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)

Documents
Document Sharing Hub

Full document details: IEC 60965 2016

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de 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.

Documents
Document Sharing Hub

Full document details: IEC 60965 2016

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

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

AVA Documents
Document Sharing Hub

Full document details: IEC 60965 2016

CONTENTS

FOREWORD....3
INTRODUCTION....5
1 Scope....7
2 Normative references....7
3 Terms and definitions....8
4 Abbreviations....9
5 Design principles....9
5.1 General....9
5.2 Main objectives....10
5.3 Safety principles....11
5.3.1 Design basis and design extension conditions....11
5.3.2 Functionality and qualification....12
5.3.3 Accessibility and operator transfer time....12
5.3.4 Control transfer, control prioritisation and security....12
5.3.5 Operational considerations....13
5.4 Human factors engineering principles....14
6 Design process....14
7 Functional design....15
7.1 General....15
7.2 Human factors....15
7.3 Location and access route....15
7.4 SCR environment....16
7.5 Space and configuration....16
7.6 Information and control equipment....17
7.7 Communication systems....17
7.8 Other equipment....18
7.9 Testing and inspection....18
8 System verification and validation....18
Annex A (informative) Assessment of safe transfer time window....20
Bibliography....21

Documents
Document Sharing Hub
Full document details: IEC 60965 2016

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:

Documents
Document Sharing Hub
Full document details: IEC 60965 2016

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.

Documents
Document Sharing Hub
Full document details: IEC 60965 2016

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;

AVA Documents
Document Sharing Hub

Full document details: IEC 60965 2016

– 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.

Documents
Document Sharing Hub

Full document details: IEC 60965 2016

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*

Documents
Document Sharing Hub

Full document details: IEC 60965 2016

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]

Documents
Document Sharing Hub
Full document details: IEC 60965 2016

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)".

AVA Documents
Document Sharing Hub

Full document details: IEC 60965 2016

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.

AVA Documents
Document Sharing Hub
Full document details: IEC 60965 2016

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.

AVA Documents
Document Sharing Hub

Full document details: IEC 60965 2016

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.

AVA Documents
Document Sharing Hub

Full document details: IEC 60965 2016

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.

Documents
Document Sharing Hub

Full document details: IEC 60965 2016