BS 4877:2016

BSI Standards Publication

Nuclear reactor instrumentation and control – Code of practice

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2016

ISBN 978 0 580 87517 5

ICS 27.120.10

The following BSI references relate to the work on this document:
Committee reference NCE/8
Draft for comment 16/30310379 DC

Publication history

First published December 1972
Second (present) edition, October 2016

Amendments issued since publication

Date	Text affected

Contents

Foreword *ii*

1 Scope *1*
2 Normative references *1*
3 Terms, definitions and abbreviations *1*
4 General I&C design principles *4*
5 I&C systems *13*
6 Reactor and plant instrumentation *20*
7 Secondary circuit, turbine and electrical systems *28*
8 Design recommendations *29*

Annexes
Annex A (informative) Nuclear power plants – I&C systems – A guide to applicable standards *44*

Bibliography *61*

List of tables
Table A.1 – IAEA Safety guides, IEC SC45A standards and other relevant standards *44*
Table A.2 – List of existing standards and technical reports and their titles *46*

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 62, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 October 2016. It was prepared by 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.

Supersession

This British Standard supersedes BS 4877:1972, which is withdrawn.

Information about this document

This British Standard has been written by I&C engineers based on experience of typical UK plants so far constructed, with experience of some other plants.

This is a full revision of the standard, originally published in 1972, and introduces the following principal changes:

a) the role of the design base of the plant and the life cycle in the I&C design;

b) summaries of the principal reactor faults for which protection is needed;

c) an outline of the main I&C systems on a nuclear plant and their role in defence in depth;

d) the addition of recommendations for specific measurements, e.g. control rod position, secondary coolant, emergency feedwater flow and electrical system state;

e) the addition of recommendations covering the use of software; and

f) an annex listing and describing the most relevant International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC) documents.

This British Standard gives objectives and recommendations based upon practical experience and meets the principles of the relevant IAEA publications. Detailed references to standards are not included within the clauses, but Annex A contains a comprehensive guide to the relevant IEC and IAEA Safety Guides and Standards.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Users of this British Standard are expected to be able to demonstrate compliance with all recommendations contained within.

Conformity to this British Standard does not, in itself, meet the requirements of the Office for Nuclear Regulation for nuclear safety justification and users are directed to the ONR (www.onr.org.uk) for further information.

This British Standard has been developed for use by designers, constructors and users of nuclear power plant instrumentation systems, to give guidance and the background to the design and implementation practice for the instrumentation and control (I&C) systems of a nuclear plant.

The users of this document are expected to include:

a) experienced I&C engineers unfamiliar with nuclear power and engineers of other disciplines;

b) engineers needing a comprehensive guide to the relevant IEC standards;

c) those needing a basis in the key safety role of I&C systems in nuclear power;

d) managerial and other professionals needing a background on current practice; and

e) I&C engineers who wish to understand the general principles of I&C on nuclear plants, readable by those with limited experience, and who might have responsibility for others who are designing the detailed I&C for the plant.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type and does not constitute a normative element.

The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the Clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

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

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

This page deliberately left blank

1 Scope

This British Standard provides recommendations for determining the I&C design and identifying the I&C systems and measurements required on a nuclear reactor plant, including the equipment required for reactor safety and protection, automatic control, and for the information and control in the main and supplementary control rooms of the nuclear reactor plant.

This British Standard provides recommendations for a clear life cycle for the design and implementation of control and instrumentation systems. This includes the documentation of the I&C design basis, classification of functions according to their safety importance, identification of a fault schedule and of internal and external hazards such as fire, environmental and seismic events or flood.

This British Standard also provides recommendations for the main I&C systems on the plant and control rooms including:

- sensors;
- actuator interface operation;
- measurements;
- measurement methods;
- the reactor protection system;
- control and display facilities for reactor control and instrumentation; and
- power supplies and communication systems.

This British Standard does not cover commercial or managerial matters, the measurement and control of radioactivity releases, or the specific faults that require protection. It does not cover refuelling systems, the emergency control centre or technical support centre, off-site support for emergencies, or what constitutes an acceptable radiological risk.

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.

BS 3693, *Recommendations for design of scales and indexes on analogue indicating instruments*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

NOTE Terms are used in accordance with the definitions in the IAEA safety glossary [1].

3.1.1 accident conditions

deviations from normal operation that are less frequent and more severe than anticipated operational occurrences

3.1.2 anticipated operational occurrences
operational processes deviating from normal operation which are expected to occur at least once during the operating lifetime of a facility (e.g. a nuclear power plant) but which, in view of appropriate design provisions, do not cause any significant damage to items important to safety or lead to accident conditions

3.1.3 defence in depth
design of a nuclear facility which includes the following five levels of defence:

a) level 1: prevents deviations from normal operation and the failure of items important to safety;

b) level 2: detects and controls deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions;

c) level 3: prevents damage to the reactor core or radioactive releases requiring off-site protective actions in the event that an accident occurs and returns the plant to a safe state;

d) level 4: mitigates the consequences of accidents that result from failure of the third level of defence in depth;

e) level 5: mitigates the radiological consequences of radioactive releases that could potentially result from accidents.

NOTE 1 The IAEA requirements for design introduce the concept of defence in depth in the design of a nuclear facility.

NOTE 2 The IAEA description is more comprehensive than that given above.

NOTE 3 Levels 1 to 4 mainly relate to the on-site provisions, the fifth level mainly relates to off-site provisions.

3.1.4 design basis accident
postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits

3.1.5 design extension conditions
postulated accident conditions that are not considered for design basis accidents, but are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits

NOTE Design extension conditions involving significant core degradation are also called severe accidents.

3.1.6 failure
continuing occurrence of a defect in the main plant which threatens plant safety

NOTE The term failure refers to a continuing condition such as the state following a component or module failure of the I&C systems and sensors, or the continuing state of failure of a plant item.

3.1.7 fault
initiating event leading to a state of failure

3.1.8 normal operation
operation within specified operational limits and conditions

3.1.9 partial trip
trip condition detected by a single redundancy of the safety system which has not been voted

3.1.10 safety system
complete system of plant and I&C equipment that ensures the safety of the plant and reactor

NOTE 1 Its parts consist of the protection system, the safety actuation system and the safety system support systems.

NOTE 2 Other items important to the safety of the plant equipment as a whole, as opposed to items not important to safety, but which are not part of the safety system, are termed by the IAEA "the safety-related items or systems", which is ambiguous as a term, as many USA documents use the term in its normal sense in English use, to mean any item of the safety system.

NOTE 3 The I&C equipment that provides the detection of unsafe conditions and initiates the actuations needed to ensure safety forms "the protection system", which in turn is divided into safety groups for each fault requiring protection.

3.1.11 safety group
assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

3.1.12 safety monitoring unit
trip amplifier or equivalent that feeds a processed measurement of a potential trip condition (which might be a partial trip) to the safety logic assemblies concerned

3.1.13 safety-related system
system important to safety that is not part of a safety system

NOTE A safety-related instrumentation and control system, for example, is an instrumentation and control system that is important to safety but which is not part of a safety system.

3.1.14 single failure criterion
criterion applied to a safety group performing all actions required to respond to a postulated initiating event (PIE) in the presence of the following:

a) any single detectable failure within the safety system in combination with:
   1) any undetectable failures, i.e. any failure that cannot be detected by periodic testing, alarm or anomalous indication;
   2) all failures caused by the single failure;
b) all failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety group; and
c) the removal from service or bypassing of part of the safety system for testing or maintenance that is allowed by plant operating limits and conditions

3.2 Abbreviations

For the purposes of this British Standard, the following abbreviations apply.

AGR	advanced gas-cooled reactor
ATWT	anticipated transient without trip
BWR	boiling water reactor

CCF	common cause failure
DNBR	departure from nuclear boiling ratio
EMI	electro-magnetic interference
EQ	equipment qualification
ESF	engineered safety feature
HDL	hardware description language
HF	human factors
HMI	human machine interface
HVAC	heating, ventilation and air conditioning
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
LOCA	loss of coolant accident
MCR	main control room
PA	public address
PAMS	post-accident monitoring system
pfd	probability of failure on demand
PIE	postulated initiating event
PORV	power-operated relief valve
PWR	pressurized water reactor
RPV	reactor pressure vessel
RTD	resistance temperature detector
SCR	supplementary control room
SFC	single failure criterion
SGTR	steam generator tube rupture
SI	safety injection
SIDS	safety information display system
SPDS	safety parameter display system
V&V	verification and validation

4 General I&C design principles

4.1 Safe operation

*COMMENTARY ON **4.1***

Safe operation of a nuclear power plant is the responsibility of management, and involves the management of administrative and technical measures necessary to ensure security of hardware and software from inadvertent or malicious actions.

The I&C design should ensure safe operation of the nuclear power plant throughout the life of the nuclear reactor.

The I&C design should identify and analyse the faults that could occur on the plant including, as appropriate:

a) reactivity faults, causing increases in neutron flux and power, excess reactor temperatures, coolant instability and other effects. Reactivity faults can be

caused by incorrect control rod movements, fuel loading or neutron absorber conditions, and coolant temperature changes;

b) loss of coolant inventory, causing depressurization of the reactor vessel, active coolant entering the containment or environment, and failure to remove heat from the reactor core. These faults can be caused by breaks of instrument lines, breaks of auxiliary cooling or make-up pipework, or potentially major failures of the main coolant pipework;

c) loss of coolant circulation by the primary coolant pumps or failure of the secondary coolant systems, resulting in failure to remove heat from the reactor itself. These faults can be caused by failure of electrical supplies, or of the main feedwater pumps or systems, failures of valves controlling or managing the flow, and failure of emergency or shutdown coolant systems;

d) loss of incoming grid electric power, or of electrical supply distribution, or failure of emergency supplies to operate correctly. These faults can cause plant trips, loss of power to pumps and valves, loss of I&C functions, and changeover to alternative supplies;

e) failure of support systems such as HVAC of the plant or MCR. These faults might cause loss of habitability of the control room and loss of cooling to systems;

f) internal and external hazards, including seismic events, storm, flood, lightning strike, high energy release and fire. These hazards can cause plant damage, loss of access to plant areas, and damage to electrical systems. Fire could affect cables with major problems of plant operation and monitoring; and

g) other faults not covered by a) to f) which should be determined in order to identify the most effective plant operations needed to contain them. These hazards could cause plant damage, loss of access to plant areas, and damage to electrical systems.

For all postulated initiating events (PIE) of the faults identified by the safety analysis process, the I&C systems should provide automatic protection actions which restore the plant to a safe state without the need for operator action for a minimum of 30 min from the detection of the PIE.

NOTE 1 On a nuclear plant, a small number of potential faults could be identified whose frequency of occurrence and consequences are so low that they can be mitigated by operator action. A small number of possible faults, e.g. gross reactor vessel failure, could be discounted due to the very great care taken in design, manufacture and inspection of the plant item to ensure a very low probability of failure.

A fault schedule should be produced listing potential plant fault situations which could occur in the reactor and associated plant, the consequences of the fault, and the protection provided against the fault.

The I&C systems should include functions that alert operators to conditions that indicate possible fuel failure and that produce an automatic reactor trip before serious damage occurs.

The design of the I&C architecture should fulfil the following high-level plant objectives:

1) prevent the escape of radioactivity by keeping the reactor within its safe operating envelope by arresting transients and preventing them from causing danger; and

2) provide economic and efficient operation.

Instruments that display and record a small set of key plant variables, e.g. shutdown flux, reactor trip state, emergency coolant flow, should be available to allow operators to understand the status of critical safety functions and to implement accident management strategies.

NOTE 2 For future nuclear power plants, it is intended that the operator is able to control and monitor the equipment required for core cooling and containment venting, regardless of the status of normal plant power systems.

4.2 I&C Life cycle

The development of each I&C system should follow a defined life cycle covering:

a) input or identification of design basis requirements;

b) development of design and allocation of functions to systems;

c) implementation;

d) verification and validation;

e) installation and testing on site; and

f) commissioning.

This life cycle should take into account the following requirements and constraints:

1) the results of the plant safety analysis;

2) the design of the mechanical plant systems;

3) the civil engineering requirements;

4) the desired operational arrangements and modes of operation of the plant;

5) the maintenance requirements and availability targets; and

6) the ageing, obsolescence and replacement policies.

4.3 I&C design system interaction

The I&C design should take account of the civil and mechanical engineering processes of the nuclear power plant design, including:

a) equipment and plant location;

b) identification of equipment sizes and weights;

c) equipment seismic supports;

d) cable separation for hazard withstand;

e) cable access to equipment;

f) cable routeing and support; and

g) power supplies and power requirements of each system.

4.4 I&C design basis

The I&C designers should obtain a design basis document identifying the potential faults of the reactor plant and its associated systems. This analysis should include:

a) an assessment of the severity to nuclear safety of each plant fault;

b) the estimated frequency of each fault; and

c) their consequences to nuclear safety.

The estimated frequency of each fault, the probability of failure of the mitigation, and the resulting hazard frequency and consequences should be identified. Where these consequences are excessive, additional mitigation requirements should be included.

From the plant design process the I&C functions required to mitigate the hazards from plant faults should be identified, i.e. the functions of the protection system, safety actuation system and safety support system. The required reliability of the safety functions should be determined and specified in the design basis of the I&C.

The overall plant analysis should determine how safety is to be maintained following a severe reactor accident or external hazard that could potentially lead to widespread loss of on-site power supplies and a corresponding loss of operator capability to monitor and control the plant from the MCR.

The I&C design basis document should be prepared with input from the operating authority of the reactor with regard to the performance requirements. It should identify:

1) the postulated initiating events as a fault schedule, giving the method of detection of each fault for which reactor protection should be provided;
2) the hazards (such as fire, flood, storm and seismic event) through which the plant is required to operate or to remain safe;
3) any appropriate design extension conditions; and
4) the defence in depth functions to be provided by the I&C systems and plant for such fault conditions (see **3.1.3** for a description of the levels of defence that constitute the defence in depth provisions).

From this I&C design basis document, the structure of the I&C system, the functional role of each part contained within it, and the performance required from it should be determined.

The I&C functions should be categorized according to their importance to safety and allocated to the I&C systems. The I&C systems and equipment should then be classified according to their importance to safety. This classification should then determine the degree of attention to quality required for each equipment system (which could perform several functions of different safety importance) during design and implementation, and should determine the requirements for equipment qualification.

I&C system performance, e.g. response time, sensitivity, resolution, and range should be suitable to support the safety functions.

Individual requirements documents should be generated for each part of the overall I&C system.

The analysis and identification of the control functions, indications and alarms that are to be available in the MCR and the SCR, and their role in safety, should form part of the I&C design basis. This should include input from experienced control room operators.

The experience gained from previous operational occurrences and accidents should be included in the design and implementation of the I&C systems, and in the intended use to be made of the I&C systems by the operators.

4.5 Management systems and quality assurance processes

A standard format and identification system for each level of the design documents should be established. These should be prepared in a manner that allows tracing between the levels of detail for all safety requirements. Controlled processes for the preparation, authorization, issue and revision of design documents should be established.

Design documentation should be subject to an independent review process, with V&V of the documents and their implementation.

The design processes should conform to relevant standards (see Annex A) in order to achieve both a design and V&V of the design and its implementation to a level consistent with the importance to safety of each system.

Configuration management of documents, equipment and software should be implemented as a critical requirement for safety.

I&C systems should be analysed and tested before they are put into service, and the limits within which the systems might be configured should be confirmed and documented. Commissioning programs should be designed to validate I&C functions before those functions are used, to ensure nuclear safety.

4.6 Equipment qualification

*COMMENTARY ON **4.6***

Equipment that is exposed to environments no more demanding than that of equipment rooms might only require standard commercial acceptance testing, together with validation of functional and performance requirements.

Some safety equipment in reactor containment and elsewhere can be exposed to high temperatures, steam and acid environments in which it is required to operate to preserve safety, and therefore more extensive testing and demonstration is required.

All I&C systems should be subject to appropriate equipment qualification to provide assurance of their capability to perform their required functions.

For safety system and equipment that might be exposed to harsh environments at reactor faults, e.g. within the containment of water cooled reactors, extensive and controlled tests of sample units should be carried out.

If the equipment performance is affected by ageing, the tests should be carried out on equipment that has been suitably aged prior to testing.

For equipment that is required to perform during or after a seismic event, seismic testing should be carried out.

NOTE The most severe seismic conditions are defined in the design basis of the plant as a whole, and broken down by building floor level and location after computer studies of the seismic spectra for each equipment location.

The I&C system should withstand electrical interference, based on the maximum levels of interference expected, including potential interference from radio or wireless communication systems.

I&C systems should not emit EMI levels sufficient to affect the operation of other systems. The design should identify requirements for cable routeing, screening and earthing arrangements.

The use of wireless transmission and radio communications on site should be prohibited where equipment is located that is not qualified for their use.

4.7 I&C system architecture, redundancy and the single failure criterion

The architecture of the I&C system should conform to the defence in depth requirements of the NPP (see **3.1.3** for a description of levels 1 to 4 of the defence in depth that apply to the I&C). The basic rules that apply are as follows:

a) for any specific PIE, I&C systems should only perform functions at one of level 1, level 2 or level 3 and should be independent of the I&C systems performing functions at the other levels for the same PIE;

b) where the reliability (pfd) targets are more onerous than can be claimed for a single non-diverse I&C system for a function at level 3, at least two diverse systems should be provided;

c) I&C systems that perform functions at level 4 should be independent of I&C systems performing functions at levels 1, 2 or 3.

The I&C system architecture should include redundant units, modules and power supplies from redundant sources. The architecture should ensure that safety groups of equipment performing the safety functions are separated such that failure to operate any one safety group does not prevent another safety action taking place when required.

Redundancy of equipment should be provided, including the information system and control systems, in a manner that allows continued operation of the plant if single modules, units or power supply sources fail.

NOTE 1 The reactor safety and protection functions are typically provided by four independent channels of protection logic operating four plant sets of safety equipment for frequent faults of the design basis.

The architecture of the I&C system should reflect the means of achieving defence in depth of the reactor, such that each level of defence is, so far as practicable, independent in its sensors, logic and actuations from the earlier level which is expected to operate. Each level should be provided with redundancy, which should meet the single failure criterion (SFC) where a radiation hazard can be expected due to the plant fault, if not mitigated.

The SFC should be applied to systems performing category A functions. For category B functions, redundancy should be applied, taking into account the specific reliability requirements.

NOTE 2 BS EN 61226 establishes a method of classification of the information and command functions for nuclear power plants, and the I&C systems and equipment that provide those functions. See Annex A, Table A.2.

The I&C system should exploit diversity of sensor types and methods of operation, to reduce the potential for CCF.

NOTE 3 The architecture of the I&C system might depend on equipment technology without diversity where no practicable means of achieving this are available.

To achieve independence, the architecture of the I&C system should be based on clear separation of protection channels that include the sensors, logic and actuators needed for the safety groups of the safety system. Separation should be maintained between safety channels, between redundant safety groups or guard lines and between power supplies.

4.8 Reliability assessment and calculation

*COMMENTARY ON **4.8***

The safety systems of NPPs are subjected to reliability assessment to ensure hazard frequencies and their consequences are reduced to an acceptable level. The safety assessment makes assumptions regarding the reliability of I&C systems and equipment which have to be substantiated by the I&C design. The reliability assessment sets out to determine the probability of random failure, often assuming that the design is proved correct before entry into service. However, where complex systems are employed (typically involving software, including HDL) the practical limitations of design assessment and validation often result in a contribution representing the probability of a design error (CCF) being included. This is usually done by placing limits on the claimed reliability of such systems and combinations of systems.

The design of all I&C systems and equipment should be justified to meet the reliability claimed within the safety assessment for each function being implemented.

The assumptions and data used in reliability calculations should be documented and justified.

Calculations of system reliability should include methods to allow for common cause failure, where appropriate.

Calculations to demonstrate that the design reliability requirement of any I&C system has been achieved should assume that:

a) all equipment is tested to demonstrate its correct functioning at defined intervals;

b) an unrevealed, unsafe failure exists until the next maintenance activity;

c) any annunciated failure is repaired within a defined period; and

d) each channel is in an unsafe, failed condition for a defined period while being repaired or maintained.

Only in exceptional circumstances (i.e. where directly relevant failure rates have been observed) should a claimed probability of failure on demand for a system be less than 10^{-4}.

Assumptions regarding operator response and repair durations should be subject to human factors assessment to demonstrate their suitability and degree of conservatism.

All data used within the reliability analysis should ensure that the reliability analysis can demonstrate an appropriate confidence level.

Where digital equipment based on programmable computer methods is used, the assessment of reliability should be underwritten by comprehensive V&V and analysis methods.

Once the I&C systems and equipment enter service, the practical reliability achieved should be monitored and compared with the results of the reliability assessment to ensure the validity of the assessment.

NOTE Repetitive unreliability can lead operators to distrust and even ignore the information given and actions taken by the I&C system. This loss of trust has, in the past, led operators to delay responding to accident conditions, and to wrongly initiate plant restart after reactor trips without further investigation.

Safety and safety-related systems should be designed to minimize spurious actions or misleading indications and alarms.

4.9 Human factors

*COMMENTARY ON **4.9***

*This subclause relates closely to **8.4** and **8.5**, but is intended to cover aspects relating to the whole design process. Detailed human factors input is essential for the I&C system's success.*

The I&C design process should take into account the development of a clear identification and description of the distinct roles of the different operating staff and their interaction with the controls and information provided for them.

A specific human factors assessment of the control room design, its functions and layout, and the information and controls that it provides should be carried out. This should address:

a) the potential for operator error and the provisions for preventing such error; and

b) all claims for operator action in response to plant faults.

During the design, a task analysis should be undertaken to identify the user requirements for the I&C and for the HMI, both for the control room areas and for local-to-plant functions.

HMI facilities and operating procedures should be reviewed to ensure that safety claims can be met. Assessments should be undertaken to ensure that all defined operations can be carried out correctly and within the necessary timescales.

The design of the control room should take account of ergonomic factors such as human physical limits of reach and perception, and limits of noise and environment. The design should allow for factors such as the operator's diagnosis of the situation, and actions taken, during abnormal operation (see **4.10**).

NOTE Operators have been known to make a diagnosis of a situation and hold to it as a confirmation bias (mind set), which could be incorrect, and then not take account of evidence which might change their understanding of the situation.

The arrangement of controls and instruments, and their operating actions which cause plant changes, e.g. open or close a valve, start or stop a pump, etc., should be consistent and adopted throughout the plant.

Operator aids should be provided to facilitate use of the available information for assessing plant conditions, e.g. fault transient support software.

The I&C system, and the HMI in the control rooms, should ensure the operator can assess and confirm that conditions in the power plant are safe.

4.10 Safety and control arrangements for abnormal operation

*COMMENTARY ON **4.10***

For the majority of its life, the reactor of a nuclear power plant is in an intact state and at normal power operation. This subclause considers various other planned nuclear power plant states, such as commissioning, fuel loading, maintenance, modification and testing, and various postulated plant fault conditions, such as anticipated operational occurrences, design basis accidents and design extension conditions (including severe accident and extreme hazard situations).

4.10.1 Commissioning, fuel loading, maintenance, modification and testing

*COMMENTARY ON **4.10.1***

During commissioning, before fuel is loaded, or at other times on an operable plant, e.g. upon changing from one operating mode to another, the plant is operated in various test modes. These can require the safety system to be partly or totally disabled, since reactor pressure can be low, actuators might be disabled or under test, instruments might not yet have been put into service, or might be being calibrated or otherwise tested. During fuel loading operations, the reactor is in a state that allows access to the fuel channels, and off-load refuelling designs require the coolant circuit to be at atmospheric pressure and the coolant level to be that of the refuelling canal with the reactor vessel head removed. During refuelling, many other at-plant activities are undertaken for maintenance and upgrading the plant and I&C systems. Special operational bypass features are therefore needed for the safety system during these conditions.

All commissioning procedures and tests, and the I&C provided for the tests, should be planned and analysed prior to the test for any safety threats that could occur, to ensure that instrumentation is available in suitable positions to monitor the conditions that could arise.

NOTE Administrative measures include the use of processes in which formal checks are conducted and approvals obtained before specified actions are permitted. Physical measures include the use of interlocks which prevent certain actions from being taken until certain physical conditions within the plant have been fulfilled.

If the safety system is not fully functional or has special bypass features included for testing or commissioning the plant, administrative and physical measures should be taken to ensure it is returned to a fully operable state after the test is completed, and that this is confirmed, before reactor operation takes place.

When routine tests are required for a plant (e.g. for testing control rod trip insertion times or estimating core reactivity), the I&C systems should be assessed to ensure that all safety hazards that could arise are monitored, so that complete protection is available during the tests.

Operational bypass features required to enable the plant to be configured for tests, fuelling or refuelling conditions should be in accordance with **8.2.5**.

For all commissioning and fuel loading operations, communication systems should be available to ensure administrative control of all at-plant operations (see **5.4.4**).

Indications should be provided to identify that the plant is under maintenance or testing.

4.10.2 Postulated plant fault conditions

*COMMENTARY ON **4.10.2***

A highly conservative approach might be appropriate for some aspects of the design dependent on the reactor type and associated safety case, to ensure that anticipated operational occurrences, design basis accidents and design extension conditions can be safely managed. Extensive work has been undertaken to investigate accidents that have occurred and to design support systems and operator aids that can be used in such conditions.

Instrument channels providing data required to monitor plant conditions or to take control actions under design basis or design extension conditions should measure and display the full range of parameter values that might occur under those conditions.

Operator aids should be provided to support the use of the available information for assessing plant conditions.

*NOTE See **8.4** and **8.5** for further information.*

An indication should be given when plant conditions deviate from normal.

4.10.3 Design extension conditions

I&C systems that monitor plant conditions or take control actions under beyond design basis conditions should be able to measure and display the full range of parameter values that might occur under anticipated operational occurrences, design basis accidents and design extension conditions.

If significant fuel failure is a possibility there should be operable instrumentation that can detect radioactive releases.

For emergency response situations, the maximum range of the activity monitors should exceed the physically achievable radiation level for the specific location.

High range radiation monitors should be available to emergency responders.

5 I&C systems

5.1 Safety system

*COMMENTARY ON **5.1***

The functions of the safety system (which includes the reactor protection system, see the IAEA safety glossary [1]) provide the principal means of defence for the plant, and include a range of diverse features regarding sensing method, equipment type or safety function, where two different actuations could achieve the same result.

5.1.1 General

The protection against each fault should be, where practicable, actuated from two physically different variables, one of which should be, where possible, a direct measurement of the parameter of greatest concern.

Instrumentation intended to initiate safety actions (either automatically or by operator action) should be redundant. Means should be available to resolve conflicting readings. Diverse measurements should be provided.

Each redundant instrument channel provided for automatically or manually initiating a protection system function should meet all performance and display requirements necessary to ensure that the function is initiated when required.

5.1.2 Reactor protection system

*COMMENTARY ON **5.1.2***

The reactor protection system operates to maintain the safety of the reactor and the limitation of any active releases to the environment by automatically shutting down the reactor when PIE conditions are detected. The system also initiates post-trip actions or engineered safety features to ensure the safety of the reactor as it shuts down and continues to monitor and operate when fully shut down. Its reliability is therefore of paramount importance.

Some designs have a diverse protection system or other supporting safety equipment, with different sensors and different actuations to accomplish the shutdown and post-trip or ESF functions.

Normal practice is for the logic to require at least any two out of four channels detecting that a partial trip condition exists to cause an action. Other logic arrangements can be used. Maintenance activities can isolate one channel using interlocks with identification of its bypassed state appropriately.

All nuclear power plants should include an automatic reactor protection system which should initiate a controlled shutdown if reactor conditions pass limiting safe values. It should ensure that the likelihood of radiation hazards to the public and plant are below acceptable limits.

The protection system should operate automatically for all faults, without the need for operator action, for a period of 30 min.

Exceptions from automatic operation of the protection system in response to a fault should be justified, based on formal criteria which include:

a) potential consequences for plant safety (i.e. the safety risks are acceptable); and

b) demonstration that the plant transient develops slowly enough for the operators to assess the situation before having to take action, without needing a safety claim on their actions for at least 30 min.

The reactor protection system includes the automatic protection system logic, its sensors and interfaces to actuators, and should provide the following safety functions:

1) the nuclear reactor trip and emergency shutdown;
2) a safety power cut-back on some reactors;
3) safety interlocks, such as to prevent unacceptable control rod movements or unacceptable plant configurations; and
4) initiation of ESF actuations for water reactors or post-trip sequences for AGRs.

Protection systems should be designed to ensure that maintenance does not result in loss of the protection function.

The protection system and its support features should conform to the SFC (see **3.1.14**). The protection system should provide redundant channels of protection (typically called guard lines) which are mutually isolated and separated such that plant hazards, e.g. fire in a single cable or equipment separation group, cannot disable the protection provided.

The reliability of the protection system equipment and its technology should be assessed in order to determine the need for diversity of protection methods, which can be by separate equipment, separate sensors and actuation, or by support from equipment that is not typically used for safety. As far as practicable, the failure of all components of one type and design should not prevent operation of the associated safety function.

The need for diversity of equipment, functionality, actuation or protection methods within the protection system, and the provision for a secondary shutdown system or for back-up protective actions or systems, should be determined through the reliability assessment (see **4.8**), estimated frequency of reactor faults and probability of failure to provide protection.

The reliability assessment should determine the routine intervals for test and maintenance.

The protection system should also include redundant sensors feeding safety monitoring units (e.g. trip amplifiers) which in turn provide logic signals for each partial trip state, operating on a majority decision voting basis to detect each PIE in a redundant manner. The partially detected states should be voted by safety logic units to detect that a protective action is needed, which in turn should cause a safety actuation to take place.

The voting method should provide an optimum balance between safety and the avoidance of spurious trips due to sensor or other I&C failures.

When intertripping is required between the reactor protection system and other plant systems, e.g. a diverse protection system or the main turbine trip, the two tripping systems should be electrically isolated so that failure of one cannot cause failure of the other to provide protection.

5.1.3 Engineered safety features and post-trip sequences

*COMMENTARY ON **5.1.3***

*The ESF and post-trip sequencing functions fall within level 3 of the defence in depth (see **4.7**).*

The ESF plant and its actuations should provide defence against faults in addition to and in support of the methods of tripping the reactor.

NOTE 1 When the reactor is tripped, the cooling of the reactor is typically reduced in a controlled manner with margins to prevent a reactor criticality due to negative reactivity temperature coefficient effects as the coolant and reactor temperature reduces.

The emergency feedwater pumps feeding the steam-raising systems should be initiated when the main feedwater is reduced or lost at a trip.

The emergency electrical supplies should be started with a load shedding and re-loading sequence if the plant electrical supplies fail.

For water reactors, these sequences should form part of the third level of the defence in depth of the reactor in order to bring the reactor to a safe state even if it is not successfully tripped.

For significant faults on water reactors, e.g. a LOCA, a safety injection sequence should be initiated to provide emergency coolant injection to the reactor, and if necessary, to isolate containment and initiate containment protection.

NOTE 2 Operations to cause reactor containment isolation, and to start containment hydrogen recombiners or electrical supplies, might be required to prevent radioactivity or other hazards arising.

5.1.4 Relationship between the safety system and other I&C systems

The safety system functions should be independent of reactor control functions and those of other I&C systems.

The safety system should be designed to ensure that no action, failure or combination of failures in the control systems could lead to a situation in which protection is not provided.

NOTE A measurement system can provide inputs to both the protection system and a control system as long as failure of the measurement function cannot cause a transient due to loss of the control function and result in failure of the protection against that transient. The use of a sensor for control that is also used for protection could cause an unsafe state if (for example) the sensor fails low and a controller continues to raise power to meet a demand value. Unless suitable measures are adopted, the failed sensor signal might not initiate the safety action. This condition has been experienced on a nuclear plant.

Protection system failures should not affect the control systems in a way that could increase reactivity.

In all cases, the safety action should have priority over any other control action.

5.2 Automatic control systems

*COMMENTARY ON **5.2***

Automatic control is provided to maximize plant efficiency and availability and to reduce operator workload during operation at power and reactor start-up. The use of digital or computer-based equipment for automatic control can have advantages of providing an integrated control function for the plant, with the potential for automation of some start-up and load changing operations.

In normal operation, automatic control maintains plant conditions within defined safe limits to reduce demands on protection systems, maximize plant efficiency and maximize the fatigue life of major plant components. An automatic control system contributes to safe operation by reducing the initiating frequencies of some potential faults, by restricting initial conditions for transients to those assumed in the fault analysis and by contributing towards fault mitigation. In relation to a specific PIE, reactor control systems might therefore perform functions that equate to levels 1, 2 or 3 of the defence in depth for the reactor. For any specific PIE, however, such systems would be expected to contribute to one level only of the defence in depth.

Generally, the overall plant control scheme is based on a "reactor follows turbine" control approach. With "reactor follows turbine", a load demand is set in the turbine load control system and the other control systems follow the turbine control system's lead. Some designs have used "turbine follows reactor", where the turbine accepts the power the reactor generates.

Automatic control systems should typically be provided for:

a) reactor power;

b) steam generator or boiler conditions;

c) secondary coolant feed water flow; and

d) turbine load.

They should be independent of protection systems and have sufficient redundancy to prevent loss of automatic control or loss of generation on failure of a main control module or a single power supply source.

Continuous control systems should be designed for bumpless transfer between modes of control. They should have interlocks to prevent incorrect engagement of automatic control.

The automatic control systems should be interlinked to provide a coordinated response to changing load demands. The automatic control systems should have controls, indications and alarms to:

1) allow manual control;

2) allow transfer between modes of control;

3) enable a control system demand value to be set, checking the value is acceptable;

4) monitor process variables under control;

5) monitor that the position of process control actuators is correct; and

6) alert operators to control system failures.

Automatic control of emergency feedwater should operate after any reactor trip.

5.3 Main control room and supplementary control room

5.3.1 Control room systems

*COMMENTARY ON **5.3.1***

The MCR provides a centre for all normal and emergency operation of all control functions except those that involve maintenance. It typically allows start-up from a cold prepared state of plant to full power, and shutdown for normal and fault conditions. The MCR typically includes mimic panels or displays with controls over the electrical distribution system. Normal practice is to have selection at or close to plant or switchgear for local-to-plant or for remote control from the MCR, for all plant actuations.

The SCR provides the means to shut down the reactor and confirm its state if the MCR cannot be used. Controlling fault situations from the SCR is not normally required, depending on the safety analysis regarding the probability of such situations arising coincident with use of the SCR. The use of local control points can be included in the functionality of the SCR facility if required.

A MCR should be provided for coordination of operational, safety, maintenance and control functions, including facilities for controlling the reactor and associated plant.

Operation of the automatic safety system in any way should be indicated in the MCR.

The location of the MCR and the layout of its facilities should take account of typical plant operation and of the actions and procedures necessary to deal with faults which might arise during the life of the reactor. A detailed task analysis should be carried out for major operations and potential faults requiring operator action. This analysis should be used for generating operating procedures.

For circumstances where the MCR might become inoperative (e.g. due to damage) or become uninhabitable (e.g. due to smoke) a supplementary control room (SCR) should be provided to ensure that safe shutdown can be achieved.

The design of both MCR and SCR should ensure that a safe shutdown is achievable and can be confirmed, even if a severe CCF or power failure disables all control methods that rely on a single technology.

The location of the MCR and SCR should be separate to ensure that no design basis hazard or event renders both MCR and SCR inoperative at the same time. Access to both the MCR and SCR should be protected from adverse environmental conditions, e.g. excessive radiation, toxic gases.

There should be facilities in locations separate from the MCR and SCR for technical support, operational support and on-site emergency response functions.

The number, function and status of personnel attending to the plant and the means of communication to coordinate their activities should be determined.

5.3.2 Information and soft control systems

*COMMENTARY ON **5.3.2***

An extensive computer-based information system is typically provided on nuclear plants, with input from measurement sensors and contact states, and computer processing to provide displays and records. The processing provides legends for the exact identities of each measurement and alarm. The system provides computer displays of measured value and alarm conditions, and can also provide directly driven instruments and alarm screens.

Some plants have implemented soft control in the MCR, in which computer displays show the state of the plant or a control system, with on-screen actions used to initiate the operation of plant actuators, to alter control system demands or change control modes.

A comprehensive information gathering, recording and display system should be installed to monitor the plant. It should gather sensor readings to monitor plant conditions and the states of plant, switchgear and electrical supplies, and to detect and present alarms. The information system should also be able to provide records for analysis after any plant trip or major disturbance.

The information system should have redundancy to ensure that all information necessary to monitor the reactor remains operable notwithstanding failures of single modules of the information gathering equipment or of a single source of power supplied to it. It should have redundancy of its displays and of their controls, with the ability to provide any of its information on all displays.

The information system should be able to:

a) detect abnormal states and provide alarms to the operators;

b) provide extensive displays of information covering both measurement values and alarm states and histories; and

c) process the states and conditions it detects to identify significant alarm conditions.

Instruments should directly display the required parameter of interest whenever possible, and when it is not possible, the operators should be made aware of which substitute parameter is being displayed, the relationship of the displayed parameter to the parameter of interest, and the uncertainties introduced as a result of using a surrogate parameter.

The information system should include a system specifically designed for emergency conditions. It should have measurements, processing equipment and displays that can withstand conditions arising from design basis accidents including a seismic disturbance. The system design should include means of integrating signals from all I&C sources, including the safety instrumentation of the protection system and other operational instruments.

NOTE The emergency information system on different plants has been given names of similar function, such as safety parameter display system (SPDS), post-accident monitoring system (PAMS) or safety information display system (SIDS).

Soft control functions should include a defined sequence of select, confirm and initiate for each actuation. The displays used for soft control should include the measurements of state or value over which control is to be taken. They should include suitable support states and measurements to be used by the operators to confirm correct actions have occurred, with indications of abnormality and actuator failure. Where automatic control functions are operated, the associated displays should show demand and actual plant values, with demand values, including acceptable limits.

5.4 I&C support systems

5.4.1 Guaranteed power supply systems

*COMMENTARY ON **5.4.1***

Direct current supplies, which are supported by batteries, are the most reliable form of guaranteed electrical supply. Where several different power supplies influence the operation of a system, it cannot be ensured that all fail simultaneously. In such cases the supplies can fail in unanticipated sequences that might defeat the intent of the system's fail-safe design.

Possible failure sequences of power supplies should be determined in the design of safety systems required for design basis accidents and design extension conditions.

Where I&C equipment requires a guaranteed power supply, the supply source should be battery supported.

The power supply system design should ensure that:

a) provision is made for multiple independent separated power sources;

b) the power source and supply distribution system for the reactor safety system meet the single failure criterion;

c) transient disturbances including switching, fuse failure, lightning strike and faults do not affect the safety or operation of the plant;

d) the power supply capacity maintains the instrumentation and safety system loads for a period of time in accordance with the design basis requirements; and

e) alarms are provided to warn the operator of any malfunction of power supplies which could affect reactor safety or operation.

5.4.2 Instrumentation power supplies

*COMMENTARY ON **5.4.2***

Under emergency conditions it is much easier to restore power and control to d.c. systems and single-phase a.c. systems than to complex a.c. systems.

The power supply should ensure a simple but redundant structure.

The power supplies to plant instrumentation and the safety system should ensure that the reactor maintains operational protection, control and monitoring functions at all times, even when the reactor is shut down.

5.4.3 Pneumatic and hydraulic power supplies

Pneumatic and hydraulic power supply systems should ensure a simple but redundant structure. Where pneumatic or hydraulic power supplies are used, they should conform to relevant IEC and ISO standards (see Annex A).

The layout and construction of the power supply system should be such that mechanical failure of any component cannot cause damage to the reactor plant.

Fluid contamination which might adversely affect the performance of equipment powered from pneumatic or hydraulic supplies, e.g. water in pneumatic or hydraulic fluids, should be prevented.

For operation of valves of high safety importance, reservoirs should be provided which enable a predefined number of valve operations upon loss of the pneumatic or hydraulic supply system power. The minimum reservoir capacity should be for at least two complete operations remaining on loss of electrical power or loss of ability to pressurize the system reservoir.

Containment isolation valves should adopt a preferred safe state on loss of power or operating medium.

Alarms should be provided to alert the MCR to partial loss of pneumatic or hydraulic supply system pressure. Instrument air systems for air-operated valves required for design basis accidents and design extension conditions should be capable of operating the valves for an extended period without depending upon plant electrical power or other plant support systems.

5.4.4 Communication systems

*COMMENTARY ON **5.4.4***

Normal practice is for the plant to have an internal telephone system, a direct wire telephone system, radio systems for off-site communications, with a public telephone, and a PA system for the entire plant. The centre for these systems is the MCR. The telephone links can be arranged to have handset redundancy with different access codes. In addition, internal fire alarm, emergency and radiation warning alarm sounds are provided at all locations. Provision is made for communication to the technical support centre and also any emergency response centre, with redundant channels and power supply support.

Robust back-up communications and status reporting methods should be established and practised to ensure safe and correct operation of the plant during design basis accidents and design extension conditions.

Two independent means should be provided for each required type of communication.

The communication system should enable information and instructions to be transmitted between manned locations throughout the plant, and provide external communications with fire, ambulance and police services.

The telephone communication system should be based on automatic exchange telephone systems. An alternative independent and physically separated telephone channel, and also a radio system, should be provided to ensure communication during emergency conditions.

For limited range communications within the plant area, direct line telephones or intercom systems should be used as an alternative communication system.

The control room personnel should have priority use for selected communication channels during emergencies. The layout of controls and design of communications systems in the control locations should allow control room operators to communicate with field operators where necessary.

NOTE An open intercommunication system, where all messages are heard at all locations, enables a faster response in emergencies.

The number of warning sounds in the MCR should be limited to four separate tones or sounds, including telephones.

There should be warning sounds for excess radiation, fire, emergency, etc., which are audible at all plant locations, to warn personnel of hazards.

All normal communication should be via the MCR and therefore the viability of an alternative communication centre should be determined to allow for damage to the MCR or situations where the MCR becomes uninhabitable.

A PA system should be used.

6 Reactor and plant instrumentation

6.1 Sensors and actuators

6.1.1 Sensors

*COMMENTARY ON **6.1.1***

A typical plant includes many temperature sensors, neutron flux detectors, level and limit switches, auxiliary contacts on switchgear and relays, position measurement devices, pressure sensors used for direct pressure and for level detection from differential pressure, and flow measurement using differential pressure across an orifice. Many specialist instrument types can be used, such as transit time flow measurement, chemical concentration instruments, moveable flux chambers or self-powered neutron flux detectors.

The number and positioning of the sensors installed should ensure continuous monitoring of plant conditions, allowing for failures of some sensors during operation.

Sensors should have short- and long-term compatibility with their environmental conditions, including temperature, humidity, vibration, noise, lighting, radiation, etc., in order to minimize potential measurement errors and physical deterioration.

Sensors should be suitably qualified and be able to provide measurements in the worst conditions of spatial and temperature distortions at their locations to ensure that the reactor protection system is not prejudiced. As such, sensors located in areas potentially subject to high radiation levels should be constructed from materials that can withstand prolonged irradiation. Electrical insulation should not become degraded.

Instrument channels should be regularly checked as part of surveillance procedures to ensure that failures can be detected before the overall measurement function is disabled.

NOTE 1 Typically, redundant channels are needed to accomplish this.

If sensor locations are changed, e.g. to account for different operating conditions, the new location should be based upon analysis that confirms this location is suitable for measuring the variable of interest and that the measurements to be made are within the capabilities of the instrumentation.

Sensors monitoring the coolant circuit should be securely fixed and not interfere with access for any internal inspection work on the coolant circuit. Those parts of the sensor system (both permanent and temporary) which are in contact with the coolant should be constructed from materials compatible with the coolant itself and with other materials within the coolant circuit.

The location of sensors in the plant fluid systems should ensure measurement errors due to adjacent pipe connections or other features are avoided. Fluid flow effects should be determined in the positioning of sensors.

The number and location of sensors required to measure variables having spatial dependence should have a clear basis that addresses all operating modes in which the information is needed. The interactions between plant design and instrument application should be determined.

Vibration and loose-parts monitoring systems should be installed to assist in preventing accidents due to failures within the core or the reactor cooling system.

NOTE 2 Vibration and loose parts monitoring systems typically depend on acoustic sensors mounted on the pressure vessel and main coolant pipework under the thermal insulation and arranged, using computer processing, to give coverage of the internals of the reactor.

6.1.2 Actuators

*COMMENTARY ON **6.1.2***

Normal practice is for actuators to be provided in association with the mechanical plant, with the initiation of an actuator and its control to be part of the I&C systems. The interface to switchgear is typically made by 50 V d.c. auxiliary relays, controlled by MCR switches or by multiplexer outputs operated from the MCR by switches or by soft control methods, with monitoring of the switchgear state adopted using auxiliary contacts.

The I&C system should provide outputs to switchgear, valves and pneumatic or hydraulic systems which initiate and control the actuators for protection and control actions. The actuator interfaces in switchgear should provide feedback signals to the initiating system or control room switch, module or displays that indicate the state adopted.

Actuators for control rod movement and for continuous control valves such as the main feedflow control system should provide a position feedback signal to ensure that the actuators are monitored by the control system.

The I&C actuator interfaces should provide indications to the control room that the plant item is under local control or in a maintenance or test mode at the plant area.

6.2 Control rod position

*COMMENTARY ON **6.2***

Control rods are typically operated in several groups or lifts, moved out of the reactor in sequence at start-up, but all inserted directly at a reactor trip. Control rods which are out of alignment with others of the same lift or group create asymmetric flux profiles which can be significant reactor faults requiring a reactor trip.

Neutron absorber material is included in most designs at selected core locations to ensure suitable flux profiles and patterns exist. They do not typically have installed instrumentation and rely on administration and the flux profile measurements to ensure correct positioning.

Control rod position is an important measurement required for safety and operation. Failure of a rod to insert at a trip reduces the shutdown reactivity margin. Failure of many rods to trip is a severe fault, although some designs are able to overcome this. Dropping or insertion of a single rod at power can cause severe flux distortion.

A single group of control rods is typically used for adjustment of reactor power or reactor outlet temperature under automatic control, which uses position in its action.

Control rod position is measured by various methods. These include digitizing discs on the control rod drive motors, potentiometers, linear transformers and control rod drive pulse counting methods. Limit switches can be used to detect that each control rod is fully inserted or fully withdrawn, independent of the sensing of intermediate positions.

The position of all control rods should be measured. Position detection for a dropped or fully inserted control rod should be provided.

Measures should be provided to detect an individual control rod that is out of line with other related rods, or has failed to enter the core, or has entered the core when others have not.

The failure of a control rod or of several control rods to insert into the core at a reactor trip should provide a signal to the reactor protection system to initiate back-up methods of reactor shutdown.

6.3 Switchgear and valve position

*COMMENTARY ON **6.3***

The position of valves and switchgear and some tank levels are monitored by limit switches, level switches, and contactor or switchgear auxiliary contacts. These operate indicating lights and alarms, or provide computer information system inputs for alarms and plant state displays.

Normal practice is for discrepancy switches to be used with open/close (or similar) demand actions made by overthrow of the switch from normal positions that monitor the normal state of open or closed. Indicating lamps show valve in movement and valve or switchgear in a different state to the control switch position.

Some throttle valves, and the gas circulator inlet guide vanes on AGR, are provided with position measurement for the intermediate positions of the item. The valve position and state are important for main steam line stop valves, main turbine and feedpump turbine throttle valves and pressurizer relief, power-operated valves on PWR.

Switchgear and valve positions are important for the reactor protection system operation. The detection of loss of electrical supplies, turbine trip, spurious valve operation, and of various tank levels for critical coolant systems depends on such switch and valve position detection. The operation of automatic control systems depends on feedback of the position of the actuators used in control to detect that each movement demanded takes place and to detect failures of movement when demanded.

The position of valves should be monitored or measured to detect states of open or closed, and for regulating valves, their intermediate positions and states. The state of pumps, switchgear and contactors should be monitored to indicate running or stopped, open or closed, or equivalent states.

Alarms or signals to the information system should be generated from position detection, where the position is incorrect in relation to the demand or when the position changes due to automatic or plant protection actions.

The state of valves and of switchgear should be combined in suitable logic with the state of the control switch concerned, in order to indicate that the actual state is different from the demanded state. In some cases this should indicate that a valve is being moved by a control action or an automatic sequence is operating the valve or item, such as safety injection on a PWR or the post-trip actions on gas circulators for AGR.

6.4 Neutron flux measurement

*COMMENTARY ON **6.4***

Neutron flux measurement is an essential requirement for reactor protection and control and for monitoring plant power production and safety. Neutron flux detectors can therefore be used to give fast response signals of reactor power for indication, control and protection.

Neutron flux is measured to provide immediate information about current fission power and thereby to permit rapid action against unexpected reactivity transients. Many fault conditions cause excess flux or rapid rates of rise of flux that require protective action. It is essential to measure flux from the long-term shutdown (source) level to the highest possible magnitude which can occur. This ranges from watts to several thousand megawatts on a power plant, to be covered by more than one echelon of sensors.

When a reactor is shut down, installed neutron sources are typically used to provide a flux equivalent of approximately one watt to enable the correct performance of source range detectors to be confirmed, as the flux in a core of new fuel could fall to a level at which it cannot be correctly monitored.

The neutron flux within a nuclear reactor is nominally proportional to the power produced by fission and should be monitored at all times, even when shut down.

Neutron flux measurements should also be used to determine power distribution across the reactor and to assess fuel burn-up.

The core and any neutron sources should be designed to ensure that instrumentation displays provide a reactivity assessment before the nuclear reactor becomes critical.

The measurement of neutron flux should cover the full range for which control and protection is required, e.g. zero power to 200% design power, with sufficient over-range to allow for design basis excursions in power. Where two different measurement channels are used to achieve this, they should provide a range overlap with a controlled and interlocked method of changing from one to the other.

More than one type of the following measurement channels should be used to measure the neutron flux for the full power range:

a) source range, which is typically a logarithmic flux channel;

b) intermediate range, which is typically a logarithmic channel or other detector type; and

c) power range, which is typically a linear channel.

NOTE 1 Typically, two of these channel types could be incorporated into a single unit. Cambelling channels and other detector types are also used.

NOTE 2 Other flux and radiation-based measurement systems could be provided to assess flux distribution within the reactor core and provide diverse measurement of reactor power.

6.5 Temperature measurement

*COMMENTARY ON **6.5***

Temperature measurement on nuclear reactors, their fuel, coolants and their components is an essential requirement for the reactor protection system and for the safe operation of the plant for the production of power. Many faults cause excess temperature that can be detected by the protection system.

Mineral insulated thermocouples and RTDs are typically used for reactor temperature measurements.

Maximum temperature detection for a group of fuel channel outlet temperature measurements and rate of change limit trips might be necessary.

6.5.1 General

Temperature should be measured in the reactor for protection, performance, optimization, control and monitoring.

Temperature trips used for protection should have representative measurement positions, selected and used solely for this purpose.

Automatically-adjusted trip levels within an accepted range, or rate of change limits, should be used where acceptable temperatures vary significantly over the reactor operating range.

When temperature is monitored from sensors in the coolant circuits, the coolant flow should be sufficient to ensure that the temperatures are representative of the coolant condition.

When temperature measurement is provided by thermocouples, compensating and extension cables of suitable materials and cold junction compensation should be used to ensure that measurement errors are acceptable.

6.5.2 Coolant outlet and fuel channel outlet temperature

*COMMENTARY ON **6.5.2***

Fuel temperature is an essential measurement for the protection system and to initiate alarms. Some reactor designs measured fuel temperature by direct measurement of fuel can temperature. Most designs infer temperature when this is needed from the coolant temperature in the fuel channel exit. Excess fuel temperature can result from many faults. Channel outlet temperature measurements have been used to control reactor radial temperature and flux distribution and channel power in gas cooled reactors by control of individual fuel channel coolant flows and by control rod movement.

Reactor core inlet and outlet temperatures should be measured, taking account of heat transfer characteristics at the measurement position. The range of coolant flow over which temperature measurements are valid should be determined.

The measurement of channel coolant outlet temperature should assess the radial temperature distribution in the reactor.

NOTE Channel outlet temperature is used in association with fuel burn-up assessments.

When fuel temperature measurement is required, it should be derived from measurements in fuel channels. Fuel temperature can indicate either directly or indirectly that safe levels are not exceeded and should be used for detection of single and multiple fuel channel faults.

When assessing fuel temperature, the time lag between indicated temperature and actual fuel temperature should be consistent with acceptable measurement errors, as stated in the design basis.

6.5.3 Gas cooled reactor temperature

For all gas cooled reactors, the temperatures of reactor internal structures, including core support structures, should be measured to ensure that they are within acceptable temperature limits.

For gas cooled graphite moderated reactors, the moderator temperatures should be measured to provide information on the structural integrity of the moderator.

For gas cooled reactors with concrete pressure vessels, the pressure vessel temperatures and its coolant system should be monitored to ensure that the vessel concrete conditions are within acceptable limits.

6.6 Containment monitoring

*COMMENTARY ON **6.6***

Containment constitutes the last barrier to the release of radioactive material to the environment.

Conditions within the containment are monitored to detect failure of the reactor coolant pressure boundary and to establish the levels of radioactive material that have passed into the containment atmosphere.

Changes of pressure within primary or secondary containment should be monitored for safety.

Radiation and moisture levels in the containment of a water cooled reactor should be monitored to detect possible leaks of the reactor coolant.

Radiation in the containment should be monitored to determine the extent of damage to the fuel upon major breach of the reactor coolant pressure boundary.

Hydrogen concentration should be monitored for accident conditions where fuel/coolant interaction takes place and used to initiate hydrogen recombiners.

The position of all containment isolation valves should be monitored.

6.7 Coolant conditions

6.7.1 Coolant temperature

*COMMENTARY ON **6.7.1***

The safe removal and efficient utilization of the nuclear heat from the core depends upon a supply of coolant and its temperature and pressure. Excessive coolant temperature or rate of rise or fall of coolant temperature can be a PIE. These measurements are therefore essential for the reactor protection system, the plant control systems and the monitoring systems needed by the operators.

In all nuclear reactors, coolant temperature should be monitored for safety.

The bulk coolant temperature at reactor inlet and outlet should be measured to ensure reactor protection and control, and should be displayed in the MCR.

The time lag between indicated temperature and actual temperature introduced during transients should be consistent with acceptable measurement errors, as stated in the design basis, and cover the operational range of coolant flow.

The range of coolant flow over which temperature can be correctly measured should be determined.

6.7.2 Coolant flow

*COMMENTARY ON **6.7.2***

The maintenance of sufficient coolant flow is necessary to ensure heat removal from the reactor. Detection of loss of coolant circulation is therefore essential for reactor protection.

Coolant circulation control devices include pumps, circuit isolation valves, inlet guide vanes and their motors.

The coolant mass flow in each coolant circuit should be monitored to ensure reactor protection and should be displayed in the MCR. Coolant circulating pump conditions should be displayed.

The method of coolant flow measurement should be the most direct possible and should indicate coolant flow over the whole operating range from shutdown and low power to full power.

The coolant flow measurement should allow detection of flow variation due to both pump or circulator speed variation and valve or gas circulator inlet guide vane movement.

If the flow or motor power varies outside acceptable limits, including loss of pump or circulator power, alarms and corrective action should be initiated from a measurement of flow or by signals coming directly from the device which causes the flow variation.

The consequences of a reversal of coolant flow should be determined, with warnings and, if necessary, protection provided.

On nuclear reactors where individual main coolant circuits are isolated, the flow failure protection should ensure that reduced power operation is possible.

6.7.3 Coolant pressure

*COMMENTARY ON **6.7.3***

The pressure of the primary coolant is an important measurement for the safety of most reactors. Loss of coolant pressure or excess pressure are faults requiring protection as they involve loss of the capacity to remove heat from the reactor. At low temperature during shutdown, the correct balance of coolant temperature and pressure is required to prevent the possible brittle fracture conditions of steel vessels. The pressurizer on a PWR is monitored for pressure, as rate of change of pressure is important for detecting loss of coolant. The coolant pressure of an AGR is monitored to detect hot gas release to the pile cap and annulus areas and initiate safety actions.

To ensure cooling, the pressure of the coolant should be maintained within limits appropriate to the operating power level. The coolant pressure should be monitored to detect unacceptable changes of coolant pressure due to breach of the coolant boundary, loss of coolant, etc.

For water cooled nuclear reactors, the reactor coolant pressure and its rate of change should be monitored by the protection system to detect a LOCA.

Coolant pressure measurements should be used to ensure correct conditions prior to bringing an individual coolant circuit into service. This should allow for interlocks and safety actions where an auxiliary coolant system is rated at a lower pressure than the normal pressure of the reactor at power.

6.7.4 Coolant level

For water reactors, the coolant level in the reactor vessel should be monitored, allowing for the effect of both normal coolant flow and design extension conditions.

In reactors where the coolant is used as a radiation shield, instrumentation should indicate that a safe level of coolant is maintained.

Where storage tanks provide a cooling water reserve for use under emergency conditions, the level of stored water should be monitored and warnings provided if the water level drops below safe levels.

On a PWR, the coolant level in the pressurizer should be monitored for the minimum and maximum levels, in accordance with the design basis, to ensure reactor protection.

6.7.5 Coolant purity and composition

*COMMENTARY ON **6.7.5***

Coolant chemical dosing is used to control chemical reactions between the coolant and the materials in contact with it. Coolant composition measurements can be arranged to monitor the products of the reactions between the coolant and the remainder of the coolant system. This information can then be used to indicate that the components of the coolant system are in good condition. Coolant water chemistry control is of great importance in controlling boiler life. Monitoring of coolant concentration of oxygen, methane and carbon monoxide is needed on AGRs. Extensive monitoring of additive concentration is needed on PWRs to control steam generator or boiler tube conditions.

When additives are added to the reactor coolant, the chemicals and bulk coolant should be measured to ensure that they are of the correct composition.

Coolant purity should be measured by either manual or continuous sampling, depending upon the speed with which unacceptable conditions could develop.

On water cooled nuclear reactors, coolant boron concentration (boric acid) should be monitored to ensure sufficient shutdown margin and to control reactivity during load shedding with xenon reactivity poisoning and any later return to power.

NOTE Water cooled reactors typically add and remove boric acid to the coolant to control reactivity. Boric acid injection systems are included to ensure a sufficient shutdown margin, and can be initiated by the safety system.

6.7.6 Coolant leakage

*COMMENTARY ON **6.7.6***

On water cooled reactors, minor leaks from the coolant circuit, which are too small to be detected by the pressure instrumentation, could develop.

If there is a likelihood of coolant leakage, a coolant leak detection system should be installed, taking into account detection of the toxic or radioactive nature of any coolant leaks. This should employ chemical or radiometric sampling external to the coolant circuit, or, where appropriate, a record of the rate of coolant make-up.

On an AGR, temperature detection of the reactor annulus and pile cap, and rate of change of reactor pressure, should be used to detect the release of hot coolant to the atmosphere and initiate a safety system action.

6.7.7 Coolant activity

The bulk coolant activity should be monitored to detect fuel failure. AGRs should monitor individual fuel channels in order to locate fuel elements with faulty fuel cladding.

7 Secondary circuit, turbine and electrical systems

7.1 Secondary coolant circuit measurements

*COMMENTARY ON **7.1***

The conditions of the steam generators or boilers are important to safety as they show that sufficient cooling is being provided to remove heat from the reactor. Faults that require protection of the reactor or the boilers can involve measurements of the boiler secondary coolant level, the boiler tube temperatures, and the feedwater flow to the boilers.

The protection system on pressurized water reactors should monitor the steam generator level and the steam and feed flow to ensure heat removal from the reactor.

Steam pressure should be measured by the protection system and provided with a rate of change limited trip to detect loss of secondary coolant or spurious closure of a main steam valve and to initiate suitable protection.

To control boiler tube erosion, the level at which boiling begins in once-through boilers on AGRs should be controlled by monitoring boiler tube temperatures.

7.2 Condensate measurements

The secondary coolant activity of the condensate on a PWR should be measured to detect leakage of primary circuit coolant to the secondary coolant (SGTR) and to provide warnings to the operators.

7.3 Emergency feedwater flow measurement

The emergency feedwater flow should be measured and displayed in the MCR by a specific set of transducers designed for that flow level, and should be able to withstand the higher pressure at their orifice plate (or its equivalent) at full values of feed pressure and flow.

7.4 Turbine stop and throttle valve conditions

The status of each main turbine should be monitored to provide signals to the protection and the control systems to ensure required automatic actions.

NOTE A trip of the turbine might, typically, require an intertrip of the reactor. The stop and throttle valve conditions are used by the control systems.

7.5 Electrical system measurements and controls

The turbo-generator output electrical power and frequency, and the main circuit-breaker positions of the station switchgear, should be monitored to provide indications of generated power and connection status of the station electrical systems in the MCR.

The status of the main grid connection of the plant should be controlled and displayed in the MCR. Depending on the design, loss of grid connection should initiate:

a) power reduction to “house load”; or

b) reactor trip and the associated safety system actions, as appropriate.

The connections of the station electrical systems should be controlled in the MCR, including associated displays for the arrangement of distribution boards, feeders, interconnectors and transformers.

The MCR should have provisions for control and operation of the station emergency supplies, their batteries and diesels or other generator power sources.

Operation of the emergency electrical generators by the protection system should be indicated in the MCR.

8 Design recommendations

8.1 Systems dependent on computer software

*COMMENTARY ON **8.1***

The use of software in safety systems in UK nuclear power plants can provide many benefits to the operation and control of the plant systems. However, the licensing of these safety systems has been problematic, as the technology can be complex and its reliability cannot be determined by traditional methods.

The overall I&C architecture needs to specify and select the individual I&C systems that together constitute the overall I&C architecture. The selection of the technology to be used in each of these I&C systems is a key decision that can have serious implications for all aspects of the programme. Attention is drawn to the Nuclear Safety Technical Assessment Guide *[2] to assist in gaining such an understanding. See also Annex A for IAEA and relevant safety standards.*

8.1.1 General

Computer-based safety systems should be designed and documented to ensure that the assignment and execution of I&C functions are clearly traceable and that any potential interactions between functions can be identified. In common with all safety systems, computer-based systems which implement functions of lower safety significance should not be able to affect systems which implement functions of higher safety significance.

Computer-based safety systems should be designed to minimize the potential for CCF by the implementation of a diverse system and other forms of diversity (e.g. hardware, design of software and its implementation).

NOTE 1 Attention is drawn to the Office of Nuclear Regulation's Nuclear Safety Technical Assessment Guide *[2] for the design and licensing of computer-based safety systems for nuclear power plants.*

NOTE 2 The precedents established in the UK have shaped the regulatory expectations of the ONR and these are contained in a Nuclear Safety Technical Assessment Guide *[2]. The relevant principle presented in the* Nuclear Safety Technical Assessment Guide *[2] is reproduced below. The key recommendations of this guide are then summarized.*

"Where the system reliability is significantly dependent upon the performance of computer software, the establishment of, and compliance with, appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of production excellence and confidence-building measures."
*(*Safety Assessment Principle *ESS.27 [2])*

The design, V&V and production processes for the computer-based safety system should provide robust evidence of both production excellence and confidence building in order to ensure a multi-legged approach.

Modifications to digital system software, including configuration data, should be verified and validated before being placed into service.

Computer software should include robust protection to ensure spurious, unauthorized or malicious software cannot be included or introduced into any system depending on software.

8.1.2 Production excellence

The evidence of production excellence should cover the total life cycle, from initial specification through to operation, and should comprise all of the following elements.

a) Best practice should be used for the design, development and V&V activities. Particular attention should be given to the definition and management of the requirements and the configuration control of the software design. National and international standards should be used to ensure the application of best practice (see Annex A).

b) A quality assurance programme and plan meeting appropriate quality assurance standards should be implemented (see Annex A).

c) A comprehensive testing programme should be undertaken to detect errors in the design as well as confirming system functionality. The V&V activities should be undertaken by personnel who are independent from the specification and design activities.

d) A programme of dynamic testing should be performed on the computer-based safety system to demonstrate that the system is capable of meeting its reliability requirements.

8.1.3 Confidence building

Confidence building should consist of a comprehensive and independent assessment of the functionality and performance of the computer-based safety system, including a review of precedents. The following activities should be undertaken to provide suitable evidence.

a) A complete check of the final, validated production software should be undertaken by a team that is independent of the system's supplier or suppliers. This should include a detailed and searching analysis of the software, using static analysis and other suitable methods. In addition, an independent review of the complete design and production process should be carried out to check that the product meets the specification and that the tools and methods employed have been correctly applied.

b) An independent assessment of the test programme should be undertaken. This should cover all test phases and include a review of the traceability of the requirements through the design, development and production stages.

8.2 Reactor protection system

8.2.1 General

The reactor protection system, including its circuits, components and equipment should be of a fail-safe design to ensure that failure of the power supply or any component or an open or short circuit automatically initiates the protection system partial trip or actuation state of that part of the system.

Self-monitoring and dynamic operation features should be identified and included in order to underpin this design principle.

NOTE 1 Equipment for protection is typically operated by signals that cycle continuously between two conditions, and failure to cycle is used to indicate failure of the equipment. Alternatively, self-monitoring methods such as message parity and cyclic redundancy checks can be used. Equipment is used in some designs to inject test signals and confirm correct action, by connection at routine maintenance intervals.

NOTE 2 There might be exceptions to a simple fail-safe approach for some ESFs, such as to close steam valves, for which spurious closure of one valve alone might be a potential fault.

A detailed safety analysis should be conducted to determine whether an "energize to actuate" approach is to be implemented rather than an "actuate on loss of power" arrangement for each safety action.

The time response of the protection system equipment for each possible protection action should be determined to ensure that the overall safety system, including the mechanical plant, meets the design basis requirements.

The response times and performance assessment of the reactor protection system should allow for analysis tolerances, measurement errors and drift, and determine:

a) component tolerances;

b) instrument accuracy;

c) protection system set points; and

d) possible degradation over time.

For each plant fault, the probability of the protection system not performing its correct function should be calculated and take account of:

1) the type of plant;

2) the predicted frequency of the fault;

3) the hazard resulting from the fault if the protection system fails; and

4) the requirements for maximum permissible frequency and magnitude of any release, and for fuel damage limitation.

The required level of probability of failure to provide protection on demand (pfd) should be identified in the final design basis documents, taking account of practicality and safety in the I&C equipment design, in conjunction with the safety analysis and the requirement to demonstrate to very high confidence the integrity and validity of the software and hardware.

NOTE 3 A similar calculation could be used to demonstrate that the reactor protection system does not reduce the plant availability to below the requirements in the design basis document.

The reactor protection system design should include majority voting arrangements to ensure tolerance of single failures while avoiding loss of availability. The voting arrangements should permit maintenance on only one redundant channel at any one time, and prevent more than one channel being made inoperative.

During any reactor protection system maintenance or calibration procedure, the system should operate correctly in the presence of one failure.

Where changes in plant conditions occur, the set-points needed for the various changes should be established in advance. If the need for changes occurs on a regular basis or if the changes need to be made quickly, additional trip functions, including any operational bypass functions, should be included.

8.2.2 Reactor protection system design

The reactor protection system design should provide the following functionality.

a) Means should be provided for the control of access to all equipment for adjustment of trip levels (when adjustment is justified by the safety analysis) and for maintenance.

b) Facilities should be included to allow all components to be tested and calibrated during plant operation.

c) Equipment and cabling should be clearly and distinctly labelled and protected against damage.

d) Plant operational and maintenance bypasses (vetoes) should be provided only where essential. Where these are provided, they should be under key control, with alarms linked to the MCR.

e) Adjustment of trip setting controls should be limited by design features to permissible levels.

f) Setting of reactor protection system set points should be independently verified and reviewed.

g) Maintenance and test procedures should be designed such that the safety and availability characteristics of the protection system are not compromised.

h) Measured values and states of all protection system signals should be available in the MCR and recorded, using isolators if appropriate.

i) Protection system equipment should be electrically isolated to ensure that if other equipment malfunctions, it cannot cause a safety group to fail. The equipment of each redundant safety group should be electrically and physically isolated from each other safety group, such that messages needed for voting across guard lines cannot prevent a protective action due to failure.

NOTE The separation of cables, I&C equipment and plant is achieved by spatial separation, separate raceways, separation of cable trays (potentially with fire proofing) cable trunking and ducts, and separate cable routes wherever possible. Use is made of separated rooms with fire doors, with rapid acting fire detection and control systems where common areas cannot be avoided, and fire-resistant penetrations where cables are required to pass from one separation group to another. The term "segregation" has been used for this process, but can be ambiguous and "separation" is preferred.

j) A systematic approach to the use of diversity, to provide protection against CCF, should be adopted in the design of the safety system. Where software forms a direct or implicit part of the safety system equipment, an assessment should be made of the use of any common software in protection groups or defence in depth levels of protection for which independence between the groups is claimed.

The associated process for the functionality described in a) to j) should be documented.

8.2.3 Reactor trip and the protection system

*COMMENTARY ON **8.2.3***

The negative reactivity capable of being inserted by control rods or other means, and the timescale over which this takes place to achieve and retain safety at a trip, is outside the scope of this British Standard.

The complete safety system should be designed to allow for potential failures of shutdown mechanisms. Reactor shutdown should occur even if a predetermined small number of control rods fail to insert upon reactor trip.

The protection system should operate its final actuators within a defined period from the trip parameters passing their acceptable levels, in accordance with the design basis (typically less than 1 s).

The actions of the safety system should be automatic and independent of the control system and operator.

NOTE The actions of the safety system include the engineered safety features (ESF) and the post-trip actions.

Once tripped, it should not be possible to reset the system until all variables are at safe levels. Reset should only be possible manually.

A manual trip facility should be provided at the MCR and SCR. The manual trip facility should:

a) interrupt the circuits to the trip mechanisms as directly as practicable;

b) operate to minimize the possibilities of the trip being prevented by a short or other circuit fault (e.g. due to a fire) on the cables and wiring between the manual trip facility and the final trip mechanisms; and

c) allow for separation of the connections of the channels of the safety system.

The safety system should ensure that no single failure, including failure of a single safety power supply, can trip the reactor.

The safety system should be designed so that the operator can determine:

1) that trip levels are correctly set;

2) if any of the channels are in the tripped condition;

3) if any of the channels are approaching the tripped condition;

4) if any maintenance procedures are in progress;

5) the group of channels which caused any trip; and

6) any faults or failures of the protection system equipment.

8.2.4 Safety power cut-back system

*COMMENTARY ON **8.2.4***

A safety power cut-back system is one which automatically reduces reactor power in a controlled manner. It forms part of the defence in depth of the plant by reducing the frequency of challenges to the reactor protection system. Typically this would be achieved by automatic insertion of control rods or by simply preventing further withdrawal of control rods.

A safety power cut-back system should form part of the protection against faults which could damage fuel or release radioactivity. There should be no faults for which a safety cut-back system is the only protection.

8.2.5 Safety interlock system

*COMMENTARY ON **8.2.5***

Safety interlocks, which permit or prevent certain operations affecting reactor safety when prescribed conditions exist, prevent unsafe conditions or loss of availability.

Operational bypasses are safety interlocks which allow the transfer of protection from one instrument range to another as power is raised, under operator control. Maintenance bypasses enable a safety channel to be maintained without loss of plant operation.

The safety interlock system should ensure that:

a) no single failure, including failure of a power supply, prevents a safe interlock action;

b) it is electrically and, where relevant, mechanically independent from all systems outside the reactor protection system;

c) transfer from one protection instrument channel to another is performed by the operators in a safe and systematic manner; and

d) if power falls from one instrument range to a lower range, then the protection provided by the lower range is automatically restored.

Maintenance bypasses should be installed to remove any one redundancy of the protection system from service for maintenance and testing, and to limit it to only one at any one time. Interlocks should also be used to prevent a further redundant safety group from being taken out of service at the same time.

Interlocks should be provided where automatic testing systems are used, to ensure that the testing system cannot leave the system in an unsafe mode.

Where a protection system design permits faulty sensors to be removed from service, interlocks or administrative safeguards (such as permit to work procedures) should be implemented to limit the number of sensors bypassed.

Interlocks should be provided to ensure withdrawal of control rods from the reactor core in the correct sequence.

Reactors with on-load refuelling should have interlocks to ensure that the fuelling equipment cannot cause a radiation hazard. The interlocks should include redundancy and also diversity of means of preventing potential unsafe conditions.

I&C systems should provide information indicating why interlocks have prevented operations.

Physical controls, e.g. locks, should be in place to prevent human error leading to hazardous plant conditions.

8.3 Control systems

8.3.1 Turbine load control system

*COMMENTARY ON **8.3.1***

The turbine load control system controls turbine power production by adjusting the position of turbine valves to attain the setting of required turbo-generator load. It can have two or more control modes that determine how the control system responds to changes in grid frequency.

In base load mode, the turbine load control system should maintain a constant load output irrespective of grid frequency.

In load-following mode, the turbine load control system should adjust turbine load demand to provide a degree of counteraction to changes in grid frequency, thereby contributing to control of grid frequency.

For "reactor follows turbine" designs, the turbine load control system should provide load signals to other control systems to schedule main controlled parameters according to load and coordinate control system response to changes in load demand.

8.3.2 Main feed control system

*COMMENTARY ON **8.3.2***

The main feed control system controls secondary circuit feed flow to match steam production to turbine load.

On PWRs, feed flow should be controlled by adjusting the position of the main feed regulating valve and the speed of main feed pumps to set the steam generator water level.

On AGRs, boiler feed flow should be controlled by adjusting the position of the main feed regulating valve and the speed of main feed pumps to set the steam pressure at the inlet to the turbine and to hold the boiling level in the boiler within limits.

NOTE In both PWRs and AGRs, feed-regulating valves and feed pump speed are controlled automatically or monitored in the MCR to maintain a constant pressure drop across the feed regulating valves, to minimize wear on the valve.

8.3.3 Primary circuit control systems

*COMMENTARY ON **8.3.3***

The primary circuit and power control systems control the primary circuit conditions to match power transfer from the reactor core to the secondary circuit. The primary coolant flow is not necessarily altered in this process.

The PWR control system controls primary circuit pressure and volume by controlling the temperature and level of water in the pressurizer and holds primary circuit pressure to a set point. The power control responds to the changes in inlet temperature caused by variation in the feedwater and steam flow.

On AGRs, the primary coolant flow is controlled by adjusting the inlet guide vane position to bring the reactor inlet temperature to a set point scheduled according to turbine load, in conjunction with the feedwater flow control.

The conditions of the primary circuit should be controlled to match the power removed by the secondary circuit.

8.3.4 Reactor power control system

*COMMENTARY ON **8.3.4***

The reactor power control system matches reactor power to the amount being removed by the steam generators or boilers. The reactivity of a core depends on the coolant temperature, and control of coolant inlet temperature is therefore important for power control. Control rod movements are made to balance the flux to the power demand and during the change of power itself.

The core of an AGR is divided into areas, each of which is individually controlled to maintain radial stability and the demand channel outlet temperature.

The reactor power control system should have interlocks to prevent control rod withdrawal on high flux and on low margin to core limits.

On PWRs, reactor power should be controlled by adjusting control rod positions to bring reactor inlet temperature to a set point scheduled according to turbine load and feedwater flow.

On AGRs, reactor power should be controlled by adjusting control rod positions to bring the reactor channel outlet gas temperature to a set point scheduled according to turbine load, or by compensating for variations in coolant inlet temperature.

On AGRs, reactor power for each sector or zone should be individually controlled to ensure radial flux stability by adjustment of control rods to the required temperature for the sector or zone.

8.4 Control room design

8.4.1 Location of equipment

Both the MCR and SCR should, as far as possible, be sited in a position invulnerable to damage and protected from potential major accidents. The SCR should be separate from the MCR.

The MCR should, as far as possible, provide staff access to the control equipment for the reactor plant and the associated plant, including the valve actuators, switchgear and local control stations for emergency auxiliary equipment.

Auxiliary equipment, such as control equipment, plant computers and safety equipment associated with the MCR, should be located in separate, adjoining rooms. Access to these rooms should be controlled from the MCR.

8.4.2 Environmental factors

The safety system should monitor the environmental conditions of the MCR to ensure protection from hazards, smoke, radiation or pollution.

The MCR, SCR and any associated equipment annexes should be provided with heating, ventilation and air conditioning, and other equipment limiting the range of temperature, humidity, noise, lighting, etc., to levels which do not adversely affect the performance of the reactor operators, or of the equipment in the control rooms.

The MCR and SCR should be designed to avoid glare and reflections from instruments and polished surfaces.

The cable access to the MCR, SCR and associated equipment should ensure separation of cables serving the equipment, according to the relevant safety divisions of the plant.

8.4.3 Staffing and method of operation

The location of the MCR and the layout of its facilities should take account of the expected method of operating the plant, including actions and procedures necessary to control major or minor hazards which could arise during the life of the reactor, including:

a) the number, function and status of personnel typically attending the plant;

b) the means of communication necessary to coordinate their activities; and

c) the form of procedures (i.e. paper-based or computerized) that are intended to be used by the operators for guiding their activities in the MCR, and at other locations.

The number of staff required to control the reactor and associated plant depends on the degree of automation of the control and surveillance function, but should be sufficient to ensure the safety of the plant in the event of failure of the automatic equipment.

Local, at-plant control should switch out all remote control from both the MCR and SCR and from automatic systems, to ensure personnel safety during maintenance.

When local control could be hazardous to the reactor or associated plant, the MCR should override or administratively prevent it.

Plant actuations should be taken by operation of low voltage interposing relays (e.g. 50 V d.c.) in the switchgear, or by direct operation of low voltage contactors. Control actions over displays and alarm indications should be taken by contacts whose state is sensed by the computer or alarm equipment concerned at a low voltage compatible with the equipment.

For soft control systems, the interface should be taken through the soft control intercommunication system and made by a suitable power output, operating a low voltage contactor or interposing relay in switchgear.

8.4.4 Control and instrument panels

A detailed assessment of the controls, indications and displays required in the MCR should be carried out, including assessment of the control functions that are to be automatic and those that are manual. Human factors expertize should be consulted in the assessment.

The time between an operator carrying out a control action and the plant response shown in the control room should be acceptable to operator expectations and reaction times.

8.4.5 Arrangement of equipment on control panels

The positioning, identification and format of controls and instruments should ensure rapid and accurate comprehension by the operator of changes in nuclear plant state, e.g. by taking account of the size, layout and proportions of the controls and displays. Colour should be used as an aid to this only if the colour vision of the operators can be guaranteed.

The instrument and control panels should ensure that if any single display or control device is disabled, the nuclear reactor and its associated plant can be safely controlled, or shut down.

Indicating instruments should use pointers and dial markings conforming to BS 3693, and should be placed such that they can be accurately read by the operator in their normal position.

The plant, component and device identification method should be consistent throughout the nuclear plant, in the control rooms and on all displays and alarm legends, and use a consistent method of abbreviation where the length of legends is limited.

Common terminology for identifying plant systems, instrument readings and control actions should be used in plant manuals and operating procedures by all station staff, and for all displays and controls.

8.5 Information systems

*COMMENTARY ON **8.5***

*The information system as a whole typically consists of a computer-based system (the plant computer) together with plant condition and alarm displays, with some measurements and alarm legends presented directly. The system as a whole includes a subset of information of high importance providing safety information (see **8.5.3**).*

8.5.1 Measurement identification

Each measurement and state should be associated with a descriptive legend. It should be possible to relate the legend to the tag identity of each instrument or sensor.

8.5.2 Displays

Safety displays should be provided with redundancy.

Computer displays should have redundancy, with the role of each display being interchangeable to ensure that all information is available if one display fails.

NOTE Some displays might be assigned a preferred role.

Displays should indicate a change of measured value or state within a response time acceptable to operator perception and reaction times, typically 1 s.

Records of plant data and operational states should be included in the plant computer functions, including data capable of developing a retroactive understanding of accidents.

8.5.3 Safety parameter display system

*COMMENTARY ON **8.5.3***

The safety parameter display system (SPDS) provides the basic instrumentation display to the operators that enables them to ensure that the reactor is shut down and safe after any trip or reactor fault. It is therefore designed and produced to withstand the consequences and environment of the worst design basis fault of the reactor. Many of the sensor measurements needed for the SPDS could be directly connected to an associated display device.

The SPDS should be installed to ensure a safe shutdown can be identified as having been achieved, and to monitor design basis and design extension conditions. The criteria for including a parameter or alarm for display on the SPDS should be defined.

The SPDS should incorporate redundancy to allow confirmation that a safe shutdown has been achieved, even if there is a fault in the SPDS or loss of power to it.

The SPDS should be seismically qualified.

Alternative methods of providing equivalent information should be determined, including the joint use of computer-based information and seismically qualified indicators. These alternative methods should be identified based on what instruments are to be installed, and be included in the operating manuals for handling the events in question.

NOTE Operating procedures include actions to be taken during emergencies.

Measurements indicating the status of critical safety functions and barriers to radiological releases should be displayed and positioned in the MCR to ensure they are within operator sight at all times.

Severe accident displays should be included and identified within the SPDS, independent of other display instrumentation, where appropriate.

Power supplies required to support the SPDS, including severe accident displays, should ensure autonomous and robust support from redundant sources.

8.5.4 Alarm systems

*COMMENTARY ON **8.5.4***

An alarm system consists of alarm initiating signals and alarm legends, together with a single audible warning device and controls to accept the warning and cancel its sound. A computer display of alarms includes display page turning and related controls. Reset controls clear alarm legends, which are displayed again if the alarm still exists.

The plant computer system can display all alarms, with links to the displays of all measurements. Alarms provided independently from the plant computer also typically provide that information to the plant computer for recording and display.

Alarm system designs should include processes to cover:

a) identification of the most significant alarms in any situation;

   NOTE 1 This might involve grouped alarms, or priority assignment to certain alarms, or processing based on logic, timing or other means. Some plants use a "first up" method of display in which only the first alarm to appear in a group is shown.

b) alarms which are present for long periods, or which are defective;

c) alarms which repeatedly clear and reappear; and

d) the likelihood of large numbers of alarm signals being produced in a short timescale during major nuclear plant trips or changes of operating regime.

NOTE 2 When plant trips or electrical systems fail, large numbers of state changes occur and some designs might class many of these as alarms. Several hundreds of changes can occur in a few minutes, and this rate can continue until plant conditions stabilize. Processing all the changes and identifying what has occurred is difficult to implement but can be valuable.

Alarm systems should cover the complete plant, with information available to MCR operators through the plant computer system.

Alarm systems should indicate the area, or item of equipment, in which the alarm arises in addition to defining the precise alarm situation.

Computer-based alarm systems should initiate alarms when they are detected, ideally within 1 s. Alarms that clear should be marked as such, but not re-displayed as this causes excessive numbers of alarm legends when alarms clear and repeat.

The alarm system should hold lists of current alarms or those which have been accepted, and also be able to present those alarms in groups.

NOTE 3 It is good practice to provide a link to displays of the associated measurements of any alarm.

Alarm system controls should ensure that the warning is acknowledged and permit the alarm legend to be reset. These controls should not prevent the operation of the audible alarm if another alarm signal is received. The alarm legend should not automatically reset when the alarm is acknowledged.

Alarms should be provided to alert operators to conditions that change the characteristics of I&C functions which might otherwise appear to be acting normally, e.g. low-voltage alarms for ion chamber power supplies.

A newly detected alarm should initiate an audible warning with an intermittent sound. The sound should be cancelled by an alarm accept control.

An alarm legend might have multiple initiations, in which case the receipt of an alarm from one of the initiations should not be blocked by another initiation in the group already in the alarm condition.

Alarms and their legend display should be latched until a reset control is operated to clear the memory of that incident.

8.5.5 Alarms of high operational importance

Where the safety of the reactor is dependent upon operator action following receipt of a specific alarm, that alarm should be designated a safety alarm.

Safety alarms should be easily identifiable and employ redundancy, fail-safe techniques or both.

A set of alarms designated as “high importance” should be identified for safety and operational purposes, which could be directly connected (as opposed to multiplexed or scanned) and supported with information provided by the plant computer displays.

NOTE Alarms of high importance are defined as ones which indicate that the operators need to act to preserve safety, maintain generation or be aware that if an alarm occurs operation might be difficult or hazardous, e.g. if the standby equipment for the plant computer fails, followed by failure of the running computer.

The number of such alarm legends in the MCR should typically not exceed 300.

Alarms should be initiated for any change in safety parameters beyond limits set in the reactor protection system. They should include loss of standby equipment to allow operator action to restore their availability.

8.6 Neutron flux measurement

8.6.1 Source range channels

*COMMENTARY ON **8.6.1***

Source range channels provide neutron flux and reactor period or doubling time indications and protection during shutdown and the initial stages of power raise. They can also provide interlock signals to control systems during the early stages of power raise.

Source range channels should measure neutron flux for shutdown, sub-power range and early stages of start-up just beyond criticality. They should be provided with methods of retraction, isolation or shielding from exposure to flux beyond their range, to increase service life to an acceptable level.

Source range measurement channels should confirm that the reactor is shut down following a trip and be operable for long periods during protracted shutdowns.

8.6.2 Intermediate range channels

*COMMENTARY ON **8.6.2***

Intermediate range channels provide wide range neutron flux and reactor period or doubling time indications and protection during power raise and operation at power. They can also provide interlock signals to control systems during power raise.

Intermediate range channels should measure the early stages of start-up to full power, covering six to eight decades of reactor power, on a logarithmic scale.

8.6.3 Power range channels

*COMMENTARY ON **8.6.3***

Power range channels provide power range neutron flux indications, and flux and rate of change of flux protection during operation at power. For water cooled reactors they can also provide axial flux profiles and an input to calculation of DNBR and linear power density. They are typically linear d.c. channels using uncompensated ion chamber detectors.

Power range channels should measure the upper two decades of reactor power on a linear scale with a capacity for a typical over-range of 200% of reactor power.

8.6.4 Nitrogen-16 gamma channels

*COMMENTARY ON **8.6.4***

The concentration of Nitrogen-16 (N-16) in the coolant at the reactor outlet is dependent upon reactor neutron flux when at power, by activation of the oxygen in the water by the flux, with a delay due to the coolant transit time through the reactor.

N-16 gamma radiation monitoring channels on water reactors can provide:

a) a diverse reactor power indication (with a slow response); and

b) an input to DNBR and linear power density calculations.

If N-16 power is required, it should be measured using gamma detectors located around the reactor coolant outlet, with compensation for any coolant flow variation.

8.6.5 Measurement channels

The reactor power measurements for the different types of flux channel used to cover the full range from fully shut down to full power (with a suitable over-range capacity) should overlap by a power factor of ten at each change of flux measurement channel.

MCR displays of reactor power should identify those channels that are within their correct operational range.

Operational bypasses and interlocks should be used to maintain effective instrumentation and protection when transferring measurement from one channel to another covering a different range.

The output signal of a measurement channel should monotonically increase without foldover, with increasing neutron flux over the whole range to which the detector is exposed. A neutron flux above the upper limit of the channel operating range should not lead to a reduction in channel output.

8.6.6 Linear flux channels

The instrument power supply should ensure that linear flux channels continue to operate during a loss of the primary source of the instrumentation power supply.

8.6.7 Logarithmic flux channels

*COMMENTARY ON **8.6.7***

Pulse counting channels might discriminate more effectively against gamma radiation backgrounds, this being particularly important for lower reactor power level measurement and protection.

The logarithmic flux channels should measure the power and provide the measurement for derivation of reactor period or doubling time.

NOTE These signals are used for indication and protection during nuclear reactor start-up and for use during any protracted shutdown period.

Logarithmic flux assemblies should be either direct current, pulse counting or Campbelling channels.

A lower signal level should be defined below which pulse counting and logarithmic assemblies should not be used due to the difficulties in achieving an accurate measurement.

8.7 Flux detectors

8.7.1 Detector siting

Detectors should be sited in a neutron flux representative of the reactor flux for the whole reactor or the section or axial part of the reactor of interest. Detectors should be sited to minimize their effect on potential reactivity changes.

All detectors should be positively located when in the operating position.

The radiation levels should be such that a detector life of approximately ten years is obtained. Removal of one detector, with its safety group bypassed, should not significantly change the output of the detectors of the remaining operational safety groups.

Shielding should be used for replacement of detectors. As flux detectors become highly active in use, special equipment should be used when they are removed from service.

Back-up detectors should be installed unless detectors can be easily changed with the nuclear reactor at power.

8.7.2 Detector errors

*COMMENTARY ON **8.7.2***

Detector positions might need to be adjustable either for sensitivity adjustment or to limit the dose rate to low range detectors when the reactor is at power by removal from a high flux.

Neutron flux detectors are sensitive to gamma or beta radiation arising from their own activation or the reactor structure.

Where misleading signals could occur during detector movement, the position of the detector, or its assembly, should be monitored.

The proportion of the total signal from gamma or beta radiation should not exceed 10% of the true signal over the operating range of the detector.

The potential effects of saturation should be determined when assessing the performance of detectors over their full operating range, including fault conditions.

8.7.3 Measurement of flux distributions and reactor power

*COMMENTARY ON **8.7.3***

*Measurement of reactor core power from N-16 gamma channels (see **8.6.4**) or by reactor heat balance measurements are diverse from neutron flux. In some cases, an important derived measurement is DNBR.*

In addition to the measurement of neutron flux for control and protection purposes, the axial and radial flux distribution in the reactor core should be measured in order to assess performance and to detect asymmetric faults, e.g. control rods or absorbers out of position.

Appropriate means of measurement of reactor power should be provided, e.g. N-16 or power balance calculations, independent of the main neutron flux measurements.

The design of the flux measurement system should allow for the effects of flux distribution on the measurements. Periodic flux distribution measurement should be undertaken to show consistency with theoretical analysis by, e.g. activation of wires or balls inserted and removed from the reactor, inserting a flux chamber into the reactor core at sample locations through tubes, or the inclusion of self-powered neutron detectors in thermocouple assemblies in interstitial core locations to provide temperature and flux profiles.

8.7.4 Calibration and test facilities

Flux measuring channels for high reactor power should be regularly calibrated by means of reactor heat balance measurements to ensure that they indicate the correct thermal power. Sensitivity adjustments should be provided to allow for calibration varying over time.

Lower power flux measuring channels should also be calibrated by comparison with the high power channels.

Flux measuring channels should allow testing of the detector and measurement channel both during shutdown and with the nuclear reactor at power in a manner that does not prejudice safe operation.

8.8 Pressure and differential pressure measurement

Where pressure sensors are used for pressure, flow or level measurement, the likelihood of solid material blocking the impulse pipes or instrument balance pipes and affecting the sensors should be minimized.

Condensate pots should be used for the measurement of the water level in steam generators, pressurizers and the reactor vessel.

If filters are fitted in the impulse lines, precautions should be taken to ensure protection of the reactor if there is a blocked filter.

Barrier membranes with filled lines should be used where long runs of impulse pipe are required.

The signal delay due to instrument pipework and tapping arrangements should be determined during the design phase and included in performance and safety assessments.

Pressure transmitters should be used to provide the measured signal to the reactor protection system, MCR or other control system.

NOTE Differential pressure level instruments are subject to large errors when the temperature of their sensing lines or the density of the fluid being measured changes from the conditions assumed for their calibration.

Instrument racks should have locked, double isolation of impulse pipes and tapping points for personnel safety to ensure an operational configuration and, during maintenance, safe conditions for operating staff. Pipework and balance lines for instrument calibration should have locked isolation valves in operation.

Annex A (informative)

Nuclear power plants – I&C systems – A guide to applicable standards

This annex identifies the international guides and standards of most relevance to the development and implementation of I&C systems for nuclear power plants (NPP).

These international guides and standards comprise:

a) the IAEA safety guides that define the high-level principles;

b) the IEC SC45A series of nuclear sector standards that give the requirements for I&C systems and equipment specifically applicable to NPP; and

c) other standards that apply to the I&C for a number of industrial sectors, including the nuclear sector.

The guides and standards are presented in the form of a summary table (see Table A.1) that lists these by identifier alone, plus a more detailed table that gives the title and a scope outline for each (see Table A.2).

The summary table is organized into groups according to the broad topics addressed and is further divided into those guides and standards which are considered of principal and those of secondary relevance.

The more detailed table is arranged by originating organization and the numerical order of the guides or standards for each organization. Many of the IEC standards are adopted as either BS IEC or BS EN and are listed accordingly in both tables.

The full set of relevant international guides and standards is under continuous development. The annex reflects the situation as of October 2016, the guides and standards included being either published or for which approval for publishing has been formally announced.

Table A.1 **IAEA Safety guides, IEC SC45A standards and other relevant standards** *(1 of 2)*

	Principal	**Secondary**
High-level principles	IAEA SSR-2/1 (Rev. 1) IAEA SSG-39	IAEA SSG-30
System architecture and life cycle aspects	BS EN 61513 BS EN 61226 [A)] BS EN 60709 [A)] BS EN 60671 BS EN 62340 IEC 62645	BS EN 61508 (all parts) BS IEC 61225 BS IEC 61888 BS IEC 61497 IEC 60744 [A)] BS EN ISO 9001
Computer-based systems important for safety	BS EN 60987 BS EN 60880 BS EN 62138 [A)] BS EN 62566 BS IEC 62671	BS EN 61500 [A)] BS ISO/IEC 12207-1

Table A.1 **IAEA Safety guides, IEC SC45A standards and other relevant standards** *(2 of 2)*

	Principal	Secondary
Suitability for environment	BS IEC/IEEE 60780-323 IEC 60980 BS IEC 62342 BS IEC 62465 BS IEC 62003 [A)] BS EN 61000-4-1 to BS EN 61000-4-6 [B)] BS EN 60529 [B)]	BS IEC/IEEE 62582-1 BS IEC/IEEE 62582-2 BS IEC/IEEE 62582-3 BS IEC/IEEE 62582-4 BS IEC/IEEE 62582-5 BS IEC 62765-1
Control rooms and associated HMI	BS EN 60964 [A)] BS EN 60965 BS EN 61839 BS IEC 62646 [A)]	IEC 60960 BS EN 61227 BS EN 61772 BS EN 62241 IEC 61771 BS 3693
Core monitoring/other specific instrumentation	BS IEC 60568 BS IEC 61468 IEC 60911 BS IEC 62397	BS IEC 60737 BS IEC 62117 IEC 61224 BS IEC 62651
Radiation monitoring	BS IEC 60951-1 BS IEC 60951-2 BS IEC 60951-3 BS IEC 60951-4 BS IEC 60768 BS IEC 60515	BS IEC 62705 BS IEC 61504 [A)] IEC 61031 [A)] BS EN 60761 (all parts) [B)] BS IEC 61559-1 [B)] IEC 61559-2 [B)]
Other monitoring/ miscellaneous	BS IEC 62385 IEC 60910 IEC 61250 [A)] BS IEC 62808	BS IEC 60988 IEC 61502 IEC 60772 [A)] BS IEC 61501 BS IEC 60860 [B)]

[A)] Currently under revision.

[B)] Not within the SC45A scope.

Table A.2 **List of existing standards and technical reports and their titles** *(1 of 15)*

Identifier	Title	Summary scope statements
IAEA SSR-2/1 (Rev. 1)	Safety of Nuclear Power Plants: Design [Specific Safety Requirements]	Establishes design requirements for the structures, systems and components (SSC) of a nuclear power plant (NPP), as well as for procedures and organizational processes important to safety, that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events were they to occur. *NOTE The publication is expected to be used primarily for land-based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications.*
IAEA SSG-39	Design of Instrumentation and Control Systems for Nuclear Power Plants [Specific Safety Guide]	Provides guidance on the overall I&C architecture and on the I&C systems important to safety in nuclear power plants for meeting the safety goals of the plant. Provides guidance on the design, implementation, qualification and documentation of I&C systems important to safety in nuclear power plants to meet the requirements of IAEA SSR-2/1 (Rev. 1). Describes I&C specific issues that are relevant to implementing the recommendations of certain other safety guides, such as those which cover the management system, commissioning, installation, operation, and operating limits and conditions.
IAEA SSG-30	Safety Classification of Structures, Systems and Components in Nuclear Power Plants [Specific Safety Guide]	Provides recommendations and guidance on how to meet the requirements established in SSR-2/1 and GSR Part 4 [Safety Assessment for Facilities and Activities] for the identification of SSCs important to safety and for their classification on the basis of their function and safety significance. Applies to the design of all SSCs important to safety for all plant states, including all modes of normal operation, during the lifetime of an NPP.
BS IEC 60515	Nuclear power plants – Instrumentation important to safety – Radiation detectors – Characteristics and test methods	Establishes the characteristics and test methods for gas-filled radiation detectors, installed external to the core of nuclear reactors, that are used for their instrumentation and protection
BS EN 60529 [B)]	Degrees of protection provided by enclosures (IP code)	Describes a system for classifying the degrees of protection provided by enclosures of electrical equipment with a rated voltage not exceeding 72.5 kV.

Table A.2 **List of existing standards and technical reports and their titles** *(2 of 15)*

Identifier	Title	Summary scope statements
BS IEC 60568	Nuclear power plants – Instrumentation important to safety – In-core instrumentation for neutron fluence rate (flux) measurements in power reactors	Applies to in-core (on-line) neutron detectors, together with associated components and instrumentation, designed for purposes important to reactor safety: protection, information or control. The detector types usually used are direct current ionisation chambers, fission ion chambers and self-powered neutron detectors. Provides guidance for the design of in-core instrumentation for neutron flux measurements in thermal neutron reactors designed for power production.
BS EN 60671	Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing	Lays down the principles for testing I&C systems performing category A, B and C functions, per BS EN 61226, during normal power operation and shutdown, so as to check the functional availability, especially with regard to the detection of faults that could prevent the proper operation of the functions important to safety. Covers the possibility of testing at short intervals or continuous surveillance, as well as periodic testing at longer intervals. Establishes basic rules for the design and application of the test equipment and its interface with the systems important to safety. Considers the effect of any test equipment failure on the reliability of the I&C systems
BS EN 60709 [A)]	Nuclear power plants – Instrumentation and control systems important to safety – Separation	Applies to nuclear power plant I&C systems, and their cables that are important to safety. Also applies to temporary installations which are a part of those I&C systems important to safety (e.g. auxiliary equipment for commissioning tests and experiments). Defines the assessments needed and the technical requirements to be met for I&C systems important to safety and their cables, in order to achieve adequate physical separation between redundant sections of a system and between a system and another system.

Table A.2 **List of existing standards and technical reports and their titles** *(3 of 15)*

Identifier	Title	Summary scope statements
BS IEC 60737	Nuclear power plants – Instrumentation important to safety – Temperature sensors (in-core and primary coolant circuit) – Characteristics and test methods	Applies to general aspects of system and component design, manufacturing and test methods for temperature sensors, including thermocouples and RTDs, used in-core and for the primary coolant circuit in nuclear power reactors. Places emphasis on features specific to the nuclear application. Makes recommendations concerning components and sensors only when they relate to the containment of such components within the reactor primary envelope and/or in high radiation fields. Provides guidance to ensure that (a) the reactor conditions do not damage the temperature sensors and (b) the in-core temperature measuring system and the sensor installation do not prejudice the safe operation and the availability of the reactor.
IEC 60744 [A)]	Safety logic assemblies of nuclear power plants – Characteristics and test methods	Provides principles of design, construction and testing of safety logic assemblies used in protection systems. Includes provisions for acceptance and in operating testing, reliability criteria and protection from external influences.
BS EN 60761 (all parts) [B)]	Equipment for continuously monitoring of radioactivity in gaseous effluents	Part 1: General requirements. Part 2: Specific requirements for radioactive aerosol monitors including transuranic aerosols. Part 3: Specific requirements for radioactive noble gas monitors. Part 4: Specific requirements for radioactive iodine monitors. Part 5: Specific requirements for tritium monitors.
BS IEC 60768	Nuclear power plants – Instrumentation important to safety – Equipment for continuous in-line or on-line monitoring of radioactivity in process streams for normal and incident conditions	Applies to the continuous in-line or on-line monitoring of radioactive substances within plant process streams of nuclear power plants during normal operation and incident conditions. Provides criteria for the design, selection, testing, calibration and functional location of the equipment for the monitoring of such plant process streams.
IEC 60772 [A)]	Electrical penetration assemblies in containment structures for nuclear power generating stations	Addresses the engineered safety requirements to be met in the design, calculation, fabrication, assembly, testing, installation and maintenance of cable penetrations in reactor containments.

Table A.2 **List of existing standards and technical reports and their titles** *(4 of 15)*

Identifier	Title	Summary scope statements
BS IEC/ IEEE 60780-323	Nuclear facilities – Electrical equipment important to safety – Qualification	Describes the basic requirements for qualifying electrical equipment important to safety and interfaces (electrical and mechanical) that are to be used in nuclear facilities. The principles, methods and procedures described are intended to be used for qualifying equipment, maintaining and extending qualification, and updating qualification, as required, if the equipment is modified. The qualification requirements demonstrate and document the ability of equipment to perform safety function(s) under applicable service conditions, including design basis events and certain design extension conditions, and reduce the risk of environmentally induced common-cause equipment failure.
BS IEC 60860 [B)]	Radiation protection instrumentation – Warning equipment for criticality accidents	Applies to equipment intended to provide warning of a criticality accident by the detection of gamma radiation, neutrons or both from such an event. Prescribes general, radiation detection, environmental, mechanical, electromagnetic and documentation requirements and to specify acceptance criteria for criticality accident warning equipment.
BS EN 60880	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions	Applies to the software of computer-based I&C systems of nuclear power plants performing category A functions as defined by BS EN 61226. Provides requirements for the purpose of achieving highly reliable software. Addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation. Has been widely used for regulatory acceptance. Provides guidance on methods which are beneficial or which have adverse effects on software integrity. Also refers to BS EN 61508 which has a detailed description of techniques recommended for high integrity software.
IEC 60910	Containment monitoring instrumentation for early detection of developing deviations from normal operation in light water reactors	Gives recommendations on the data to be measured to enable an operator to diagnose developing deviations from normal functioning so as to take corrective action at an early stage. (Text identical to Annex 11 to IAEA Safety Guide No. 50-SG-D12 [3].).

Table A.2 **List of existing standards and technical reports and their titles** *(5 of 15)*

Identifier	Title	Summary scope statements
IEC 60911	Measurements for monitoring adequate cooling within the core of pressurized light water reactors	Defines requirements for additional instrumentation to measure coolant parameters, which are of interest when abnormal conditions arise with either one or two phases of coolant or with gas included in the reactor vessel. The information obtained on coolant conditions assists the operator to decide on actions needed to maintain adequate core cooling.
BS IEC 60951-1	Nuclear power plants – Instrumentation important to safety – Radiation monitoring for accident and post- accident conditions – Part 1: General requirements	Provides general guidance on design principles and performance criteria for equipment to measure radiation and fluid (gaseous effluents or liquids) radioactivity levels at nuclear power plants during and after an accident.
BS IEC 60951-2	Nuclear power plants – Instrumentation important to safety – Radiation monitoring for accident and post- accident conditions – Part 2: Equipment for continuous off-line monitoring of radioactivity in gaseous effluents and ventilation air	Provides general guidance on the design principles and performance criteria for equipment for continuous off-line monitoring of radioactivity in gaseous effluents and ventilation air used in nuclear power plants for accident and post-accident conditions.
BS IEC 60951-3	Nuclear power plants – Instrumentation important to safety – Radiation monitoring for accident and post- accident conditions – Part 3: Equipment for continuous high range area gamma monitoring	Provides general guidance on the design principles and performance criteria for equipment for continuous high range area gamma monitoring in nuclear power plants for accident and post-accident conditions.
BS IEC 60951-4	Nuclear power plants – Instrumentation important to safety – Radiation monitoring for accident and post- accident conditions – Part 4: Equipment for continuous in-line or on-line monitoring of radioactivity in process streams	Provides general guidance on the design principles and performance criteria for equipment for continuous in-line or on-line monitoring of radioactivity in process stream in nuclear power plants for accident and post-accident conditions.
IEC 60960	Functional design criteria for a safety parameter display system for nuclear power stations	Considers the functional design criteria for a safety parameter display system (SPDS) giving concise information to aid operating personnel, particularly in abnormal conditions. An SPDS is made up of instruments, displays, computer hardware and software either constituting a stand-alone system or integrated into the control room information system. Applies only to control rooms designed in accordance with the IEC control room design standards (see BS EN 61772, BS EN 61839).

Table A.2 **List of existing standards and technical reports and their titles** *(6 of 15)*

Identifier	Title	Summary scope statements
BS EN 60964 [A)]	Nuclear power plants – Control rooms – Design	Establishes requirements for the human-machine interface (HMI) in the main control rooms of nuclear power plants. It also establishes requirements for the selection of functions, design considerations and organization of the HMI and procedures to be used systematically to verify and validate the functional design. The requirements reflect the application of human factors engineering (HFE) principles as they apply to the HMI during normal and abnormal plant conditions. Emphasizes the importance of determining the I&C requirements of the whole plant, and then identifying the requirements of the main control room (MCR) for normal and other operational conditions. The standard has extensive recommendations on the data processing and display system requirements. Note also the supplementary standards BS EN 61227, IEC 61771, BS EN 61772, BS EN 61839 and BS EN 62241.
BS EN 60965	Nuclear power plants – Control rooms – Supplementary control room for reactor shutdown without access to the main control room	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 shutdown 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. Also establishes requirements for the selection of functions, the design and organization of the human-machine interface (HMI), and the procedures used systematically to verify and validate the functional design of the supplementary control room.
IEC 60980	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations	Applies to electrical and I&C equipment of the safety systems of nuclear power plants, including components or equipment of any interface whose failure could adversely affect the performance of the safety systems. It presents acceptable seismic qualification methods and requirements to demonstrate that electrical and I&C equipment can perform their safety-related functions during and after an earthquake.
BS EN 60987	Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems	Applies to computer systems' hardware for systems important to safety used in nuclear power stations. The requirements specified are applicable but not restricted to the following items of such systems, down to the component level: external power supplies to the computer system; internal architecture; input/output equipment and interfaces; data transmission means; storage devices; and test devices.

Table A.2 **List of existing standards and technical reports and their titles** *(7 of 15)*

Identifier	Title	Summary scope statements
BS IEC 60988	Nuclear power plants – Instrumentation important to safety – Acoustic monitoring systems for detection of loose parts: Characteristics, design criteria and operational procedures	Applies to on-site systems used for continuous monitoring of structure-borne sound measured at the reactor coolant boundary of light water reactors for the purpose of detecting loose, loosened or detached metallic parts which have the potential to cause damage to the reactor core, other internals of the primary circuit or to the primary circuit pressure boundary. It covers system characteristics, design requirements and operational procedures.
IEC TR 61000-4-1 [B)]	Electromagnetic compatibility (EMC). Testing and measurement techniques – Overview of the IEC 61000-4 series	
BS EN 61000-4-2 [B)]	Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test	
BS EN 61000-4-3 [B)]	Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test	
BS EN 61000-4-4 [B)]	Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/ burst immunity test	
BS EN 61000-4-5 [B)]	Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test	
BS EN 61000-4-6 [B)]	Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques– Immunity to conducted disturbances, induced by radio-frequency fields	
BS EN 6100-6-5	Electromagnetic compatibility (EMC) – Part 6-5: Generic standards – Immunity for equipment used in power station and substation environment	

Table A.2 **List of existing standards and technical reports and their titles** *(8 of 15)*

Identifier	Title	Summary scope statements
IEC 61031 [A)]	Design, location and application criteria for installed gamma radiation dose rate monitoring equipment for use in nuclear power plants during normal operation and anticipated operational occurrences	Provides guidelines for the design principles, the location, the application, the calibration, the operation, and the testing of installed equipment for continuously monitoring local gamma radiation dose rates in nuclear power plants under normal operation conditions and anticipated operational occurrences.
IEC 61224	Nuclear reactors – Response time in resistance temperature detectors (RTD) – In situ measurements	Defines the criteria for the choice, conception and use of equipment for the measurement of the response time of RTD used in the safety and control systems of nuclear reactors.
BS IEC 61225	Nuclear power plants – Instrumentation and control systems important to safety – Requirements for electrical supplies	Specifies the performance and the functional characteristics of the electrical supply systems required for the I&C systems important to safety of a nuclear power plant. Also provides guidance on the possible use of these supplies for other I&C systems.
BS EN 61226 [A)]	Nuclear power plants – Instrumentation and control important for safety – Classification of instrumentation and control functions	Establishes a method of classification of the information and command functions for nuclear power plants, and the I&C systems and equipment that provide those functions, into categories that designate the importance to safety of the function. The resulting classification then determines relevant design criteria, which are the measures of quality by which the adequacy of each function in relation to its importance to plant safety is ensured. The design criteria are those of functionality, reliability, performance, environmental durability and QA.
BS EN 61227	Nuclear power plants – Control rooms – Operator controls	Supplements BS EN 60964 and identifies the human-machine interface (HMI) requirements for discrete controls, multiplexed conventional systems and soft control systems.
IEC 61250 [A)]	Nuclear reactors – Instrumentation and control systems important for safety – Detection of leakage in coolant systems	Defines the requirements for instrumentation needed to detect leakage from reactor coolant systems of light water nuclear reactors. Methods of leak detection are described, and characteristics of different methods of detection and of differentiating between allowable and abnormal leakages are given.
BS IEC 61468	Nuclear power plants – In-core instrumentation – Characteristics and test methods of self-powered neutron detectors	Applies to in-core detectors and instrumentation which are designed for purposes important to safety: protection, control and information. Restricted to characteristics and test methods for self-powered neutron detectors (SPNDs) used for neutron fluence rate (flux) and spatial power measurements in nuclear reactors. Gives requirements, recommendations and guidance on selection of the type and characteristics of SPNDs for different possible applications of SPNDs.

Table A.2 **List of existing standards and technical reports and their titles** *(9 of 15)*

Identifier	Title	Summary scope statements
BS IEC 61497	Nuclear power plants – Electrical interlocks for functions important to safety – Recommendations for design and implementation	Provides recommendations for the design and implementation of electrical interlocks used actively or passively to prevent unsafe conditions or to ensure specific safe conditions and states during the operation of nuclear power plants.
BS EN 61500	Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions	Establishes the requirements for data communication between equipment providing functions at category A, or between equipment providing functions at category A and equipment providing functions at other categories, as defined in BS EN 61226.
BS IEC 61501	Nuclear reactor instrumentation – Wide range neutron fluence rate meter – Mean square voltage method	Applies to instrument and measurement channels which generate a calculation of the mean square voltage (MSV) of a signal arising from a neutron detector, in order to extract from it information relating to the neutron fluence rate (flux) of a nuclear reactor.
IEC 61502	Nuclear power plants – Pressurized water reactors – Vibration monitoring of internal structures	Applies to systems used for monitoring the vibratory behaviour of the internal structures of pressurized water reactors (core barrel, thermal shield, upper and lower core support, etc.) and fuel assemblies on the basis of neutron fluctuations observed outside the vessel and vessel vibrations. The main objective of monitoring is to detect degradation of internal structures.
BS IEC 61504 [A)]	Nuclear power plants – Instrumentation and control systems important to safety – Plant-wide radiation monitoring	Provides guidance on the design principles and performance criteria for computer-based radiation monitoring systems. Such systems are provided to integrate the monitoring of plant-wide processes, effluent streams and area radiation. Integrates data processing, storage, optimization and correlation of data flow and displays.
BS EN 61508 (all parts)	Functional safety of electrical/electronic/ programmable electronic safety-related systems	Part 1: General requirements Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems Part 3: Software requirements Part 4: Definitions and abbreviations Part 5: Examples of methods for the determination of safety integrity levels Part 6: Guidelines on the application of BS EN 61508-2 and BS EN 61508-3 Part 7: Overview of techniques and measures

Table A.2 **List of existing standards and technical reports and their titles** *(10 of 15)*

Identifier	Title	Summary scope statements
BS EN 61513	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	Provides requirements and recommendations for the overall I&C architecture which might contain either of the following technologies used in I&C systems important to safety: conventional hardwired equipment, computer-based equipment or a combination of both types of equipment. Highlights also the need for complete and precise requirements, derived from the plant safety goals, as a prerequisite for generating the comprehensive requirements for the overall I&C architecture, and hence for the individual I&C systems important to safety. Introduces the concept of a safety life cycle for the overall I&C architecture, and a safety life cycle for the individual systems. By this, it highlights the relations between the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety, and the relations between the overall I&C architecture and the requirements of the individual systems important to safety.
BS IEC 61559-1 [B)]	Radiation protection instrumentation in nuclear facilities – Centralized systems for continuous monitoring of radiation and/or levels of radioactivity – Part 1: General requirements	Applies to centralized systems intended for continuous monitoring of radiation and/or levels of radioactivity in nuclear facilities, primarily in support of radiological protection in the working areas. It applies specifically to centralized data processing systems, data links, and equipment siting and layout. It also applies to indications displayed locally and centrally.
IEC 61559-2 [B)]	Radiation in nuclear facilities – Centralized systems for continuous monitoring of radiation and/or levels of radioactivity – Part 2: Requirements for discharge, environmental, accident or post-accident monitoring functions	Supplements Part 1 of the standard to include discharge, environmental, accident, and post-accident monitoring functions that are not within the scope of that part.
IEC 61771	Nuclear power plants – Main control room – Verification and validation of design	Specifies verification and validation procedures for the design of the control-room system of nuclear power plants, and gives verification and validation criteria for the assignment of functions and for the integrated control-room system.
BS EN 61772	Nuclear power plants – Control rooms – Application of visual display units (VDUs)	Supplements BS EN 60964 and presents design requirements for the application of VDUs in main control rooms of nuclear power plants. Assists the designer in specifying VDU applications (including displays on individual workstations and larger displays for group-working or distant viewing) together with or instead of conventional panel displays.

Table A.2 **List of existing standards and technical reports and their titles** *(11 of 15)*

Identifier	Title	Summary scope statements
BS EN 61839	Nuclear power plants – Design of control rooms – Functional analysis and assignment	Specifies functional analysis and assignment procedures for the design of the control room system for nuclear power plants and gives rules for developing criteria for the assignment of functions. It supplements BS EN 60964. Applies to the design of new control rooms or to back-fits to existing control-rooms.
BS IEC 61888	Nuclear power plants – Instrumentation important to safety – Determination and maintenance of trip setpoints	Defines the requirements for assuring that automatic set points for nuclear safety system instrumentation are established and maintained within specified limits in nuclear power plants and nuclear reactor facilities.
BS IEC 62003 [A)]	Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing	Establishes requirements for electromagnetic compatibility (EMC) testing of instrumentation and control equipment supplied for use in systems important to safety at nuclear power plants. It lists the applicable IEC standards (principally the BS EN 61000 series) which define the general test methods, and provides the necessary application-specific parameters and criteria to ensure that nuclear safety requirements are met.
BS IEC 62117	Nuclear reactor instrumentation – Pressurized light water reactors (PWR) – Monitoring adequate cooling within the core during cold shutdown	Presents requirements for the monitoring of adequate core cooling within the reactor core for safe operation of PWRs during cold shutdown conditions when the coolant temperature is below 100 °C.
BS EN 62138 [A)]	Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions	Provides requirements for the software of computer-based I&C systems performing functions of safety categories B and C as defined by BS EN 61226. It complements BS EN 60880 which provides requirements for the software of computer-based I&C systems performing functions of safety category A. It is also consistent with, and complementary to, BS EN 61513.
BS EN 62241	Nuclear power plants – Main control room – Alarm functions and presentation	Provides the functional requirements for the alarm systems in the main control room of nuclear power plants. It also establishes the human factors requirements and the design guidelines for alarm presentation for the main control room of nuclear power plants.
BS EN 62340	Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)	Gives requirements related to the avoidance of CCF of I&C systems that perform category A functions. It applies to I&C systems using conventional hard-wired equipment, computer-based equipment or a combination of both types.

Table A.2 **List of existing standards and technical reports and their titles** *(12 of 15)*

Identifier	Title	Summary scope statements
BS IEC 62342	Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing	Provides strategies, technical requirements and recommendations for the management of ageing of nuclear power plant I&C systems and associated equipment.
BS IEC 62385	Nuclear power plants – Instrumentation and control important to safety – Methods for assessing the performance of safety system instrument channels	Defines requirements for demonstrating acceptable performance of safety system instrument channels through response time testing, calibration verification, and other means.
BS IEC 62397	Nuclear power plants – Instrumentation and control important to safety – Resistance temperature detectors	Describes the requirements for RTDs suitable for nuclear power plant services, including those for design, materials, manufacturing, testing, calibration, procurement and inspection.
BS IEC 62465	Nuclear power plants – Instrumentation and control important to safety – Management of ageing of electrical cabling systems	Provides strategies, technical requirements and recommended practices for the management of normal ageing of cabling systems that are important to safety in nuclear power plants. In addition, informative annexes give examples of cable testing techniques, procedures and equipment that can be used to ensure that ageing degradation does not impact plant safety.
BS EN 62566	Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions	Provides requirements for achieving highly reliable HDL-programmed Devices (HPD), for use in I&C systems of nuclear power plants performing functions of safety category A as defined by BS EN 61226.
BS IEC/IEEE 62582-1	Nuclear power plants – Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 1: General	Provides requirements related to specific methods for condition monitoring in electrical equipment important to safety of nuclear power plants. It also includes requirements which are common to all methods.
BS IEC/IEEE 62582-2	Nuclear power plants - Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 2: Indenter modulus	Contains methods for condition monitoring of organic and polymeric materials in I&C systems using the indenter modulus technique in the detail necessary to produce accurate and reproducible measurements.
BS IEC/IEEE 62582-3	Nuclear power plants – Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 3: Elongation at break	Contains methods for condition monitoring of organic and polymeric materials in I&C systems using tensile elongation techniques in the detail necessary to produce accurate and reproducible measurements.

Table A.2 **List of existing standards and technical reports and their titles** *(13 of 15)*

Identifier	Title	Summary scope statements
BS IEC/IEEE 62582-4	Nuclear power plants – Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 4: Oxidation induction techniques	Specifies methods for condition monitoring of organic and polymeric materials in instrumentation and control systems using oxidation induction techniques in the detail necessary to produce accurate and reproducible measurements.
BS IEC/IEEE 62582-5	Nuclear power plants - Instrumentation and control important to safety – Electrical equipment condition monitoring methods – Part 5: Optical time domain reflectometry	Contains methods for monitoring the attenuation condition of optical fibres and cables in instrumentation and control systems using optical time domain reflectometer (OTDR) measurements in the detail necessary to produce accurate and reproducible measurements.
IEC 62645	Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems	Establishes requirements and provides guidance for the development and management of effective security programmes for I&C computer-based systems for nuclear power plants, possibly integrating HPD (HDL-programmed devices), otherwise known as I&C CB&HPD systems. Inherent to these requirements and guidance is the criterion that the power plant I&C CB&HPD system security programme conforms to the applicable national I&C CB&HPD security requirements. Defines adequate programmatic measures for the prevention of, detection of and reaction to malicious acts by digital means (cyber-attacks) on I&C CB&HPD systems. This includes any unsafe situation, equipment damage or plant performance degradation that could result.
BS IEC 62646 [A)]	Nuclear power plants – Control rooms – Computer-based procedures	Establishes requirements for the whole life cycle of operating procedures that the designer wishes to computerize. It also provides guidance for making decisions about which types of procedures are to be computerized and to what extent.
BS IEC 62651	Nuclear power plants – Instrumentation important to safety – Thermocouples: characteristics and test methods	Describes the requirements for thermocouples suitable for NPP applications. The requirements specified cover design, materials, manufacturing, testing, calibration, procurement and inspection.
BS IEC 62671	Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality	Addresses certain devices that contain embedded software or electronically-configured digital circuits that have not been produced to other IEC standards which apply to systems and equipment important to safety in nuclear power plants, but which are candidates for use in nuclear power plants.

Table A.2 **List of existing standards and technical reports and their titles** *(14 of 15)*

Identifier	Title	Summary scope statements
BS IEC 62705	Nuclear power plants – Instrumentation and control important to safety – Radiation monitoring systems (RMS): Characteristics and lifecycle	Applies to radiation monitoring systems (RMS) installed in Nuclear Power Plants that are intended to be used during normal operations and anticipated operational occurrences, and to be used during and/or after accident conditions. Gives requirements for the life cycle management of RMS and gives guidance on the application of existing IEC standards covering the design and qualification of systems and equipment.
BS IEC 62765-1	Nuclear power plants - Instrumentation and control important to safety – Management of ageing of sensors and transmitters – Part 1: Pressure transmitters	Provides strategies, technical requirements and recommended practices for the management of ageing to ensure that ageing of pressure transmitters important to safety in nuclear power plants can be identified and that suitable remedial actions are undertaken as necessary to demonstrate that the safety of the plant is not impaired. Deals with analogue electronic pressure transmitters, which have an electrical signal output that is a function of pressure applied on the sensing part and which are included in I&C systems important to safety.
BS IEC 62808	Nuclear power plants – Instrumentation and control systems important to safety – Design and qualification of isolation devices	Establishes requirements for the design, analysis and qualification of isolation devices used to ensure electrical independence of redundant safety system circuits, or between safety and lower class circuits, as specified in BS EN 60709. Includes guidance on the determination of the maximum credible fault that is applied to the isolation devices. The maximum credible fault can be used as a basis for the test levels used in testing based on other standards (e.g. BS EN 61000-6-5 or BS IEC 62003).
BS EN ISO 9001	Quality management systems – Requirements	Specifies requirements for a quality management system when an organization: a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

Table A.2 **List of existing standards and technical reports and their titles** *(15 of 15)*

Identifier	Title	Summary scope statements
BS ISO/IEC 12207	Systems and software engineering – Software life cycle processes	Establishes a common framework for software life cycle processes, with well defined terminology, that can be referenced by the software industry. It contains processes, activities, and tasks that are to be applied during the acquisition of a software product or service and during the supply, development, operation, maintenance and disposal of software products. Software includes the software portion of firmware.
BS 3693	Recommendations for design of scales and indexes on analogue indicating instruments	Gives recommendations for the design of scales and indexes of analogue indicating instruments in which an index moves in relation to a fixed array of scale marks to display the value of a measured quantity, or in which the scale moves in relation to a fixed index. Basic designs are given for scales for single, dual and multi-range fixed or portable instruments.

[A)] Currently under revision.

[B)] Not within IEC SC45A scope.

Bibliography

Standards publications

Table A.2 lists international guides and standards of most relevance to the development and implementation of I&C systems for nuclear power plants.

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC SC45A, *Instrumentation, control and electrical systems of nuclear facilities*

Other publications

[1] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA). *IAEA Safety Glossary: Terminology used in Nuclear Safety and Radiation Protection*. Vienna, IAEA, 2007.

[2] Office for Nuclear Regulation. *Nuclear Safety Technical Assessment Guide.* NS-TAST-GD-046 Revision 3.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY. IAEA Safety Guide No. 50-SG-D12: Design of the Reactor Containment. Vienna, IAEA, 1985.

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

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

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.