

BS 4877:2025



BSI Standards Publication

Nuclear reactor instrumentation and control – Code of practice

bsi.

AVA Documents
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2025

Published by BSI Standards Limited 2025

ISBN 978 0 539 26244 5

ICS 27.120.10

The following BSI references relate to the work on this document:

Committee reference NCE/8

Draft for comment 24/30470900 DC

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

Contents

	Page
Foreword	III
1 Scope	1
2 Normative references	2
3 Terms, definitions and abbreviations	2
4 General I&C design principles	5
4.1 Safe operation	5
4.2 I&C Life cycle	6
4.3 I&C design system interaction	7
4.4 I&C design basis	7
4.5 Management systems and quality assurance processes	9
4.6 Examination, inspection, maintenance and testing	9
4.7 Systems dependent on computer software	10
4.8 Hardware description language programmed device	12
4.9 Equipment qualification	12
4.10 I&C system architecture, redundancy and the single failure criterion	13
4.11 Reliability assessment and calculation	14
4.12 Human factors	15
4.13 Safety and control arrangements for abnormal operation – Commissioning, fuel loading, maintenance, modification and testing	15
4.14 Cybersecurity	16
4.15 SMART devices	17
5 I&C systems	17
5.1 Safety system	17
5.2 Automatic control systems	20
5.3 Main control room and supplementary control room	21
5.4 I&C support systems	23
6 Reactor and plant instrumentation	24
6.1 Sensors and actuators	24
6.2 Control rod position	26
6.3 Valve and switchgear position	26
6.4 Neutron flux measurement	27
6.5 Temperature measurement	27
6.6 Environmental monitoring	29
6.7 Coolant conditions	29
7 Secondary circuit, turbine and electrical systems	31
7.1 Secondary coolant circuit measurements	31
7.2 Condensate measurements	32
7.3 Emergency feedwater flow measurement	32
7.4 Turbine stop and throttle valve conditions	32
7.5 Electrical system measurements and controls	32
8 Design recommendations	32
8.1 Reactor protection system	32
8.2 Control systems	36
8.3 Control room design	37
8.4 Information systems	39
8.5 Neutron flux measurement	41
8.6 Flux detectors	43
8.7 Pressure and differential pressure measurement	44

Annex A	(informative) Nuclear power plants – I&C systems – A guide to applicable standards	45
	<i>Table A.1 — Summary table</i>	46
	<i>Table A.2 — List of existing standards and technical reports and their titles</i>	48
	Bibliography	69

Summary of pages

This document comprises a front cover, an inside front cover, pages I to IV, pages 1 to 73, 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 28 February 2025. 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 the committee manager.

Supersession

This British Standard supersedes [BS 4877:2016](#), which is withdrawn.

Information about this document

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

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

This British Standard guides users in meeting the requirements of international standards principally of the IEC TC45/SC 45 A series of standards. These in turn are set against the principles set out by the IAEA. This British Standard is aimed at anyone with an interest in meeting the standards, including designers, managers and safety assessors. The intention is to include specific UK aspects and the examples given are typically based on past or potential future UK power plant design. While not intending to be a guide to obtaining UK regulatory approval, due note is taken of regulatory expectations, where appropriate. Detailed references to standards are generally not included within the clauses, however some specific points are highlighted.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at knowledge.bsigroup.com, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

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

Users may substitute any of the recommendations in this British Standard with practices of equivalent or better outcome. Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this document 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.

Where words have alternative spellings, the preferred spelling of the *Shorter Oxford English Dictionary* is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

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

1 Scope

This British Standard provides recommendations and guidance for the design and safety assurance of instrumentation and control (I&C) systems and equipment for nuclear power plants.

This British Standard covers the I&C systems and equipment required for reactor safety and protection, automatic control and other instrumentation and information functions.

Recommendations and guidance are also provided for the main and supplementary control rooms, and for the power supplies to the I&C systems.

NOTE 1 This British Standard presents the key principles that apply to the design and safety assurance of these I&C systems. A comprehensive list of the relevant National and International Standards that apply to I&C systems and equipment of nuclear power plants is given in [Annex A](#).

The scope of the I&C systems and equipment covered by this British Standard includes:

- a) sensors and the measurement of plant variables;
- b) the reactor safety and protection system;
- c) nuclear power plant instrumentation;
- d) plant control systems;
- e) information display facilities;
- f) power supplies for the I&C systems; and
- g) communication systems.

This British Standard does not include recommendations for:

- 1) I&C for refuelling systems and related facilities;
- 2) the emergency control centre;
- 3) the technical support centre and the off-site support facilities;
- 4) radiological risks; and
- 5) commercial or managerial matters.

NOTE 2 In order to cover the scope of I&C systems and equipment listed in a) to g), this British Standard is organized into the following clauses:

- a) *general I&C design principles;*
- b) *I&C systems;*
- c) *reactor plant instrumentation;*
- d) *secondary circuit, turbine and electrical systems;*
- e) *detailed design recommendations for specific instrumentation; and*
- f) *list of all relevant National and International Standards ([Annex A](#)).*

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions, or limits the application, of this document¹⁾. 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*

BS EN 60880:2009, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer based systems performing category A functions*

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

BS EN 62566:2014, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL programmed integrated circuits for systems performing category A functions*

BS EN IEC 62138:2019, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer based systems performing category B or C functions*

BS EN IEC 62566-2:2020, *Nuclear power plants – Instrumentation and control systems important to safety – Development of HDL programmed integrated circuits – Part 2: HDL programmed integrated circuits for systems performing category B or C functions*

BS EN IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

NOTE See also the definitions in the International Atomic Energy Agency (IAEA) Nuclear Safety and Security 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 but which, in view of appropriate design provisions, do not cause 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;

¹⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

- d) Level 4: mitigates the consequences of accidents that result from failure of the third level of defence in depth; and
- e) Level 5: mitigates the radiological consequences of radioactive releases that could potentially result from accidents

NOTE 1 The IAEA-NSS-GLO [1] also defines defence in depth for nuclear security as “combination of multiple layers of systems and measures that have to be overcome or circumvented before nuclear security is compromised”.

NOTE 2 The IAEA requirements for design introduce the concept of defence in depth in the design of a nuclear facility.

NOTE 3 The IAEA description is more comprehensive than that given.

NOTE 4 Levels 1 to 4 relate to the on-site provisions, the fifth level 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 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 comprise conditions in events without significant fuel degradation and conditions involving significant core degradation; the latter also being called severe accidents.

3.1.6 failure

loss of ability of a structure, system or component to function within acceptance criteria 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

NOTE A fault could arise from a malfunction or defect within a structure, system or component or due to external influences or human error.

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 A safety system's 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 as “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 actions required for a particular postulated initiating event so 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 or a safety feature for design extension conditions

NOTE A safety-related instrumentation and control system, for example, is an I&C 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 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) undetectable failures, i.e. any failure that cannot be detected by periodic testing, alarm or anomalous indication; and
 - 2) failures caused by the single failure;
- b) 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

3.1.15 surveillance testing

periodic testing to verify that structures, systems and components continue to function or are capable of performing their functions when called upon to do so

3.2 Abbreviations

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

AGR	advanced gas-cooled reactor
BWR	boiling water reactor
CCF	common cause failure
CPLD	complex programmable logic device
DNBR	departure from nucleate boiling ratio
EIMT	examination, inspection, maintenance and testing
EMI	electro-magnetic interference
ESF	engineered safety feature
FPGA	field-programmable gate array
HDL	hardware description language
HMI	human machine interface

HPD	HDL programmed device
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
PDB	pre-developed block
pdf	probability of failure on demand
PIE	postulated initiating event
PWR	pressurized water reactor
SCR	supplementary control room
SFC	single failure criterion
SIDS	safety information display system
SPDS	safety parameter display system
SSC	structures, systems and components
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 provide 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;

NOTE 1 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;

NOTE 2 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;

NOTE 3 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;

NOTE 4 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 heating, ventilation and air conditioning (HVAC) of the plant or main control room (MCR);

NOTE 5 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; and

NOTE 6 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.

- g) other faults and hazards not covered by a) to f) which should be determined in order to identify the most effective plant operations needed to contain them.

NOTE 7 These could cause plant damage, loss of access to plant areas, and damage to electrical systems.

For 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 8 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 meet the following high-level plant objectives:

- 1) prevent the uncontrolled 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 key plant variables should be available to allow operators to understand the status of the reactor plant, critical safety functions and to allow implementation of accident management strategies.

NOTE 9 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) results of the plant safety analysis;
- 2) design of the mechanical plant systems;
- 3) civil engineering requirements;
- 4) desired operational arrangements and modes of operation of the plant;
- 5) maintenance requirements and availability targets; and
- 6) 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

4.4.1 General

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 plant fault; and
- c) the potential consequences of each plant fault 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, and 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 determine the degree of attention to quality and safety assurance 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 documentation 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 supplementary control room (SCR), and their role in safety, should form part of the I&C design basis, and 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.

4.4.2 Postulated plant fault conditions

COMMENTARY ON 4.4.2

A highly conservative approach might be appropriate for some aspects of the design dependent on the reactor type and associated safety case, so 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](#) for further recommendations on information systems and alarms.

Indication should be given when plant conditions deviate from normal.

4.4.3 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.

4.5 Management systems and quality assurance processes

A standard format and identification system for each level of the design documents should be established and 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 verification and validation (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 assurance.

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 provide nuclear safety.

4.6 Examination, inspection, maintenance and testing

NOTE 1 IAEA and Office for Nuclear Regulation's (ONR) principles and guidance require the performance of a regime of examination, inspection, maintenance and testing (EIMT) to ensure that the levels of reliability and availability of structures, systems and components (SSC) important to safety remain in accordance with the assumptions in the design basis.

As part of overall plant EIMT it is normal for the I&C system to be subject to periodic testing to verify it is fault free and operating reliably (surveillance testing); a surveillance testing programme should be established to verify that the levels of reliability and availability of SSCs important to safety remain in accordance with the assumptions and intent of the design throughout the design life of those SSCs.

NOTE 2 Diagnostic tests are a subset of surveillance testing used to confirm the continued operation of I&C systems within their assumed performance and to confirm the absence of faults. Diagnostic tests could be built into the I&C system (sometimes referred to as "on-line") or be periodically carried out by temporary connection of external test equipment. Built-in tests could be continuous or periodic. Tests carried out using external equipment could be performed while the I&C system is on-line, performing its safety function or it might be necessary to take the system off-line to carry out the test(s).

The reliability calculations for the I&C system should take into account the diagnostic tests performed. Where these are periodic, suitably pessimistic intervals should be assumed to allow for uncertainty. The reliability of the tests themselves should be taken into account.

Where systems have to be taken off-line for testing, redundancy and by-passes should be included, where necessary, to allow for continued safe plant operation if the test interval cannot be aligned with a period, such as refuelling where the I&C system might not be required. The plant safety analysis should take into account these configurations in its reliability analysis.

Where diagnostic tests require the connection of external equipment, the potential effects on plant safety of faults within that equipment should be determined. If deemed necessary, suitable interfacing protection should be provided.

Test equipment should be of suitable quality and be subject to safety classification. Where it might interfere with the proper operation of the I&C system, it should be assigned the same class as that system.

Where an I&C system is taken off-line for testing, there should be a means of confirming that it has been returned to operation correctly.

4.7 Systems dependent on computer software

COMMENTARY ON 4.7

The use of software in safety systems in 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 is critical to the functional reliability that can be achieved and demonstrated since it defines the relationship and influence between the many system and sub-system components. The selection of the technology to be used in each of these I&C systems and sub-systems is a key decision that can have serious implications for the achievement of the I&C functional and reliability requirements as well as other aspects of the programme.

See [Annex A](#) for IAEA and other relevant nuclear safety standards.

4.7.1 General

The use of computer-based designs in safety and safety-related systems should be justified formally, taking account of the potential benefits of such systems versus the difficulties that might arise in their safety assurance and licensing. Designs based on the use of hardware description languages (HDL) should be treated in the same way.

The reliability requirements of computer-based safety and safety-related systems should be derived from the risk reduction that the I&C system is required to achieve. The safety functions implemented by these systems should be categorized and the safety systems classified in accordance with recognized National and International Standards.

Computer-based safety and safety related systems should be designed and documented so that the assignment and execution of I&C functions are clearly traceable and that 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 and safety related systems should be designed to minimize the potential for common cause failure (CCF) by the implementation of diversity (e.g. hardware, design of software and its implementation), including the consideration of a diverse I&C system. The guidance given in [BS EN 61513](#) should be taken into account.

NOTE 1 Attention is drawn to the ONR Nuclear Safety Technical Assessment Guide [2] for the design and licensing of computer-based safety systems for nuclear power plants. Although written for use by the ONR's assessors, this document provides the designer with the current regulatory expectations for the licensing of I&C systems that employ computer software.

The standards, methods and practices adopted should be consistent with the required reliability of the I&C system, with particular emphasis placed on the following aspects:

- a) available good practices;
- b) top-down design methods;
- c) comprehensive verification of each design phase; and
- d) thorough validation testing.

Good practices should be identified by taking account of the guidance and recommendations in the appropriate National and International Standards

NOTE 2 See [Annex A](#), and in particular [BS EN 60880](#) and [BS EN IEC 62138](#).

The design, V&V and production processes for the computer-based safety and safety-related systems should be selected with the objective of providing robust evidence that the design meets all the requirements with high levels of safety assurance.

Modifications to the software in a computer-based safety system, including configuration data, should be verified and validated before being placed into service.

Computer software should include robust protection so that spurious, unauthorized or malicious software cannot be included or introduced into a system which depends on software.

The design of computer-based systems should include a cybersecurity programme to minimize the cyber threats to safety. Guidance should be sought from the relevant National and International Standards, including the need to take account of the potential interaction between safety and security.

4.7.2 Practices and methods

Good methods, tools and practices should be selected based on guidance and recommendations in appropriate National and International Standards. Alternative and new methods, tools and practices should be justified formally in accordance with these standards.

The methods, tools and practices should cover the total life cycle and provide comprehensive evidence of correct implementation and usage. The following should be selected:

- a) good methods, tools and practices 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 verify the application of good methods, tools and practices (see [Annex A](#));
- b) a quality assurance programme and plan, meeting appropriate quality assurance standards;
- c) a comprehensive testing programme 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; and
- d) a V&V programme of the computer-based safety system to demonstrate that the system can meet the reliability requirements.

An independent review should be undertaken of the complete design and production process to check that the product meets the specification and that the tools, methods and practices employed have been correctly applied.

This review should include an independent assessment of the supplier's V&V test programme. This should cover all test phases and include a review of the traceability of the requirements through the design, development and production stages.

4.7.3 Additional validation test evidence

In some circumstances, it might be appropriate to generate additional independent evidence for the design and safety assurance of the I&C system, particularly for those systems implementing category A functions with onerous reliability claims; these additional assessments should conform to the guidance and recommendations in the appropriate National and International Standards (see [Annex A](#)).

For the most significant safety systems with the most onerous reliability claims, these assessments should include a complete check of the final, validated production software undertaken by an independent team. This could include a detailed and probing analysis of the software, using proven methods and qualified tools which conform to appropriate National and International Standards (see [Annex A](#)); such activities should be graded based on the safety significance of the system.

The independent teams should be sufficiently independent of the I&C system's supplier (or suppliers), particularly the supplier's internal V&V teams. Evidence should be documented to justify the level of independence.

4.8 Hardware description language programmed device

COMMENTARY ON 4.8

The unique term used for programmable logic within the nuclear industry is Hardware Description Language (HDL) Programmed Device (HPD). HPDs provide a digital technology for safety and safety related applications within NPP I&C. Blank HPDs are available from many manufacturers, providing differences in the fundamental technology and types of native block. The most common types of blank HPD electronic component are Field Programmable Gate Arrays (FPGA) and Complex Programmable Logic Devices (CPLD).

Modern HPD hardware architectures allow for greater functional capabilities that can implement simple to complex safety functions. When compared to other digital solutions using microprocessors, HPD solutions can be made simpler, more testable, and easier to qualify. The IAEA document, Application of FPGAs in Instrumentation and Control Systems of Nuclear Power Plants NP-T-3.17 [3] provides a description of the HPD technology.

A HPD is an integrated circuit that contains native blocks that can be user-configured and interconnected to implement an application produced in a HDL or using a higher system level software tool.

A HDL design is typically a mixture of pre-developed blocks (PDB) and application specific blocks. The specific HPD configuration is produced from the HDL design using a series of complex software tools.

In terms of regulatory assessment only, HPD-based systems are treated in the same way as software-based systems (see 4.7).

HPDs should be developed and verified to their own specific standards rather than to a software standard.

The selection of an appropriate blank HPD electronic component should be determined and the reasons for the selection justified.

The HDL design should be a transferable design not dependent on specific HPD hardware architecture features.

The HPD should be developed and verified using a rigorous process, graded depending on the safety category. The development and verification process for a HPD should be in accordance with [BS EN 62566:2014](#) for category A functions and [BS EN IEC 62566-2:2020](#) for category B and category C functions.

If the developed HPD contains an embedded processor native block or PDB, the software application running on that block should be developed in accordance with [BS EN 60880:2009](#) for category A functions and [BS EN IEC 62138:2019](#) for category B and category C functions. The software application development and verification should be in accordance with 4.7.

4.9 Equipment qualification

COMMENTARY ON 4.9

Equipment 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.

I&C systems should be subject to appropriate equipment qualification to provide assurance of their capability to perform 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, tests should be carried out on equipment that has been suitably aged prior to testing.

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

NOTE 1 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 within the normal environment, including equipment emissions and potential interference from wireless systems.

I&C systems should not emit EMI levels sufficient to affect the operation of other systems. The design should identify requirements for cable routing, screening and earthing arrangements. Margins between equipment susceptibility levels and the EMI environment in which equipment resides should be maintained.

NOTE 2 The use of wireless technology, radio communications or equipment with high EMI emissions might need to be prohibited in areas where equipment is located that has not been demonstrated to have suitable immunity to generated EMI.

4.10 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.

NOTE 1 See 3.1.3 for a description of levels 1 to 4 of the defence in depth that apply to the I&C.

The following rules should be met:

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

The I&C system architecture should include redundant units, modules and power supplies from redundant sources. The architecture should be designed such that safety groups of equipment performing the safety functions are separated so that failure to operate 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 2 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 3 BS EN IEC 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 4 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, cabling, marshalling, 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.

4.11 Reliability assessment and calculation

COMMENTARY ON 4.11

The safety systems of NPPs are subjected to reliability assessment so that 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 typically done by placing limits on the claimed reliability of such systems and combinations of systems.

The design of I&C systems and equipment should be demonstrated 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 which accommodate 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) an 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 safety function 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.

The quality of the data used within the reliability analysis should be consistent with the required confidence level of the overall reliability analysis.

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 verify 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.

4.12 Human factors

COMMENTARY ON 4.12

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, addressing:

- 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 human machine interface (HMI), both for the control room areas and for local-to-plant functions.

HMI facilities and operating procedures should be reviewed so that safety claims can be met. Assessments should be undertaken to verify 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 4.13).

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 allow the operator to assess and confirm that conditions in the power plant are safe.

4.13 Safety and control arrangements for abnormal operation – Commissioning, fuel loading, maintenance, modification and testing

COMMENTARY ON 4.13

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).

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 safety threats that could occur, so 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 so that 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 verify 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 [8.1.5](#).

For commissioning and fuel loading operations, communication systems should be available to provide 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.

4.14 Cybersecurity

Cybersecurity risks which could impact I&C systems should be identified, assessed and documented, e.g. in a security risk assessment (SRA). Cybersecurity risks should be managed throughout the I&C life cycle.

Security requirements to address cybersecurity risks should be identified and documented, e.g. in a security requirements statement (SRS). The security requirements should include technical, procedural and personnel security requirements such that cybersecurity risks are mitigated to an acceptable level, with non-technical requirements integrating with technical requirements.

The technical security requirements should be used as input to the I&C system life cycle, I&C platform and I&C architecture, such that the resulting I&C security design contributes effectively to cybersecurity risks mitigation.

I&C systems should be designed to conform to the technical security requirements to improve resilience to cybersecurity threats. The impact of the security design on the I&C system safety and performance should be assessed in accordance with [BS EN IEC 62859](#).

Security arrangements during the design, development, manufacture, factory test, shipping, storage, installation and commissioning phases should be implemented so that appropriate controls are in place to minimize the cybersecurity risks to the systems.

Security of the I&C supply chain facilities and services should be assessed against a relevant security standard to verify that appropriate controls are in place to minimize the cybersecurity risks to the systems.

A security justification, i.e. security case should be produced that demonstrates the level of cybersecurity risk mitigation achieved, through the examination of compliance of the relevant security requirements against each risk.

Where risk mitigation shortfalls are identified, remedial measures and mitigations should be put in place to manage cybersecurity risks.

Impact assessments should be performed for I&C systems design changes to determine their impact on cybersecurity and existing security justifications.

4.15 SMART devices

COMMENTARY ON 4.15

Discrete devices (e.g. sensors and contactors) with electronics packaged with them (known as SMART Devices) are becoming increasingly prevalent in conventional markets and high integrity industries, such as oil and gas. These devices offer a number of benefits over dumb devices, such as self-test fault reporting and calibration functions. SMART devices therefore, by their nature, contain processing of some sort (in most cases digital electronics and/or software). They need to be analysed appropriately. Of particular interest is signal processing as this can introduce more subtle failure mechanisms than dumb devices. For a SMART sensor this could be a corrupted calibration curve while an actuator might simply report its status erroneously. It is important to understand any new failure mechanisms a SMART device might introduce over and above a dumb equivalent. Of particular interest are subtle failures of a common cause nature that could undermine functionality of more than one device in a system at the same time.

Where SMART devices are considered for use, the complexity of the functionality, signal processing and failure modes of the device itself should be taken into account alongside the safety significance of its function.

NOTE 1 As device complexity and failure modes increase, the rigour and variety of qualification methods required also increases.

NOTE 2 SMART devices are also capable of making control decisions (e.g. trip functionality) and having multiple outputs (e.g. data or power switching). Placing increasing amounts of system functionality in a single device can provide a simpler system architecture design. However, as more system functionality is concentrated into a single device, the reliance on that devices predictable behaviour increases.

When designing a system that contains SMART devices, the amount of system functionality placed in a single device should be assessed as part of the system architecture alongside its safety significance.

NOTE 3 As architectural reliance on a single device increases, the rigour and variety of qualification methods required also increases.

When selecting and qualifying a SMART device for use, the following should be taken into account:

- a) willingness of device vendors to share information over and above that typically available to support assessments;
- b) robustness of the design development process of the device, including documented evidence;
- c) variety and coverage of functional testing of the configured device;
- d) cybersecurity regarding the ability to change functionality from that intended to obtain information of a sensitive nature;
- e) through-life management of the device with respect to security and functional device patches;
- f) expected availability duration (e.g. time until obsolescent); and
- g) device design changes (hardware or programmed configuration) over time away from the baseline established at initial qualification.

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 Nuclear Safety and Security 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

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 so 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. The system continues to monitor and operate when the reactor is 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 engineered safety feature (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.

Nuclear power plants should include an automatic reactor protection system which should initiate a controlled shutdown if reactor conditions pass limiting safe values. The automatic reactor protection system should provide protection such that the likelihood of radiation hazards to the public and plant is 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 advanced gas-cooled reactor (AGR).

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