BS IEC 60965:2009

BSI British Standards

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

raising standards worldwide™

BSI British Standards

National foreword

This British Standard is the UK implementation of IEC 60965:2009.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

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.

ISBN 978 0 580 59012 2

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 2009

Amendments issued since publication

Amd. No.	Date	Text affected

IEC 60965

Edition 2.0 2009-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

Q

ICS 27.120.20

ISBN 2-8318-1053-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – CONTROL ROOMS – SUPPLEMENTARY CONTROL POINTS 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

FDIS	Report on voting
45A/749/FDIS	45A/769/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 second edition cancels and replaces the first edition published in 1989. This edition constitutes a technical revision.

The main technical changes with regard to the previous edition are as follows:

- to clarify the definitions and review the requirements.
- to update the reference to new standards published since the first issue, including IEC 61227, IEC 61771, IEC 61772, IEC 61839, and IEC 62241.
- to align the Standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3.

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

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

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

INTRODUCTION

a) Technical background, main issues and 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 that recent technical developments especially those which are 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.

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

At the end of the current revision, at the FDIS stage, two further points were identified. These are: (a) requirements should be included associated with regular testing of the SCP, and (b) a theoretical assessment is needed of the time available during which the reactor will be safe but unattended, in order to move from the MCR to the SCP and for the SCP to become operational. However, since these points were not raised formally by any National Committee, they are recorded in this introduction for development in the next revision.

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 supplementary control points.

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 points of a nuclear power plant to meet safety requirements.

This standard is intended for application to supplementary control points 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 Clauses 6.15 to 6.30 of IAEA NS-G-1.3, are:

- The definition of the MCR and plant design bases for which the supplementary control points are to be used.
- Access by station staff to the supplementary control points in such emergencies.
- Assurance for the station staff that the environment at the supplementary control points is safe when they are to be used.

- Provision of information at the supplementary control points on the state of the reactor critical functions.
- Transfer of control and indication functions from the main control room to the supplementary control points in emergencies.
- Independence and separation of the cabling used by the supplementary control points from that used by the main control room.
- Assurance that a safe shutdown state has been reached using the supplementary control points.
- Communication facilities between the supplementary control points 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 and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA (now replaced by IAEA GS-R-3) for topics related to quality assurance (QA).

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

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

1 Scope

This International Standard establishes requirements for the supplementary control points provided to enable the operating staff of nuclear power plants to shut down the reactor 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 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 points.

It is assumed that supplementary control points 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 Requirements NS-R-1 “Safety of Nuclear Power Plants: Design” and IAEA Safety Guide NS-G-1.3 “Instrumentation and Control Systems Important to Safety in Nuclear Power Plants”.

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

This standard is intended for application to supplementary control points 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 points and the main control room, the ergonomic approach, the automation level and the information technology.

2 Normative references

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

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

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

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

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

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

IAEA NS-R-1:2000, *Safety of nuclear power plants: Design*

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

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
a 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.

[IEC 60964, 3.4]

3.2
local control points (or facilities)
points (or facilities) located outside the control room where local operators perform control activities

[IEC 60964, 3.17]

3.3
local operators
the operating staff that perform tasks outside the control room

[IEC 60964, 3.18]

3.4
operating staff
plant personnel working on shift to operate the plant. The operating staff includes the control room staff, maintenance engineers, etc.

[IEC 60964, 3.20]

3.5
supplementary control point
a 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. The supplementary control point may be a special control room, but in many cases comprises a set of control panels and displays in switchgear rooms or similar areas.

4 Abbreviations

I&C Instrumentation and Control

LCP Local Control Point

MCR Main Control Room

NPP Nuclear Power Plant

PIE Postulated Initiating Event

SCP Supplementary Control Points, Supplementary Control Point

V&V Verification and Validation

5 Design principles

5.1 General

Clause 6.75 of IAEA NS-R-1 states “Sufficient instrumentation and control equipment shall be available, preferably at a single location (supplementary control room) that is physically and electrically separate from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and the essential plant variables can be monitored should there be a loss of ability to perform these essential safety functions in the control room”.

Clauses 6.15 to 6.30 of IAEA NS-G-1.3 provide guidance on the requirements for supplementary control rooms (‘SCP’ in this standard), including requirements associated with the following:

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

5.2 Main objectives

The SCP shall be provided with the means to trip the reactor and bring the plant to a safe shutdown state and maintain it in that state without access to the MCR. However, the SCP are 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 SCP.

The SCP are required if the conditions within the MCR are no longer within its operational design bases, and in consequence are such that the MCR is no longer available. 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 the SCP are necessary and intended to be used shall be identified. This shall include identification and justification of the assumed duration for which the SCP may be required.

Since events leading to 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 SCP. In particular, the design of the SCP shall take account of the possible long-term unavailability of the MCR due to fire or other reasons.

The criteria for use of the SCP 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 SCP.

From an operational viewpoint (e.g. to simplify operation and avoid misunderstanding), it is preferable to have only one SCP. Care shall be taken, however, to meet safety requirements, particularly requirements for redundancy and independence.

There should be full presentation ability at all SCP of any computer-based information display and alarm system.

There shall be adequate time to reach the SCP 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. Requirements are given in 7.7.

The layout of the instrumentation and the mode of presentation at the SCP 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 controlled from the SCP may be limited to those providing the safety functions.

The SCP shall provide sufficient control over the safety functions to reach and maintain a safe shutdown state, for the defined set of PIEs and conditions for which the MCR cannot be used. The supervision and control provided at the SCP 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 NS-R-1, Clause 4.6).

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 SCP or may be a location that would not be affected by the same event that causes the SCP to be used.

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

5.3 Safety principles

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 SCP (and local control points) required for safe shutdown, monitoring to

ensure safe shutdown and critical functions control and monitoring, unusable or ineffective simultaneously.

The functions of the SCP 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 SCP.

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).

Taking into account the postulated causes of unavailability of the MCR functions, the SCP functions shall be so designed (and, if necessary, the SCP so located) that, even under emergency conditions, the SCP are accessible by safe routes.

The design shall allow adequate time for control room staff to reach the SCP after the MCR becomes unavailable. The actions and duration of unattended automatic operation of the safety functions, after initiation at the MCR, up to the time when the SCP becomes operational, should be shown to be satisfactory for this transfer. This shall allow time for access control and time to assess the plant state at the SCP.

Facilities to disable MCR control and transfer control to the SCP 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.

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 SCP and from SCP to MCR.

The control transfer facilities may be on the route from the MCR to the SCP, or at the SCP, 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 SCP. Where the facilities are located in the MCR, additional means that do not involve the MCR should also be provided.

The SCP should include a means to identify the control status of the SCP and of the MCR controls.

I&C systems shall be so designed to prevent simultaneous control of plant systems from both the MCR and SCP.

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 SCP 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.

When an SCP 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 SCP 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 SCP and vice versa. Access to the SCP, and any attempt at control transfer to the SCP, shall be indicated in the MCR.

The SCP shall be designed to minimise operator errors.

The design shall include the provision of written instructions at the SCP for operation of:

- Plant systems and control devices.
- Information and recording systems.
- Communication equipment.
- Any other equipment to be operated from the SCP.

The operating procedures for actions to be taken from the SCP shall be simple and clear.

The SCP equipment shall be qualified for the environmental conditions applicable to the design basis PIE and sequence of events for which the SCP are necessary and intended to be used.

The designer shall specify the regular testing and inspection of the SCP equipment required to meet the design principles.

The design shall permit regular training and practice in the use of the SCP 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 at the SCP.

If the safety analysis shows that long term occupation of the SCP 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 SCP shall follow the same design rules as that for the MCR.

Where multiple SCP and/or LCP are necessary, 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 SCP is necessary, 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 SCP 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 SCP design and documentation objectives and principles.

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

b) Develop the plant specific SCP 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 SCP functions with respect to their importance to safety, and define the corresponding design and qualification requirements.

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

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

g) Finalise the SCP 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).

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

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 SCP, 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.

An adequate level of illumination shall be provided to ensure that visibility is sufficient for task performance on a continuous basis without undue fatigue.

The auditory environment shall enable clear verbal communication to be held.

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

Fire is an important hazard following which use of the SCP may be required, and an assessment of the fire protection of the SCP and the human routes to them should be made and should show accessibility to the SCP 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 conditions for which the SCPs are to be used. The assessment of the cable routes should demonstrate independence of the SCP cables from the MCR cables.

It shall be possible to reach the SCP 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 SCP is required.

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 SCP. Before an SCP 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, particularly 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 SCP environment

The environmental conditions at the SCP 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.

For the design basis conditions requiring use of the SCP, the environmental conditions shown by the safety analysis for the intended location of an SCP shall not exceed those for normal unprotected human access. Where an SCP may be required for use in a beyond design basis or severe accident condition, involving the national security plan, the location should be shown to be suitable for normal human access in those conditions.

A battery powered emergency lighting system shall be continuously available even upon failure of the normal system. 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.

7.5 Space and configuration

The SCP 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 SCP configuration shall enable prompt mobilisation by the operating staff upon their arrival at the SCP.

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.

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 a single SCP does not provide the redundancy needed within itself, and redundancy is not otherwise provided by an alternative SCP, use of a local control point can, for some plant designs, provide the necessary indication or control to mitigate a failure of the SCP functionality. For exceptional conditions, if this is required by the safety arguments, this should be considered as an engineering solution rather than extending the SCP 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

SCP 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 SCP and local control points. If more than one SCP is necessary, communication between these SCPs 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 SCP and/or local control points.

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 SCP or readily accessible from the SCP 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 SCP, concerning access control, site security and actions in response to fires. If not provided elsewhere, the SCP design shall include any facilities for these functions, such that they can continue during the period that the MCR cannot be used.

8 System verification and validation

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

Due to the requirement for simplification of tasks and therefore also of information and actions, the V&V of the SCP may be made simpler than that for the MCR. The V&V of the SCP 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 SCP or its functions. During the on-site commissioning tests, the availability and reliability of the SCP shall be verified.

Bibliography

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

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

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

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

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

_____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9000 Fax: +44 (0)20 8996 7400

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

You may also buy directly using a debit/credit card from the BSI Shop on the website **www.bsigroup.com/shop**

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library.

Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.

Tel: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™

British Standards