes to the SCR;

b) assumptions regarding automatic control of plant at the time of MCR to SCR control transfer – e.g. related to automatic protection actions following manual reactor trip prior to evacuation of the MCR, or automatic control of the untripped reactor if no such manual trip was achieved;

c) analysis of the durations of safe transfer time windows for different credible scenarios – i.e. for each scenario, the time for which the analysis shows that no operator action is required for safety;

d) analysis of the time required for safe transfer of staff and SCR mobilisation for different credible scenarios – i.e. the time from the point of evacuation of the MCR until the operating staff have transferred to and mobilised in the SCR, and then fully assessed the plant status (and are thus ready to take any action required);

e) substantiation that the transfer can be accomplished reliably and within the time required – i.e. the results of analyses undertaken of the various steps in item d) above from a hazards, equipment reliability and human factors point of view, with due account being taken of any constraints arising from:

   – staff selection policy;

   – local requirements;

   – national regulations.

Bibliography

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

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

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

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

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

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

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

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

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

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

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

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

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

ISO 9241, *Ergonomics of human-system interaction*

IAEA GS-R-3:2006, *The management system for facilities and activities*

IAEA Safety Guide No, GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA Safety Guide No, GS-G-3.5:2009, *Management system for nuclear installations*

IAEA SSR-2/2, *Safety of Nuclear Power Plants: Commissioning and Operation*

IAEA Safety Guide NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

IAEA Safety Glossary:2007, *Terminology used in nuclear safety and radiation protection*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – SALLE DE COMMANDE SUPPLÉMENTAIRE POUR L'ARRÊT DES RÉACTEURS SANS ACCÈS À LA SALLE DE COMMANDE PRINCIPALE

AVANT-PROPOS

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

La Norme internationale IEC 60965 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et électriques des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette troisième édition annule et remplace la seconde édition publiée en 2009. Cette édition constitue une révision technique.

Les principales modifications techniques par rapport à l'édition précédente sont les suivantes:

a) des exigences portant sur les essais classiques réalisés sur les SCS (salles de commande supplémentaires);
b) des exigences permettant d'évaluer le temps disponible durant lequel le réacteur est en état sûr mais non surveillé, de façon à pouvoir se rendre de la SCP (salle de commande principale) à la SCS et à ce que la SCS devienne opérationnelle;

c) la référence au document SSR-2/1 de l'AIEA qui comprend les nouvelles exigences suivantes:

   1) il convient que la SCS soit fonctionnellement séparée (aussi bien physiquement qu'électriquement) de la SCP,

   2) on doit prendre en compte des mesures pour protéger contre les rayonnements les chemins d'accès à la SCS;

d) la référence au document DS431 de l'AIEA, qui est la révision du document NS-G-1.3, y compris les nouvelles exigences suivantes:

   1) la mise en œuvre d'au moins deux méthodes de communication diversifiées entre un ensemble de lieux prédéterminés,

   2) la mise en œuvre de dispositions en appui de la surveillance des tendances d'évolution des paramètres clé de l'installation;

e) des exigences relatives au rôle, à la capacité fonctionnelle et à la robustesse de la SCS en conditions hors dimensionnement;

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/1060/FDIS	45A/1078/RVD

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

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

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

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

INTRODUCTION

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

La version de 1989 de l'IEC 60965 fut développée pour établir des exigences pertinentes pour la conception de la salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale. Cette première édition de l'IEC 60965 a été largement utilisée par l'industrie nucléaire. Il a été néanmoins reconnu en 2007 qu'il serait souhaitable d'intégrer les développements techniques, particulièrement ceux basés sur le logiciel. Il a été aussi admis que les relations avec la norme portant sur la salle de commande principale (à savoir l'IEC 60964) et les normes filles en dépendant (à savoir l'IEC 61227, l'IEC 61771, l'IEC 61772, l'IEC 61839 et l'IEC 62241) devraient être clarifiées et structurées. La deuxième édition de l'IEC 60965 a été publiée en 2009.

En juin 2013, lors de la réunion de Moscou, les experts du WG A8 ont recommandé de développer une révision limitée pour prendre en compte les leçons tirées de l'accident TEPCO Fukushima Daiichi et certains commentaires formulés lors de la circulation du FDIS pour la publication de la deuxième édition. Au cours du développement de la présente révision, le titre de la norme a été amendé pour faire référence à la 'salle' de commande supplémentaire (SCS) pour des raisons de cohérence avec le document SSR-2/1 de l'AIEA.

La présente norme IEC s'intéresse principalement au processus de conception fonctionnelle de la salle de commande supplémentaire des centrales nucléaires. Il est conçu pour l'usage des concepteurs de centrales nucléaires, les maîtres d'œuvre et d'ouvrage, les constructeurs, les exploitants et les autorités d'accréditation.

b) Position de la présente norme dans la collection de normes du SC 45A de l'IEC

L'IEC 60965 est le document du SC 45A de l'IEC de troisième niveau qui traite de la question de la conception de la salle de commande supplémentaire.

L'IEC 60965 doit être lue avec l'IEC 60964 du SC 45A de l'IEC, portant sur la conception de la salle de commande principale (y compris ses normes filles), qui fournit des recommandations pour les commandes opérateurs, la vérification et la validation de la conception, l'utilisation d'unités d'affichage, l'analyse fonctionnelle et l'affectation des fonctions et les fonctions et présentation des alarmes.

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

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

Le but de cette norme est de fournir des exigences de conception fonctionnelle applicables à la conception de la salle de commande supplémentaire des centrales nucléaires afin de satisfaire aux exigences de sûreté pertinentes.

Cette norme s'applique à la conception de la salle de commande supplémentaire dont la conception débutera après sa publication. Les recommandations de cette norme peuvent être utilisées pour des rénovations, des mises à niveau et des modifications.

Les aspects pour lesquels des recommandations particulières ont été établies dans cette norme, conformément aux normes de sûreté de l'AIEA, sont les suivants:

– définition des bases de conception de la salle de commande principale et de l'installation pour lesquelles la salle de commande supplémentaire doit être utilisée;

– accès du personnel de l'installation à la salle de commande supplémentaire en cas de telles urgences;

– garantie pour le personnel de l'installation que l'environnement d'ambiance de la salle de commande supplémentaire est sûr lorsqu'on doit l'utiliser;

– mise à disposition dans la salle de commande supplémentaire d'information sur l'état des fonctions critiques du réacteur;

– fonctions de basculement et d'indication des commandes de la salle de commande principale vers la salle de commande supplémentaire en cas d'urgence;

– indépendance et séparation du câblage de la salle de commande supplémentaire de celui de la salle de commande principale;

– garantie qu'un état d'arrêt sûr a été atteint en utilisant la salle de commande supplémentaire;

– dispositifs de communication entre la salle de commande supplémentaire et l'équipe de direction de l'installation.

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

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

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

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

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

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

L'IEC 61513 a adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales de l'IEC 61508-1, l'IEC 61508-2 et l'IEC 61508-4 pour le secteur nucléaire, pour ce qui concerne le domaine de la sûreté nucléaire. Dans ce domaine, l'IEC 60880 et l'IEC 62138 correspondent à l'IEC 61508-3 pour le secteur nucléaire. L'IEC 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

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

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – SALLE DE COMMANDE SUPPLÉMENTAIRE POUR L'ARRÊT DES RÉACTEURS SANS ACCÈS À LA SALLE DE COMMANDE PRINCIPALE

1 Domaine d'application

La présente Norme internationale établit des exigences applicables à la salle de commande supplémentaire permettant au personnel d'exploitation des centrales nucléaires d'arrêter le réacteur, si celui-ci était en fonctionnement, et de maintenir l'installation dans un état d'arrêt sûr, pour le cas où les fonctions de sûreté ne pourraient plus être commandées de la salle de commande principale, en cas d'indisponibilité de celle-ci ou de ses équipements. La conception doit garantir que la salle de commande supplémentaire est protégée contre les risques, y compris les risques extrêmes locaux, entraînant l'indisponibilité de la salle de commande principale.

Cette norme fournit aussi des exigences pour le choix des fonctions, la conception et l'organisation de l'interface homme-machine, ainsi que des procédures qui doivent être utilisées systématiquement pour vérifier et valider la conception fonctionnelle de la salle de commande supplémentaire.

On suppose qu'en condition de fonctionnement normal de la centrale, hormis lors de la réalisation d'essais périodiques, aucun personnel n'est présent en salle de commande supplémentaire prévue pour réaliser les opérations d'arrêt à partir de l'extérieur de la salle de commande principale. Les exigences sont conformes aux principes d'ergonomie, tels qu'appliqués à l'interface homme-machine utilisée pour les essais périodiques ou en présence de conditions anormales de fonctionnement de la centrale.

Les installations pour les situations d'urgence, comme le centre de support technique, ou les installations destinées à la manipulation des déchets radioactifs ne font pas partie du domaine d'application de cette norme. La conception détaillée des matériels n'est pas couverte par cette norme.

Cette norme est conforme aux principes établis par les documents AIEA SSR-2/1 et AIEA Guide de sûreté NS-G-1.3.

L'objectif de cette norme est de fournir des exigences de conception fonctionnelle pouvant être utilisées lors de la conception de la salle de commande supplémentaire des centrales nucléaires afin de satisfaire aux exigences de sûreté.

Cette norme est destinée à être appliquée à la salle de commande supplémentaire dont la conception fonctionnelle débutera après la publication de la norme. Si on souhaite appliquer la norme à des centrales ou à des types de conceptions existantes, il faut s'assurer de sa cohérence avec les bases de conception. Ceci correspond, par exemple, à des points particuliers tels que la cohérence de la salle de commande supplémentaire avec la salle de commande principale, l'approche ergonomique, le niveau d'automatisation et la technologie d'information utilisée, et l'étendue des modifications à mettre en œuvre au niveau des systèmes d'I&C.

2 Références normatives

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

dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

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

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

IEC 61771, *Centrales nucléaires de puissance – Salle de commande principale – Vérification et validation de la conception*

IEC 62646, *Centrales nucléaires de puissance – Salles de commande – Procédures informatisées*

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

ISO 11064-1, *Conception ergonomique des centres de commande – Partie 1: Principes pour la conception des centres de commande*

ISO 11064-3, *Conception ergonomique des centres de commande – Partie 3: Agencement de la salle de commande*

ISO 11064-6, *Conception ergonomique des centres de commande – Partie 6: Exigences relatives à l'environnement pour les centres de commande*

AIEA N° SSR-2/1:2012, *Prescriptions de sureté particulières, Sûreté des centrales nucléaires: Conception*

AIEA N° NS-G-1.3:2005, *Guide de sureté, Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires (qui sera remplacé par le SSG-39)*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent. Concernant les autres termes, se référer à la terminologie générale définie dans l'IEC 60964, l'IEC 61513 et dans les documents relevant du programme NUSS de l'AIEA, tels que le Guide de sûreté NS-G-1.3 ou le glossaire de sûreté.

3.1
équipe de salle de commande
personnel présent en salle de commande, responsable de l'atteinte des objectifs opérationnels de la centrale, en conduisant celle-ci au moyen des interfaces homme-machine. L'équipe de salle de commande comprend en général, des opérateurs supervisant et des opérateurs manipulant effectivement les commandes; elle peut inclure le personnel d'exploitation et les experts autorisés à être présents en salle de commande, par exemple durant de longues séquences d'évènements

[SOURCE: IEC 60964:2009, 3.4]

3.2
conditions hors dimensionnement
conditions accidentelles hypothétiques qui ne sont pas prises en compte dans les accidents de dimensionnement mais qui le sont dans le processus de conception de l'installation conformément aux méthodes de type «meilleure estimation», et dans lesquelles les rejets de matières radioactives sont maintenus dans des limites acceptables. Les conditions hors dimensionnement comprennent les conditions correspondant aux évènements sans dégradation significative du combustible et les conditions avec fusion du cœur

[SOURCE: AIEA SSR-2/1:2012, révisé par DS462]

3.3
points de commande locaux
installations de commande locales
points (ou installations) situés à l'extérieur de la salle de commande où des opérateurs locaux réalisent des activités de commande

[SOURCE: IEC 60964:2009, 3.17]

3.4
opérateur local
membre de l'équipe de conduite qui remplit des tâches à l'extérieur de la salle de commande

[SOURCE: IEC 60964:2009, 3.18]

3.5
équipe de conduite
personnel de la centrale travaillant en poste pour conduire la centrale. L'équipe de conduite comprend l'équipe de la salle de commande, les techniciens de maintenance, etc.

[SOURCE: IEC 60964:2009, 3.20]

3.6
salle de commande supplémentaire
emplacement à partir duquel la commande limitée de la centrale et/ou sa surveillance peuvent être assurées pour réaliser les fonctions de sûreté identifiées dans l'analyse de sûreté, comme prescrit en cas de perte de la possibilité de réaliser ces fonctions à partir de la salle de commande principale

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

4 Abréviations

PI	Procédures informatisées
I&C	Instrumentation et Contrôle-commande
PCL	Point de Commande Local
SCP	Salle de Commande Principale
CNP	Centrale Nucléaire de Puissance
EIH	Evènement Initiateur Hypothétique
SCS	Salle de Commande Supplémentaire
V&V	Vérification et Validation

5 Principes de conception

5.1 Généralités

La prescription 66 de l'AIEA SSR-2/1 établit que: «Des instruments de contrôle-commande sont disponibles, de préférence en un point unique (salle de commande supplémentaire) indépendant de la salle de commande de la centrale nucléaire du point de vue physique, électrique et fonctionnel. La salle de commande supplémentaire est équipée de telle manière qu'elle permet de mettre et de maintenir le réacteur à l'arrêt, d'évacuer la chaleur résiduelle et de surveiller les variables essentielles de la centrale au cas où il ne serait plus possible d'assurer ces fonctions de sûreté essentielles dans la salle de commande.»

NOTE 1 La référence à la «salle de commande» est interprétée dans la présente norme comme la «salle de commande principale (SCP)».

NOTE 2 La séparation fonctionnelle signifie que la fonction de la SCS peut être assurée malgré les disfonctionnements prévus en SCP.

NOTE 3 La séparation fonctionnelle complète des liaisons menant de l'interface homme machine des points de commande jusqu'aux appareils terminaux peut être difficile à satisfaire pour toutes les fonctions d'I&C, en particulier par exemple pour les actionneurs partagés équipés d'un contrôleur logique de priorité pour faire la différence entre les commandes de la SCP et de la SCS. De tels matériels communs sont acceptables s'il existe une redondance, des moyens de secours ou des matériels sur le terrain appropriés qui permettent de réaliser la fonction d'actionnement nécessaire et qu'ils sont suffisamment isolés des risques communs existants pour minimiser le risque que la fonction soit complètement inopérante.

Les paragraphes de 6.15 à 6.30 du document NS-G-1.3 de l'AIEA fournissent des exigences pertinentes pour les salles de commande supplémentaires ("SCS" dans cette norme), ceci comprenant des exigences applicables pour les points suivants:

- définition des bases de conception de la centrale qui exigent l'utilisation de SCS (6.17, 6.19, 6.20);
- emplacement et configuration de la SCS favorisant une mobilisation rapide (6.29);
- chemin d'accès à la SCS qualifié, avec signalisation des risques et mesures de protection adaptées le long de ce chemin (6.27, 6.28);
- protection contre les accès et les utilisations non autorisés de la SCS (6.21);
- fonctions de sûreté de la SCP et de la SCS qui ne soient pas impactées par les mêmes EIH, et indépendance des circuits associés à la SCS et à la SCP (6.20, 6.23);
- commandes prioritaires entre la SCP et la SCS et transfert de la SCP à la SCS (6.18, 6.20, 6.24);
- commandes manuelles réalisées à la SCS par des actions simples (6.22);
- affichage et commandes à la SCS similaires à ceux de la SCP, autant que possible (6.22);
- prise en compte de la différence des objectifs assignés à la SCP et à la SCS (6.25);
- si une utilisation longue durée est envisagée, adaptation de l'installation au niveau habitabilité et espace de travail en fonction des tâches à réaliser (6.30).

5.2 Objectifs principaux

Les exigences de l'AIEA portant sur la conception de la SCS fournies dans le premier alinéa de 5.1, doivent être satisfaites comme détaillées dans la présente norme.

La SCS doit être pourvue de moyens pour déclencher l'arrêt du réacteur et mettre la centrale en état sûr et la maintenir dans cet état sans avoir à accéder à la SCP. Cependant, il n'est pas demandé que la SCS permette de réaliser toutes les autres fonctions commande et de surveillance qui sont traditionnellement assurées en SCP. Suivant le type de CNP et les arguments de sûreté détaillés, il convient de pouvoir intégrer en SCS des moyens permettant de faire face à un ensemble prédéfini d'EIH.

La SCS est requise lorsque la capacité de réaliser les fonctions de sûreté à partir de la SCP est perdue. Les causes possibles d'une telle situation comprennent l'incendie en SCP, des entrées importantes de fumée ou une atmosphère ambiante de la SCP dangereuse, des dégâts importants au niveau de la SCP ou de son câblage tels que les fonctions de sûreté ne puissent plus être assurées, des dégâts majeurs dans la zone de la salle de commande ou sur les équipements de la salle de commande.

Les EIH de dimensionnement et les séquences évènementielles pour lesquels l'usage de la SCS est nécessaire, doivent être identifiés. Ceci doit comprendre l'identification et la justification des conditions dont l'apparition est prévue et de leurs durées correspondantes pour laquelle la SCS peut être nécessaire.

Comme la fréquence des évènements entraînant l'indisponibilité de la SCP est très faible, on admet que l'analyse de sûreté de la centrale puisse démontrer que de tels évènements ne puissent coïncider avec d'autres évènements indépendants dans la centrale qu'à une fréquence faible acceptable, en particulier il est admis que le circuit de réfrigérant primaire est intact. Cependant on doit prendre en compte l'occurrence possible de n'importe quelle défaillance dans la centrale qui peut résulter d'un déclenchement du réacteur et de défaillances liées à la centrale à l'arrêt auxquelles sont associées des fréquences suffisamment significatives pour coïncider avec l'utilisation de la SCS. En particulier, la conception de la SCS doit prendre en compte une indisponibilité long terme de la SCP due à un incendie ou à d'autres raisons.

Les critères pour l'utilisation de la SCS doivent être clairement définis dans les procédures de conduite de la centrale.

On doit pouvoir déterminer l'état de sûreté d'ensemble de la centrale de l'extérieur de la SCP. De préférence, il convient que ce soit possible à partir de la SCS. Il convient donc que la SCS permette de surveiller de façon pertinente l'état des systèmes de la tranche et de ses paramètres clé. Il convient que toute information présentée soit conforme aux principes ergonomiques établis par les parties pertinentes de l'ISO 11064.

Pour une surveillance efficace et une analyse ultérieure des évènements, il convient d'enregistrer les paramètres clé de la tranche pour permettre l'affichage des tendances de leur évolution et pour leur utilisation ultérieure dans le cadre d'analyses différées. Il est recommandé de les enregistrer automatiquement. S'il est prévu que la SCP et la SCS ne soient pas occupées par du personnel pour des périodes de temps importantes, un enregistrement automatique doit être mis en œuvre.

Du point de vue de l'exploitation (par exemple pour simplifier le fonctionnement et éviter les incompréhensions), il est préférable d'avoir seulement une SCS. On doit faire attention, néanmoins, à la satisfaction des exigences de sûreté et en particulier aux exigences de redondance et d'indépendance. Si deux ou plus de deux points de commande sont disponibles sur une installation existante, il convient que chaque point de commande supplémentaire affiche toutes les informations nécessaires pour la réalisation des tâches opérateur.

Il convient que les affichages informatisés de la SCS fournissent les mêmes fonctionnalités pour les informations importantes pour la sûreté que celles offertes par les affichages correspondant en SCP. Il convient que le contenu des affichages pour un état de tranche donné et pour une tâche opérateur donnée soit le même qu'en SCP.

On doit avoir suffisamment de temps pour atteindre la SCS avant que de devoir y lancer des actions, de même que l'on doit y avoir suffisamment de matériel pour assurer les communications nécessaires entre les personnels de conduite concernés par ces actions ainsi qu'avec l'intérieur et l'extérieur du site. Des exigences portant sur les communications sont fournies en 7.7.

La disposition de l'instrumentation et les modes de présentation dans la SCS doivent assurer à l'équipe de conduite la présentation de l'information nécessaire pour pouvoir évaluer l'état de la centrale et diriger les opérations d'arrêt (et le maintien en l'état qui s'ensuit) du réacteur, du refroidissement long terme du cœur du réacteur et du confinement des matières radioactives.

Les systèmes de tranche qui peuvent être commandés à partir de la SCS peuvent être limités à ceux assurant des fonctions de sûreté.

La SCS doit offrir des moyens de commande suffisant liés aux fonctions de sûreté pour atteindre et se maintenir en état sûr, pour l'ensemble prédéfini des EIH et des conditions pour lesquels la SCP ne peut pas être utilisée. Le domaine de commande et de surveillance de la SCS doit couvrir l'état des fonctions de sûreté concernées ainsi que les commandes pour les lancer et les arrêter, en plus de l'état des fonctions de sûreté fondamentales associées (voir le document AIEA SSR-2/1:2012, prescription n° 4).

Les équipements pour la surveillance de la sécurité du site, des contrôles d'accès à la centrale et d'alarme incendie qui se trouvent normalement en SCP doivent aussi être implantés dans une zone indépendante. Cette zone indépendante peut être une SCS ou une zone non impactée par l'évènement qui a entraîné l'utilisation de la SCS. Dans ce dernier cas, ces zones de l'installation doivent présenter une capacité à la résistance aux risques équivalente à celle de la SCS.

La conception de la SCS doit être cohérente avec la conception de la SCP. Le processus d'identification et de conception des commandes et indications pertinentes nécessaires dans la SCS doit être conforme aux exigences de l'IEC 60964, telles que résumées à l'Article 6 de cette norme.

5.3 Principes de sûreté

5.3.1 Conditions de dimensionnement et hors dimensionnement

Le dimensionnement de base de la centrale indique normalement les risques internes et externes qui doivent être pris en compte. La conception doit garantir que de tels évènements ne sont pas susceptibles de rendre inutilisables ou inefficaces simultanément les fonctions de la SCS et de la SCP (et des points de commande locaux), nécessaires pour assurer l'arrêt sûr, la surveillance garantissant l'arrêt sûr et les commandes des fonctions critiques.

Si le dimensionnement de base est étendu pour couvrir des risques extrêmes ou des combinaisons de défaillance de faible probabilité, il convient que la conception garantisse que la SCP et la SCS ne soient pas défaillantes ensemble en de telles circonstances. La mise en œuvre du transfert des commandes vers la SCS doit prendre en compte les contraintes pratiques issues des hypothèses faites au niveau des conditions de dimensionnement et hors dimensionnement pour l'utilisation de la SCS.

L'exigence indiquée ci-dessus concernant la non-sensibilité de la SCP et de la SCS aux mêmes conditions de dimensionnement et hors dimensionnement doit être étendue à leur fonctions, systèmes et matériels supports.

5.3.2 Fonctionnalité et qualification

Les fonctions de la SCS doivent être classées conformément à l'IEC 61226, en tenant compte des critères concernant l'utilisation de la SCS décrits en 5.2.

Les équipements et systèmes doivent être conçus avec un degré de redondance conforme à leur classement de sûreté. On doit aussi prendre en compte le besoin d'isolement fonctionnel et de séparation physique, lorsque des systèmes classés de sûreté et non classés de sûreté ainsi que des systèmes redondants sont proches (voir l'IEC 60709).

Les équipements de la SCS doivent être adaptés aux conditions environnementales applicables pour leur utilisation prévue. Les équipements doivent être qualifiés pour les EIH de dimensionnement et pour les séquences évènementielles pertinentes par rapport à leur classement de sûreté. Des essais ou des analyses complémentaires peuvent être nécessaires pour avoir l'assurance que la fiabilité et la robustesse atteintes sont appropriées pour résister aux contraintes correspondant aux conditions hors dimensionnement.

5.3.3 Accessibilité et temps de transfert opérateur

Prenant en compte les causes d'indisponibilité prévues des fonctions de la SCP, les fonctions de la SCS doivent être conçues (et si nécessaire, la SCS doit être située) pour que, même en situation d'urgence, la SCS soit accessible par des chemins sûrs. Voir 7.3 pour plus de détails.

La conception doit s'assurer que le personnel de la salle de commande a le temps nécessaire pour atteindre la SCS après que la SCP soit devenue indisponible. Il convient de monter que les actions et durées associées au fonctionnement en automatique sans assistance des fonctions de sûreté, après lancement en SCP, de façon à maintenir la sûreté de la tranche jusqu'au moment où les SCS sont opérationnels, sont compatibles avec ce basculement. Ceci doit prendre en compte le temps pour accéder aux commandes et le temps pour évaluer l'état de la centrale à partir de la SCS. L'Annexe A traite des aspects à prendre en compte pour évaluer théoriquement une durée de la fenêtre de temps transfert sûre.

5.3.4 Transfert des commandes, priorités et sécurité des commandes

Les dispositifs d'inhibition des commandes de la SCP et de basculement des commandes vers la SCS doivent être prévus. Ces dispositifs doivent être classés suivant la catégorie la plus élevée des fonctions de sûreté dont les commandes peuvent être inhibées à partir de la SCP. Il doit être prouvé qu'ils sont très fiables, et si nécessaire qu'ils satisfont au critère de défaillance unique. On doit analyser et prendre en compte des défaillances possibles au niveau sécurité de la SCS et l'influence des défauts cybersécurité au niveau de la SCS sur la sécurité de l'I&C.

NOTE Ce qui précède exclut toute exigence permettant de désactiver la fonction arrêt manuel du réacteur à partir de la SCP.

Les dispositifs de transfert de commandes doivent inhiber les commandes de la SCP en garantissant qu'un incendie ou que des dégâts affectant la SCP ne déclenchent pas d'actions de commande intempestives. Les dispositifs doivent aussi être conçus pour éviter ou pour minimiser les transitoires des variables commandées lors du basculement des commandes, dans les deux sens, de la SCP vers la SCS et de la SCS vers la SCP.

Les dispositifs de transfert de commande peuvent être situés sur le trajet entre la SCP et la SCS, ou dans la SCS, ou dans la SCP elle-même si l'analyse montre que cela ne peut entraîner de défaillance au niveau de la réalisation du transfert des commandes ou au niveau des commandes à partir de la SCS. Lorsque les dispositifs sont situés en SCP, il convient de mettre à disposition des moyens supplémentaires indépendants de la SCP.

Il convient que la SCS comprenne un moyen d'identification de l'état des commandes de la SCS et des commandes de la SCP (à savoir si elles sont «actives» ou «inactives»).

Les systèmes d'I&C doivent être conçus à fin d'interdire que la SCP et la SCS puissent prendre simultanément la commande des systèmes de tranche.

Les systèmes d'I&C doivent être conçus pour que la probabilité d'occurrence de faux signaux émis par des composants de la SCP liés à des systèmes ayant un impact sur la sûreté de l'installation, soit faible et acceptable. Les systèmes d'I&C doivent être conçus pour que la probabilité d'occurrence de faux signaux émis par des composants de la SCS liés à des systèmes pouvant interférer avec la conduite et la surveillance de l'installation en SCP, en conditions normales et anormales, soit faible et acceptable. Les commutateurs de

basculement, les signaux codés, les relais d'isolement optiques sont des exemples de techniques de conception qui permettent d'atteindre ces objectifs.

Un disfonctionnement d'un équipement commandant le transfert des commandes de la SCP vers la SCS pourrait entraîner un isolement de la SCP. Ainsi, les modes de défaillance des équipements permettant la mise en œuvre de la fonction de transfert des commandes doivent être analysés et on doit montrer qu'ils sont acceptables. Cette analyse doit prendre en compte tous les EIH pour lesquels il est prévu d'opérer à partir de la SCP.

Lorsqu'une SCS est utilisée, les actions initiées à partir de celle-ci doivent avoir priorité sur toutes autres actions de commande manuelles, sauf si la commande doit être réalisée à partir d'un point de commande local.

La conception de la SCS doit prévoir des dispositions empêchant les accès ou les utilisations non autorisés. Les moyens de basculement des commandes doivent aussi prévoir des dispositions empêchant le basculement non autorisé de la SCP vers la SCS et vice versa. L'accès à la SCS ainsi que toute tentative de basculement des commandes aux SCS doivent être signalés en SCP au moyen d'alarmes.

Lorsque une SCS n'est pas occupée par du personnel en exploitation normale, on doit vérifier régulièrement la SCS pour s'assurer que le niveau de sécurité prévu est satisfait.

Toutes les procédures utilisées dans le cadre de la modification des logiciels de la SCP doivent aussi s'appliquer pour les modifications de logiciels de la SCS.

5.3.5 Considérations opérationnelles

La SCS doivent être conçus afin de minimiser les erreurs opérateur.

La conception doit prévoir que des instructions écrites soient disponibles dans la SCS pour l'exploitation:

- des systèmes de tranche et des équipements de commande,
- des systèmes d'information et d'enregistrement,
- des dispositifs de communication,
- et de tout autre matériel devant être commandé de la SCS.

Les procédures de conduite correspondant aux actions devant être initiées à partir de la SCS (par exemple refroidissement de l'installation) doivent être simples et claires. Elles doivent s'appuyer sur les principes et le mode d'affichage des procédures de conduite, et elles ne doivent s'en écarter que lorsque des différences s'imposent du fait des installations de conduite locales ou du fait des moyens et des systèmes de conduite disponibles. Il convient de fournir une formation supplémentaire quand une procédure de conduite de la SCS s'écarte de la procédure de conduite équivalente de la SCP.

Même si des procédures informatisées (PI) sont mises en œuvre au niveau de la SCS, les procédures papier doivent y être disponibles. Ceci permet de compenser la défaillance des équipements relatifs aux PI et de gérer plus facilement les combinaisons des activités en SCS et aux points de commande locaux. Concernant les recommandations portant sur la conception des PI voir l'IEC 62646.

Le concepteur doit spécifier les essais réguliers ainsi que les revues d'inspection à effectuer sur les matériels de la SCS nécessaires à l'application des principes de conception et de sûreté. Des exigences portant sur les essais classiques et les inspections sont fournis en 7.9.

La conception doit permettre la formation et un entraînement régulier à l'utilisation de la SCS sans affecter la disponibilité de l'installation.

5.4 Principes d'ingénierie des facteurs humains

Pour réaliser la meilleure répartition des fonctions garantissant la meilleure utilisation des capacités de l'opérateur et du système et pour assurer la sûreté maximale de la centrale, la conception doit porter une attention particulière aux principes d'ingénierie des facteurs humains et aux caractéristiques humaines du personnel dans les conditions d'urgence, particulièrement pour les actions rapides, c'est-à-dire pour les actions devant être réalisées dans un laps de temps réduit après activation opérationnelle de la SCS.

Lorsque l'analyse de sûreté indique qu'il peut être nécessaire d'occuper à long terme la SCS, des mesures doivent être prises pour assurer de bonnes conditions de confort (par exemple la ventilation). Ces mesures ne sont pas nécessairement conformes aux exigences applicables à la SCP.

L'interface homme-machine de la SCS doit suivre les règles de conception de la SCP, en particulier pour ce qui concerne la conception de l'interface homme-machine permettant de surveiller les paramètres clé de l'installation, et il convient de satisfaire aux principes ergonomiques tels que présentés par l'ISO 11064.

Sur une installation existante, en cas de nécessité d'utilisation de plusieurs points de commandes supplémentaires et/ou PCL, des recommandations claires doivent être fournies sur l'utilisation, le personnel et la coordination des activités relatifs à ces installations. De plus, une analyse des facteurs humains doit être réalisée pour montrer que les tâches nécessaires peuvent être réalisées de façon fiable et dans le laps de temps indiqué dans l'analyse de sûreté.

Si, uniquement pour des raisons de redondance et de séparation (par exemple pour deux trains identiques de l'installation séparés par une barrière incendie principale), plusieurs points de commandes supplémentaires sont nécessaires sur une installation existante, il convient que ceux-ci respectent un modèle de présentation, permettant de clairement identifier les éléments de l'installation concernés, et il convient que cela ne soit pas une simple présentation miroir (voir l'IEC 60964).

6 Processus de conception

Une approche système doit être utilisée pour spécifier la SCS. Il convient que ce processus se déroule parallèlement à celui de conception de la SCP et qu'il utilise des procédures, des critères et des méthodes similaires. Plus particulièrement, les éléments suivant doivent être pris en compte au niveau des principes et des objectifs de conception (et dans la documentation) de la SCS.

a) Définition des hypothèses de conception de dimensionnement et hors dimensionnement, de leurs buts et des critères de défaillance (voir 5.2).

b) Développement des fonctions spécifiques de la SCS pour la centrale, compatibles avec le dimensionnement d'ensemble.

c) Attribution de fonctions de base à l'équipe de conduite ou aux systèmes d'I&C et affectation de ces fonctions à des emplacements d'exploitation.

d) Classement des fonctions de la SCS suivant leur importance par rapport à la sûreté et définition des exigences de conception et de qualification correspondantes.

e) Conception des SCS spécifiques à l'installation conforme aux principes généraux indiqués à l'Article 5 de l'IEC 60964:2009.

f) Vérification d'une «théorie de conception» (c'est-à-dire équipe de conduite, SCS, entraînement et procédures) et validation du «système» complet (voir Article 8).

g) Finalisation des spécifications de conception des SCS fondée sur ce qui précède (voir Article 7).

h) Finalisation de la conception de détail et réalisation d'une vérification et d'une validation finales sur l'installation en final (voir Article 8).

Il convient que le processus décrit ci-dessus dresse la liste des systèmes qui doivent être commandés à partir de la SCS, ainsi que leurs configurations, et la liste des paramètres de l'installation devant être surveillés à partir de la SCS.

7 Conception fonctionnelle

7.1 Généralités

Du fait de la faible fréquence d'utilisation de la SCS et du petit nombre de tâches qui y sont accomplies, la conception doit viser à la réduction du matériel, à une haute fiabilité des fonctions et à une configuration facilitant une compréhension aisée et rapide.

7.2 Facteurs humains

Les choix concernant les considérations anthropométriques, les stéréotypes de population, l'intensité des signaux sonores, les angles visuels et de visualisation, de même que les choix d'indications analogiques ou numériques doivent être cohérents avec ceux faits pour la SCP, et il convient qu'ils soient conformes aux principes ergonomiques tels que présentés dans l'ISO 11064.

Un niveau d'éclairage suffisant doit être assuré pour garantir une visibilité suffisante pour réaliser les tâches de façon continue sans une fatigue inutile, et il convient qu'il satisfasse aux exigences de l'ISO 11064-6.

L'ambiance sonore doit permettre de communiquer verbalement facilement, et il convient qu'elle satisfasse aux exigences de l'ISO 11064-6.

Si les zones de travail sont prévues pour un usage en continu, il convient de prévoir de bonnes conditions de travail en position assise, permettant d'écrire et de disposer des documents.

Si des moyens numériques d'information et de commande sont utilisés en SCS, ceux-ci doivent fonctionner d'une façon proche ou de façon identique aux moyens d'information ou de commande équivalents de la SCP. Des considérations liées à l'environnement ou à la fiabilité peuvent nécessiter l'utilisation de matériels différents, néanmoins on doit suivre des séquences de fonctionnement cohérentes avec celles correspondantes de la SCP.

7.3 Emplacement et chemin d'accès

Le choix de l'emplacement de la SCS et la conception de la protection doivent être effectués de façon à ce qu'aucune séquence évènementielle d'aucun EIH ne puisse simultanément affecter les fonctions des SCS et de la SCP. Il convient pour cela de prendre en compte les événements qui peuvent les affecter directement ou affecter les systèmes support des SCS et de la SCP, respectivement.

NOTE La mise en œuvre pratique des exigences de situation fonctionnelle précédentes revient à séparer physiquement et électriquement les emplacements de la SCS et de la SCP.

On doit séparer de façon appropriée les câbles de la SCP et de la SCS dans le cadre de la séparation fonctionnelle (physique et électrique). Il convient que les signaux véhiculés par les câbles de ou vers les équipements présents sur le terrain soient envoyés de ou vers la SCS, et non pas par la SCP, et vice versa. Les systèmes de ventilation doivent être aussi considérés au niveau des exigences portant sur la séparation fonctionnelle et l'indépendance de la SCP et de la SCS.

L'incendie est un risque important à la suite duquel l'utilisation de la SCS peut être nécessaire et il convient de réaliser une évaluation de la protection incendie de la SCS et de ses chemins d'accès pour le personnel et il convient de montrer que l'emplacement de la SCS est accessible. Il convient de faire des évaluations comparables de tous les systèmes de service, en particulier des systèmes de chauffage, de ventilation, d'air conditionné, des chemins d'accès et de câbles, pour les autres conditions de dimensionnement pour lesquelles la SCS doit être utilisée. Il convient que la revue des chemins de câblage montre l'indépendance entre les câbles de la SCS et ceux de la SCP.

On doit pouvoir accéder à la SCS facilement en toute sécurité et dans le laps de temps imparti, malgré le contrôle d'accès. Ceci doit être possible de la SCP, lors de son évacuation et par des chemins en évitant la SCP et toutes zones potentiellement affectées par des risques à la suite desquels l'utilisation de la SCS est nécessaire. Il convient de considérer le besoin de protection contre les rayonnements le long de ces chemins d'accès.

Il convient de fournir, sur le chemin d'accès reliant la SCP à la SCS, une indication des risques potentiels (par exemple l'incendie) et des moyens de lutte appropriés (par exemple des équipements respiratoires). Avant d'accéder à une SCS, il doit être possible pour l'équipe de conduite de s'assurer que l'environnement est sûr pour ce qui concerne l'accès.

Pour alerter l'ensemble de l'équipe de conduite, en particulier les personnels qui se trouvent hors-site lors de l'évacuation de la SCP, on doit clairement signaler que la SCP est indisponible et qu'on ne doit pas y accéder pour raisons de conduite jusqu'à ce qu'elle soit à nouveau disponible.

7.4 Environnement de la SCS

Les conditions d'environnement de la SCS doivent satisfaire aux exigences issues de l'analyse de sûreté pour les situations normales et les situations d'urgence et tenir compte des règles nationales, y compris les plans de sécurité en vigueur dans les pays respectifs. Sauf s'il est montré par analyse que cela n'est pas nécessaire, on doit assurer la protection contre les rayonnements pour la SCS et ses accès. Ceci doit considérer l'accès à partir de l'extérieur du site, comme celui à partir de la SCP.

Pour les situations de dimensionnement exigeant l'utilisation de la SCS, les conditions d'ambiance indiquées par l'analyse de sûreté pour l'emplacement prévu de la SCS ne doivent pas excéder les conditions permettant l'accès normal au personnel non protégé. Lorsque l'utilisation d'une SCS peut être nécessaire durant un accident de dimensionnement ou pour des conditions hors dimensionnement, mettant en œuvre le plan de sécurité national, il convient de montrer que l'emplacement est normalement accessible au personnel dans ces conditions. Malgré cela, la surveillance des rayonnements doit être assurée pour la SCS.

Un système d'éclairage d'urgence sur batterie doit être disponible en continu dans la SCS, même sur défaillance du système d'éclairage normal ou de son alimentation de secours. Il convient que le système d'urgence fournisse un éclairage suffisant pour la réalisation de tâches sur la base d'un temps de conduite limité, dont il convient de montrer qu'il satisfait aux exigences du plan d'urgence de l'installation.

Des dispositions doivent être prises pour pouvoir utiliser des batteries portables approvisionnées par l'extérieur du site, pour rétablir les alimentations de l'éclairage et des autres dispositifs nécessaires pour continuer d'utiliser la SCS dans le cas d'une défaillance long terme du système d'alimentation électrique normal.

Les alimentations électriques des équipements de la SCS et de l'éclairage doivent être conçues conformément à la classe de sûreté et aux scénarios pertinents par rapport à l'utilisation de la SCS. Cela comprend généralement une alimentation ininterruptible.

Suivant les scénarios retenus pour l'utilisation de la SCS, il convient de prendre des dispositions supplémentaires pour un branchement à une source d'alimentation électrique

complémentaire externe. Ceci peut couvrir l'utilisation des chargeurs portables, des câbles opérationnels, des alimentations locales destinée à l'outillage qui peuvent être nécessaires pour brancher l'alimentation complémentaire et d'assurer pour cela la compatibilité des branchements.

Les considérations portant sur l'alimentation électrique complémentaire des salles de commande (SCP, SCS) doivent être cohérentes avec les dispositions portant sur les alimentations électriques complémentaires des équipements de tranche (vannes, moteurs, etc.) nécessaires lors des scénarios de perte totale des alimentations électriques courant alternatif.

7.5 Espace et disposition

La SCS doit être suffisamment spacieuse pour:

- disposer de manière rationnelle le matériel nécessaire d'information et de commande;
- pouvoir prendre des notes et ouvrir les documents et les procédures;
- ranger la documentation et les procédures;
- disposer de matériels de communication.

De l'espace supplémentaire doit être prévu pour des rajouts et des modifications.

La configuration de la SCS doit faciliter son occupation rapide par l'équipe de conduite lors de son arrivée à la SCS. L'ISO 11064-1 présente des recommandations portant sur le processus et l'ISO 11064-3 fournit des recommandations sur les principes de disposition en salle.

7.6 Matériel d'information et de commande

Tous les affichages d'information, les enregistreurs et les commandes doivent être disposés et structurés selon leurs fonctions et priorités respectives dans le but de réduire la possibilité d'erreur humaine et doivent fonctionner de la même façon que l'interface correspondant en SCP.

Les synoptiques peuvent être utilisés pour améliorer la présentation des informations.

La présentation des commandes, des indications et des synoptiques choisie pour la SCS doit suivre les mêmes principes de disposition et de conception que ceux appliqués pour la SCP.

Les principes régissant le codage, l'étiquetage et le regroupement doivent être cohérents avec ceux employés en SCP.

Des affichages et des commandes doivent être fournis au titre des fonctions de sûreté conformément à 5.2. On doit fournir ces affichages et ces commandes avec un niveau de redondance conforme à leur classement de sûreté et à leurs exigences de conception.

Pour une installation existante, lorsque un point de commande supplémentaire singulier ne présente pas, en lui-même, des caractères de redondance suffisants, et que cette redondance n'est pas assurée par un autre point de commande supplémentaire, l'utilisation d'un PCL peut, dans le cas de certaines conceptions d'installation, fournir les indications ou les commandes nécessaires pour compenser la défaillance de fonctionnalité du point de commande supplémentaire. Dans des conditions exceptionnelles, si cela est justifié sur la base d'arguments de sûreté, on peut considérer cette solution technique plutôt que de renforcer les moyens du point de commande supplémentaire. Dans ces conditions exceptionnelles on doit montrer que l'accessibilité et les contraintes de temps associées à l'accès aux PCL sont acceptables.

7.7 Systèmes de communication

Il convient que la SCS soit en communication avec le centre de décision et le centre de support technique, le cas échéant. On doit avoir un système de téléphonie interne sur l'installation pour le fonctionnement normal, ainsi que d'autres systèmes de communication, tel que des pageurs, comme exigé plant d'urgence de la centrale. Des moyens garantissant la communication entre la SCS et les PCL doivent être mis à disposition. Si pour une installation existante, plusieurs points de commandes supplémentaires sont nécessaires, la communication entre points de commandes supplémentaires doit être assurée.

Des matériels redondants utilisant des voies de transmission différentes doivent être disponibles à des fins opérationnelles, pour gérer les procédures d'arrêt et pour communiquer avec les installations pour les situations d'urgence ou leur équivalent. De tels matériels redondants doivent être disponibles pour communiquer entre la SCS et/ou les PCL.

En plus de cela, des moyens diversifiés doivent être fournis pour communiquer en la SCS et les zones particulières tels que requis dans le plan d'urgence de l'installation. Il convient que ces moyens de communication diversifiés soient:

- conçus de telle façon que seulement un moyen de communication soit impacté par une même défaillance, un même risque ou un même EIH, et
- capables de fonctionner indépendamment sur les systèmes d'alimentation du site ou extérieurs au site.

Les moyens de communication utilisés en fonctionnement normal sur l'installation peuvent être utilisés pour la communication avec la SCP durant la formation, en essais ou pour d'autres situations.

7.8 Autres matériels

Il convient que les autres matériels suivants soient ou placés dans la SCS ou facilement accessibles à partir de la SCS:

- matériel médical de première urgence;
- matériel à utiliser en situation locale d'urgence, telle que définie par le plan d'urgence de l'installation;
- documentation relative au plan d'urgence de l'installation;
- lampes portatives, détecteurs de rayonnements et matériel de lutte incendie;
- vêtement de protection et appareils respiratoires.

Il convient que l'exploitant de l'installation développe des principes de conduite à suivre lorsque les conditions en SCP requièrent l'utilisation de la SCS, pour ce qui est du contrôle d'accès, de la sécurité site et des actions de lutte incendie. Si cela n'est pas assuré par ailleurs, la conception de la SCS doit couvrir tous les moyens liés à ces fonctions, tels qu'elles soient assurées durant l'indisponibilité de la SCP.

7.9 Essais et inspections

Des essais classiques doivent être réalisés sur les fonctions associées à l'utilisation de la SCS. Ces essais doivent couvrir les points suivants:

a) éclairage d'urgence le long du chemin d'accès des opérateurs de la SCP à la SCS et de l'extérieur du site à la SCS;

b) contrôle d'accès à la SCS et fonctions de sécurité associées;

c) fonction de commande du transfert de la SCP à la SCS;

d) commande manuelle d'arrêt du réacteur à partir de la SCS;

e) commandes manuelles de maintien en état sûr du réacteur à partir de la SCS;

f) fonctions de surveillance à partir de la SCS, y compris pour des scénarios représentatifs simulés;

g) fonctions de communication à partir de la SCS;

h) autres fonctions de service à partir de la SCS (par exemple ventilation, éclairage, alimentation électriques (y compris installation d'urgence de batteries portables)).

La fréquence de réalisation des essais doit être en complète adéquation avec les hypothèses de l'analyse de sûreté.

Il doit être démontré que les dispositions prises pour les essais ne portent pas atteinte à la sûreté ou à la disponibilité de la tranche.

En plus de cela, il convient de mener des inspections de routine sur les points suivants:

- absence d'obstacle empêchant un transfert sûr par les chemins d'accès de la SCP vers la SCS et de l'extérieur du site vers la SCS,
- état général et de préparation de la SCS et des ses installations.

Lorsque cela est approprié, le personnel de conduite doit être impliqué au niveau des activités de test et d'inspection et que leur avis soit pris en compte.

8 Vérification et validation système

Le processus de vérification et de validation système pour la SCS est intimement lié au processus de vérification et de validation de la SCP. La répartition fonctionnelle homme-machine doit être réalisée en parallèle et simultanément pour la SCP et la SCS.

NOTE L'IEC 61513 fournit les exigences générales pour la V&V des systèmes d'I&C. La présente norme ne couvre que les exigences complémentaires de V&V qui sont particulières aux SCS.

Du fait de l'exigence de simplification des tâches et donc de l'information et des actions, la V&V de la SCS peut être simplifiée par rapport à celle de la SCP. Il convient de planifier la V&V de la SCS, avec des critères appropriés, en se basant sur l'IEC 60964 et sur l'IEC 61771.

Lors de la revue finale, on doit vérifier que les événements susceptibles d'entraîner une perte des fonctions de sûreté de la SCP n'ont pas d'impact sur la SCS ou sur ses fonctions. Lors des essais de mise en service, la disponibilité et la fiabilité de la SCS doivent être vérifiées.

Annexe A
(informative)

Evaluation de la fenêtre de temps sûre pour le transfert

Il est indiqué en 5.3.3 que «La conception doit s'assurer que le personnel de la salle de commande a le temps nécessaire pour atteindre la SCS après que la SCP soit devenue indisponible».

Cette annexe traite des facteurs qui peuvent être pris en compte pour démontrer cela, dont la liste est la suivante:

a) hypothèses concernant les scénarios crédibles de «perte de la SCP» – par exemple les causes et les types de «pertes de la SCP», les conséquences sur l'équipe de conduite de la SCP (par exemple sont ils disponibles ou non pour faire le transfert vers la SCS) et les conditions environnementales aux abords de la SCP et les chemins d'accès à la SCS;

b) hypothèses concernant les commandes automatiques de la tranche au moment du transfert des commandes de la SCP vers la SCS – par exemple celles liées aux actions de protection automatiques qui suivent l'arrêt manuel du réacteur avant évacuation de la SCP, ou les commandes automatiques liées au réacteur non arrêté si l'arrêt de celui n'a pas été effectif;

c) l'analyse des durées de la fenêtre de temps de transfert sûre pour différents scénarios crédibles – c'est-à-dire pour chaque scénario, le temps pour lequel l'analyse de sûreté montre qu'aucune action opérateur n'est nécessaire pour la sûreté;

d) l'analyse du temps nécessaire pour un transfert sûr du personnel et pour la mise en conditions opérationnelles de la SCS pour les différents scénarios crédibles – c'est-à-dire le temps séparant l'évacuation de la SCP du moment où les opérateurs ont transféré les commandes, ont mis la SCS en fonctionnement, ont évalué complètement l'état de la tranche (et ainsi sont prêts à engager toute action nécessaire);

e) justification du fait que le transfert peut être réalisé de façon fiable et dans le temps requis – c'est-à-dire les résultats des analyses réalisées des différentes étapes du point d) ci-dessus du point de vue des risques, de la fiabilité des équipements et des facteurs humains, en prenant bien en compte toutes les contraintes liées à:

   – la politique de sélection du personnel,

   – les exigences locales,

   – la réglementation nationale.

Bibliographie

IEC 60780, *Centrales nucléaires de puissance – Equipements électriques de sûreté – Qualification*

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

IEC 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté des centrales électronucléaires*

IEC 61227, *Centrales nucléaires de puissance – Salles de commande – Commandes opérateurs*

IEC 61508-1, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

IEC 61508-4, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

IEC 61772, *Centrales nucléaires de puissance – Salle de commande principale – Utilisation des unités de visualisation*

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

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

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

IEC 62645, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés*

ISO 9241, *Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV)*

Normes de sûreté de l'AIEA, Prescriptions N° GS-R-3: 2011, *Système de gestion des installations et des activités*

IAEA Safety Guide N° GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA Safety Guide N° GS-G-3.5:2009, *Management system for nuclear installations*

Normes de sûreté de l'AIEA N° SSR-2/2:2012, *Prescriptions de sureté particulières, Sûreté des centrales nucléaires: Mise en service et exploitation*

Guide de sûreté de l'AIEA N° NS-G-1.3:2005, *Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires*

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

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

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