BS EN 60965:2016

BSI Standards Publication

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

bsi.

National foreword

This British Standard is the UK implementation of EN 60965:2016. It is identical to IEC 60965:2016. It supersedes BS EN 60965:2011 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Instrumentation, Control & Electrical Systems of Nuclear Facilities.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 93813 9
ICS 27.120.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2016.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60965

September 2016

ICS 27.120.20

Supersedes EN 60965:2011

English Version

Nuclear power plants - Control rooms - Supplementary control room for reactor shutdown without access to the main control room (IEC 60965:2016)

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)

Kernkraftwerke - Warten - Notsteuerstelle für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 60965:2016)

This European Standard was approved by CENELEC on 2016-07-18. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

This document (EN 60965:2016) consists of the text of IEC 60965:2016 prepared by SC 45A “Instrumentation, control and electrical systems of nuclear facilities” of IEC/TC 45 “Nuclear instrumentation".

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2017-07-18
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2019-07-18

This document supersedes EN 60965:2011.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

As stated in the nuclear safety directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law. In a similar manner, this European standard does not prevent Member States from taking more stringent nuclear safety measures in the subject-matter covered by this standard.

Endorsement notice

The text of the International Standard IEC 60965:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60880	NOTE	Harmonized as EN 60880.
IEC 61227	NOTE	Harmonized as EN 61227.
IEC 61508-1	NOTE	Harmonized as EN 61508-1.
IEC 61508-2	NOTE	Harmonized as EN 61508-2.
IEC 61508-3	NOTE	Harmonized as EN 61508-3.
IEC 61508-4	NOTE	Harmonized as EN 61508-4.
IEC 61772	NOTE	Harmonized as EN 61772.
IEC 61839	NOTE	Harmonized as EN 61839.
IEC 62138	NOTE	Harmonized as EN 62138.
IEC 62241	NOTE	Harmonized as EN 62241.
IEC 9241 Series	NOTE	Harmonized as EN ISO 9241 Series.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu

Publication	Year	Title	EN/HD	Year
IEC 60709	-	Nuclear power plants - Instrumentation and control systems important to safety - Separation	EN 60709	-
IEC 60964	2009	Nuclear power plants - Control rooms - Design	EN 60964	2010
IEC 61226	-	Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions	EN 61226	-
IEC 61513	-	Nuclear power plants - Instrumentation and control important to safety - General requirement for systems	EN 61513	-
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	Series	Ergonomic design of control centres	EN ISO 11064	Series
ISO 11064-1	-	Ergonomic design of control centres - Part 1: Principles for the design of control centres	EN ISO 11064-1	-
ISO 11064-3	-	Ergonomic design of control centres - Part 3: Control room layout	EN ISO 11064-3	-
ISO 11064-6	-	Ergonomic design of control centres - Part 6: Environmental requirements for control centres	EN ISO 11064-6	-
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)		

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

FOREWORD

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*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.