AERB SAFETY GUIDE NO. AERB/NPP-PHWR/SG/D-20

SAFETY RELATED INSTRUMENTATION AND CONTROL FOR PRESSURISED HEAVY WATER REACTOR BASED NUCLEAR POWER PLANTS

Atomic Energy Regulatory Board
Mumbai-400 094
India

January 2003

Price:

Orders for this Guide should be addressed to:

Administrative Officer
Atomic Energy Regulatory Board
Niyamak Bhavan
Anushaktinagar
Mumbai-400 094
India

FOREWORD

Activities concerning establishment and utilisation of nuclear facilities and use of radioactive sources are to be carried out in India in accordance with the provisions of the Atomic Energy Act 1962. In pursuance of the objective to ensure safety of members of the public and occupational workers as well as protection of environment, the Atomic Energy Regulatory Board has been entrusted with the responsibility of laying down safety standards and framing rules and regulations for such activities. The Board has, therefore, undertaken a programme of developing safety standards, codes of practice and related guides and manuals for the purpose. These documents cover aspects such as siting, design, construction, operation, quality assurance, decommissioning and regulation of nuclear and radiation facilities.

Codes of practice and safety standards are formulated on the basis of internationally accepted safety criteria for design, construction and operation of specific equipment, systems, structures and components of nuclear and radiation facilities. Safety codes establish the objectives and set minimum requirements that shall be fulfilled to provide adequate assurance for safety. Safety guides elaborate various requirements and furnish approaches for their implementation. Safety manuals deal with specific topics and contain detailed scientific and technical information on the subject. These documents are prepared by experts in the relevant fields and are extensively reviewed by advisory committees of the Board before they are published. The documents are revised when necessary, in the light of experience and feedback from users as well as new developments in the field.

The 'Code of Practice on Design for Safety in Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/SC/D, 1989) lays down the minimum requirements for ensuring adequate safety in plant design. This safety guide is one of a series of guides, which have been issued or are under preparation, to describe and elaborate the specific parts of the code.

This guide is based on the current designs of 220 MWe and 500 MWe Pressurised Heavy Water Reactors. It prescribes guidelines for designing the safety related instrumentation and control systems of Pressurised Heavy Water Reactors.

Consistent with the accepted practice, 'shall', 'should' and 'may' are used in the guide to distinguish between a firm requirement, a recommendation and a desirable option, respectively. Appendices are an integral part of the document, whereas annexures, footnotes, references/bibliography and lists of participants are included to provide information that might be helpful to the user. Approaches for implementation different

to those set out in the guide may be acceptable, if they provide comparable assurance against undue risk to the health and safety of the occupational workers and the general public and protection of the environment.

For aspects not covered in this guide, applicable and acceptable national and international standards, codes and guides should be followed. Non-radiological aspects of industrial safety and environmental protection are not explicitly considered. Industrial safety is to be ensured through compliance with the applicable provisions of the Factories Act, 1948 and the Atomic Energy (Factories) Rules, 1996.

This guide has been prepared by specialists in the field drawn from Atomic Energy Regulatory Board, Bhabha Atomic Research Centre, Indira Gandhi Centre for Atomic Research, Nuclear Power Corporation of India and other consultants. It has been reviewed by the relevant AERB Advisory Committee on Codes and Guides and the Advisory Committee on Nuclear Safety.

AERB wishes to thank all individuals and organisations who have prepared and reviewed the draft and helped in its finalisation. The list of persons who have participated in this task, along with their affiliations, is included for information.

(Suhas P. Sukhatme)
Chairman,
AERB

DEFINITIONS

Acceptable Limits

Limits acceptable to the Regulatory Body for accident condition or potential exposure.

Accident Conditions

Substantial deviations from Operational States which could lead to release of unacceptable quantities of radioactive materials. They are more severe than anticipated operational occurrences and include Design Basis Accidents as well as Beyond Design Basis Accidents.

Anticipated Operational Occurrences

An operational process deviating from normal operation which is expected to occur during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to Items Important to Safety nor lead to Accident Conditions.

Availability

The fraction of time that an entity is capable of performing its intended purpose.

Channel (Instrumentation)

An arrangement of interconnected components within a system that initiates a single electrical output.

Common-Cause Failure

The failure of a number of devices or components to perform their functions, as a result of a single specific event or cause.

Design Basis Event

The set of events, that serve as part of the basis for the establishment of design requirements for systems, structures or components within a facility. Design basis events (DBEs) include normal operations, operational transients and certain accident conditions under postulated initiating events (PIEs) considered in the design at the facility.

Diversity

The presence of two or more different components or systems to perform an identified function, where the different components or systems have different attributes so as to reduce the possibility of common cause failure.

Engineered Safety Features

The system or features specifically engineered, installed and commissioned in an NPP to mitigate the consequences of accident condition and help restore normalcy, e.g., containment atmosphere clean-up system, containment depressurisation system, etc.

Functional Isolation

Prevention of influences from the mode of operation or failure of one circuit or system on another.

Independence

Independence of equipment, channel or a system is its ability to perform its function irrespective of the normal or abnormal functioning of any other equipment, channel or system. Independence is achieved by functional isolation and physical separation.

Items Important to Safety

The items which comprise:

(1) those structures, systems, equipment and components whose malfunction or failure could lead to undue radiological consequences at plant site or off-site;

(2) those structures, systems, equipment and components which prevent anticipated operational occurrences from leading to Accident Conditions;

(3) those features which are provided to mitigate the consequences of malfunction or failure of structures, systems, equipment or components.

Limiting Safety System Settings

Settings on instrumentation, which initiate the automatic protection action at a level such that the safety limits are not exceeded.

Operational States

The states defined under 'Normal Operation' and 'Anticipated Operational Occurrences'.

Physical Separation

A means of ensuring independence of equipment through separation by geometry (distance, orientation, etc.), appropriate barriers, or combination of both.

Postulated Initiating Events

Identified events that could lead to Anticipated Operational Occurrence or Accident Conditions and consequential failure effects.

Protection System

A part of Safety Critical System which encompasses all those electrical, mechanical devices and circuitry, from and including the sensors up to the input terminals of the safety actuation system and the safety support features, involved in generating the signals associated with the safety tasks.

Quality Assurance

Planned and systematic actions necessary to provide adequate confidence that an item or a facility will satisfy given requirements for quality.

Quality Control

Quality Assurance actions, which provide a means to control and measure the characteristics of an item, process or facility in accordance with established requirements.

Reactor Trip

Actuation of shutdown system to bring the reactor to shutdown state.

Redundancy

Provision for alternative structures, systems, components of identical attributes, so that any one can perform the required function regardless of the state of operation or failure of any other.

Reliability

The probability that a device, system, component or facility will perform its intended (specified) function satisfactorily for a specified period under specified conditions.

Response Time

The time required for a system component instrumentation to achieve a specified output state from the time that it receives a signal.

Safety Action

An action initiated by a protection system and completed by safety actuation system, with the help of safety support system to accomplish a safety task.

Safety Actuation System

A part of Safety Critical System, which encompasses all equipment, required to accomplish the required safety action when initiated by the protection system.

Safety Critical System
(See Safety System)

Safety System

System important to safety, provided to assure that under anticipated operational occurrences and accident conditions, the safe shutdown of the reactor followed by heat removal from the core and containment of any radioactivity is satisfactorily achieved (e.g., of such systems are : shutdown systems, emergency core cooling system and containment isolation system).

Safety Limits

Limits upon process variables within which the operation of the facility has been shown to be safe.

Safety Related Systems

Systems important to safety which are not included in safety critical systems and which are required for the normal functioning of the safety systems (e.g., power supplies, stored energy systems etc.).

Safety Support System

Part of safety critical systems which encompasses all equipment that provide services such as cooling, lubrication and energy supply (pneumatic or electric) required by the protection system and safety actuation systems.

Set-back

Controlled gradual reduction in power effected by Reactor Regulating System in response to an identified abnormality in one or more plant process variables, until the condition causing the set-back is cleared or the preset-limit for power rundown is reached.

Shutdown State

State of a reactor when it is maintained subcritical with specified negative subcriticality margin.

Single Failure

A random failure, which results in the loss of capability of a component to perform its intended safety function. Consequential failures resulting from a single random occurrence are considered to be part of the single failure.

Station Black Out

The complete loss of both off-site and on-site AC power supplies.

CONTENTS

FOREWORD i

DEFINITIONS iii

1. INTRODUCTION 1
   1.1 Objective 1
   1.2 Scope 2

2. DESIGN BASIS 6
   2.1 General 6
   2.2 Information Systems 8
   2.3 Control Systems 9

3. DESIGN REQUIREMENTS 13
   3.1 Independence 13
   3.2 Testability 14
   3.3 Maintainability 15
   3.4 Electrical (Electromagnetic and Electrostatic) Interference... 15
   3.5 Equipment Qualification 16
   3.6 Control Power Supplies 17
   3.7 Field Instrumentation 19

4. CONTROL ROOM 21
   4.1 Main Control Room 21
   4.2 Accident Monitoring 24
   4.3 Human Machine Interface 25
   4.4 Back-up Control Room/Points 26

5. LOCAL ALARM AND VOICE COMMUNICATION SYSTEMS.. 30

6. DOCUMENTATION 31

ANNEXURE-I: PROGRAMMABLE DIGITAL SYSTEMS 32

BIBLIOGRAPHY 37

LIST OF PARTICIPANTS 38

WORKING GROUP 38

ADVISORY COMMITTEE ON CODES, GUIDES AND ASSOCIATED MANUALS FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD) 39

ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS) 40

PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUAL ON DESIGN OF PRESSURISED HEAVY WATER REACTORS 41

1. INTRODUCTION

1.1 Objective

1.1.1 The term 'Instrumentation and Control' (I&C) is used as a collective term to encompass all instruments, equipment, systems and support features intended to monitor, control and protect the Nuclear Power Plant (NPP).

1.1.2 The safety guide on 'Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors' (AERB/SG/D-1) contains a list of safety functions that shall be accomplished and which would help to decide whether a particular I&C system is important to safety. The I&C systems important to safety comprise of

- Those systems, structures and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public.
- Those systems, structures and components that prevent Design Basis Events (DBE) from leading to Accident Conditions.
- Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

1.1.3 The safety classification of I&C systems is elaborated in AERB-SG-D-1. The instrument items and other hardware of I&C systems shall meet the requirements of the specified class.

1.1.4 The defence in depth for I&C systems is provided by dividing the items important to safety into two categories, viz. i) safety-related systems and ii) safety critical systems (see Fig.1). The safety-related systems form the first layer of safety to operate the plant in a safe manner and to minimise the need for actuation of safety critical systems. These include systems like reactor regulating system, primary heat transport system, etc. The safety critical systems form the second layer of defence and are provided to assure safe shutdown of the reactor, removal of heat from the reactor core during any deviation from normal operation and containment of radioactivity during accident conditions. The safety critical systems require a higher reliability and have three parts, viz. protection system, safety actuation system and safety support systems. The reactor shutdown systems, emergency core cooling system and containment isolation system are classified as safety critical systems.

1.1.5 The safety related I&C includes the control systems and information systems, which are necessary to operate the plant within the limiting conditions of operations and thus not necessitating the actuation of the safety critical systems. The systems and features specifically engineered to mitigate the consequences of an accident situation, having been brought under control by the actuation of one or more of the safety critical systems, also fall under the safety related I&C. A few I&C systems, which may be the principal means of accomplishing certain safety functions, such as spent fuel storage bay cooling, may still be classified as safety related, based on the consideration that sufficient period of time is available for corrective action, in case the control systems fails.

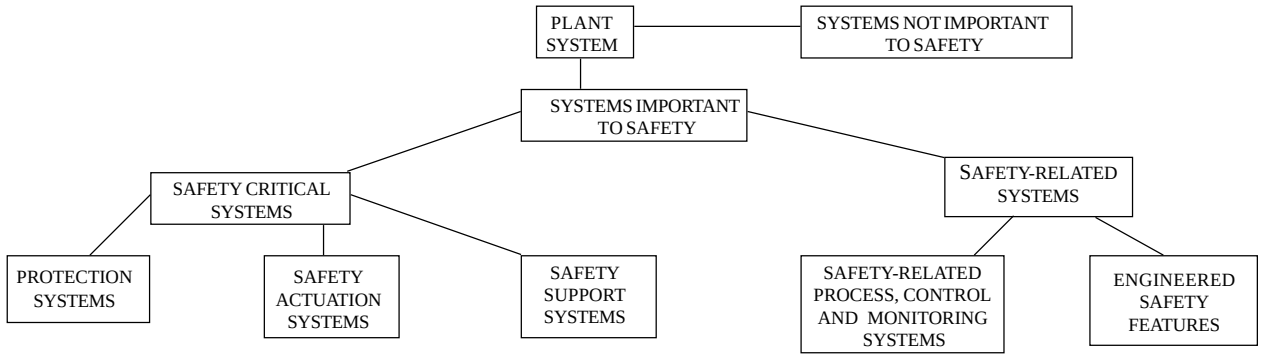
1.2 Scope

1.2.1 This safety guide deals mainly with generic design requirements for the safety-related instrumentation and control systems and is intended to expand relevant paragraphs of the 'Code of Practice on 'Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants' (AERB Code, AERB/SC/D). The necessary actuation devices to perform control actions and the associated system support features are also included within the boundaries of safety related I&C. Instrumentation and Control for safety critical systems are covered in the safety guide AERB/SG/D-10 on safety critical systems.

1.2.2 Guidelines regarding the application of the digital computers in this area are covered in safety guide, AERB/SG/D-25 on computer-based safety systems. Reference may also be made to Annexure-I attached to this guide.

1.2.3 The term 'I&C' refers to safety-related I&C in the rest of this guide. This guide is supplemented by other associated guides where specific I&C systems are covered such as on 'Fire Protection in Pressurised Heavy Water Based Nuclear Power Plants' (AERB/SG/D-4), 'Radiation Protection in Design' (AERB/SG/D-12), 'Primary Heat Transport System for Pressurised Heavy Water Reactors' (AERB/SG/D-8), Core Reactivity Control in Pressurised Heavy Water Reactors' (AERB/SG/D-7), 'Fuel Handling and Storage Systems for Pressurised Heavy Water Reactors' (AERB/SG/D-24), etc. Typical safety-related I&C systems are listed below.

(a) Reactor regulation which controls the reactor power level by reactivity control (either by positioning the control rods or by controlling the poison concentration in the moderator).



Examples:

Sensors, signal conditioners and logics for

i. Reactor shutdown

ii. Emergency core cooling

iii. Containment isolation

Examples:

- Shut-off rods and mechanisms
- Liquid poison injection devices
- Containment isolation dampers
- Emergency core cooling system,
- Valves and motors

Examples:

- Emergency power supply
- Pneumatic supply
- Cooling water supply

Examples:

- Reactor regulating system
- Primary heat transport system
- Shutdown cooling system
- Steam generator pressure I&C
- Safety critical system status monitoring
- Fuel handling and storage system
- Radiation monitoring systems
- Fire detection and extinguishing system
- Communication system
- Access control system

Examples:

- Primary containment clean-up system
- Primary containment controlled depressurisation system
- Secondary containment re-circulation and purge system
- Containment heat removal system

FIG.1: CLASSIFICATION OF SYSTEMS IMPORTANT TO SAFETY

(b) PHT system pressure control, which maintains the pressure of the primary coolant within set limits.

(c) Steam generator level and pressure control, which control the feedwater flow to maintain level and the steam drawn through turbine governor valves, etc., to maintain the pressure within set limits.

(d) Primary coolant temperature monitoring, both bulk and coolant channelwise.

(e) Shutdown cooling system I&C.

(f) Moderator system I&C.

(g) Operator information systems that monitor the safety critical and safety-related plant parameters and provide displays and annunciations to the operator.

(h) Surveillance of the safety critical system.

(i) Monitoring the status of the core in the shutdown state and during reactor start-up from the sub-critical state.

(j) Process water systems I&C associated with core heat removal.

(k) Detection and monitoring of PHT system/moderator system leakages.

(l) Monitoring of pressure tube integrity (e.g., annulus gas monitoring system).

(m) Detection and location of failed fuel.

(n) Fuel handling controls.

(o) Radiation monitoring.

(p) Waste management and spent fuel cooling instrumentation.

(q) Reactor building ventilation and survival ventilation systems for main control room and control equipment room I&C

(r) Dedicated communication system amongst main control room (MCR), back-up control room (BCR) and back-up control points (BCPs).

(s) Fire detection and suppression system I&C.

(t) Access control.

(u) Seismic monitoring.

(v) Systems, other than safety critical systems, that perform functions important to safety, such as prevention, termination or mitigation of anticipated operational occurrences or accident conditions, e.g., reactor power setback/ stepback systems and systems for post-accident containment clean-up, controlled depressurisation of containment, reactor building cooling, etc.

(w) Accident monitoring and assessment.

1.2.4 The above does not provide a complete list and the order of the above listing does not imply any gradation in the importance to safety of these I&C systems. It is possible that the functions of some of the above systems could be collectively met by one or more computer-based systems. Designer shall identify the safety-related systems and the safety classifications as per design guide, AERB/SG/D-1 on 'Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors'.

2. DESIGN BASIS

2.1 General

The I&C systems shall be designed for

- performance consistent with design bases and the safety requirements assumed or derived from the safety analyses;
- the environments in which they operate; and
- a reliability consistent with their importance to safety.

2.1.1 Performance

For each operating condition of concern, the I&C requirements shall be defined, so as to determine the performance requirements, such as range of the measured variable, accuracy, response time and output signal levels. The relationship between the instrument and the process units shall be taken into account. Whenever the range of control is maintained by overlapping instrument channels, appropriate interlocks shall be provided in the increasing and decreasing directions for automatic selection of the required range or provide clear alarm for operator action. Factors like instrument saturation, overload and fold over should not cause loss of accuracy over the entire signal range. The effects of transient and normal variations in power supply characteristics (e.g., voltage, frequency) and instrument air pressure, grounding and signal transmission losses shall be assessed in the design of the I&C systems to the extent necessary to ensure that they satisfactorily perform their safety related functions.

2.1.2 Environmental Conditions

The environmental conditions which an I&C system is required to withstand and the expected duration of operation under such conditions, shall be specified for operational states and accident conditions. Environmental conditions such as extreme temperatures, pressure, humidity, dust, ionising radiation, electromagnetic interference, corrosion, vibration, fatigue and stress shall be considered. Consideration shall be given to the hostile environmental conditions that may prevail in the locations for field-mounted instruments. Credit may be taken for the controlled environmental conditions maintained in areas like main

control room and control equipment rooms. The system shall, however, perform for such durations as may be specified, under the extreme conditions, which may result from a likely loss of such environmental control, e.g., failure of air-conditioning.

2.1.3 Reliability

2.1.3.1 Reliability of an I&C system shall be commensurate with its classification given in 1.1.3 and the importance of the intended safety function. While specifying the reliability of an I&C system as an input for design, the relative importance of the system to nuclear safety should be assessed based on the following factors:

- The nature of Design Basis Events (DBE) and potential severity of their consequences in the event of the I&C system failing.
- The period available between the occurrence of the DBE and the time taken for initiation of the safety function.
- The promptness and reliability with which alternative actions can be taken.
- The time taken for repair of the I&C system.

In general, reliability targets should be fixed based on PSA studies.

2.1.3.2 One approach to specify required reliability is to assign a numerical unavailability figure to each system with due consideration to factors mentioned above. Another approach is to specify graded, non-numerical availability requirements for the various systems. For achieving the reliability requirements, factors such as component failure rate, on-line and off-line test facilities, test frequency, repair time, accessibility for fault location and repair, power source failures and common cause failures shall all be taken into account.

2.1.3.3 In practice, a certain amount of 'trade off' amongst some of these factors may be necessary in order to optimise goals, such as minimising outage time for repair and reducing frequency of testing.

2.1.3.4 The reliability of an I&C system can be enhanced by the use of

- redundant channels of identical components or
- diverse channels using different principles, e.g., monitoring reactor power

using thermal neutron flux, or coolant temperature and flow measurements.

2.1.3.5 Redundancy shall be employed wherever single failure criterion is to be met. The applicability of this aspect to safety-related I&C depends on the relative importance of that system to nuclear safety as explained earlier. As a minimum, use of redundant channels to guard against single failure may be applied to such safety-related I&C systems whose failure may put an immediate demand on the protection system to act (e.g., systems 1 to 3 of the list in Section 1.2.3).

2.2 Information Systems

2.2.1 Information for Operators

2.2.1.1 During normal operation, the operators monitor the plant status continuously with a set of displays, annunciators and CRTs, which are provided in the main control room.

2.2.1.2 Deviations from normal operation are indicated by audio-visual devices such as alarm windows and CRTs. When these occur, the operators shall be aided by the information systems to:

- know the actions being taken by automatic systems
- analyse the cause of the disturbance and follow the subsequent changes in plant performance
- perform any manual actions within the specified time as demanded by the system design.

2.2.1.3 The information systems inputs may be generated from dedicated sensors or taken from control systems/ protection systems and connected to display devices. These inputs may also be processed in a computer-based information system for display on CRTs. In the latter case, inputs from redundant channels may terminate in a single system. In such cases, consideration must be given for maintaining channel integrity by suitable isolation devices. If the control systems are safety related and also computer-based, independence of both hardware and software between the control and information systems should be achieved by design to preserve the reliability of the control systems. For convenience of the operator, several CRTs for display of demanded information may be

distributed over a range of panels. Alarm displays should be covered by one or more dedicated CRTs at a central location for display of alarms only.

2.2.2. Recording and Printing

2.2.2.1 Adequate records or printouts for analogue process variables and for binary signals shall be generated and maintained in order to provide available chronological information about the performance and behaviour of the plant which is necessary for the following purposes:

- back-up information for shift operators (giving short- and long-term trends),
- general operational information for the plant management,
- analysis of design basis events.

2.2.2.2 Wherever multiple computer-based systems are used, the real time on all such systems should be synchronised at regular intervals to a centralised real time master clock source.

2.3 Control Systems

2.3.1 Maintenance of Process Variables within Specified Limits

For assumptions of the safety analysis to remain valid, certain plant parameters must be held within specified limits. The probability that the parameters of concern remain within these limits is based on the reliability of the I&C sysems. The design of these control and monitoring systems shall be such that, in combination with stipulated operator actions, process variables are maintained within the limits used in safety analysis.

After installation and commissioning of the I&C systems, fine tuning of various control system settings may be necessary for optimal performance. The transient and steady state performance of the plant systems in maintaining the set limits will be affected by this tuning. The dynamic performance of the control system should be assessed after such tuning to maintain the control band.

2.3.2 Set Points

The safety-related I&C systems ensure the operation of the plant within a prescribed safe operation region. In response to initiating events, including the failure of control systems, the plant may migrate beyond the safe operation

region. Thresholds are to be set in safety, or safety-related I&C systems to bring the plant back to the safe state or to initiate safety action before any significant damage is done to the plant.

2.3.2.1 The bases for selection of trip set points shall be documented and shall include data, assumptions and the method of analysis. The data used shall be taken from engineering analysis, vendor design specifications, equipment qualification tests, laboratory tests and operating experience. Any assumptions used, such as ambient temperatures during equipment calibration and operation, shall be clearly identified. In protection system channels, sufficient allowance/margin shall be provided between the trip set point and the safety limit to ensure that the safety systems are actuated before reaching safety limits. This is done by taking into account the inaccuracies of actuation equipment and I&C systems and the dynamic responses of process systems.

2.3.2.2 The inaccuracies include:

(a) Instrument calibration uncertainties caused by

- calibration standard
- calibration equipment
- calibration method

(b) Instrument inaccuracies during normal operations and also during specified design basis event in caused by :

- any internal reference inaccuracy, including conformity to input-output relations, hysterisis, dead band and repeatability,
- power supply voltage changes,
- power supply frequency changes,
- temperature changes,
- humidity changes,
- pressure changes,
- vibration (in-service and seismic),

- radiation exposure,
- analogue to digital conversion.

(c) Instrument drift

(d) Process-dependent effects

The determination of the trip set point allowance shall account for uncertainties associated with the process variable. Examples include the effect of fluid stratification on temperature measurement, the effect of changing fluid density on level measurement, and process oscillations or noise or frequency change.

(e) Calculation uncertainties

The determination of the trip set point allowance shall account for uncertainties resulting from the use of a mathematical model to calculate a variable from the measured process variables; for example, the use of differential pressure to determine flow.

(f) Dynamic effects

The determination of the trip set point allowance shall allow for response delays in the instrument channels. The instrument channel response time shall be no more than the limiting response time required by the safety analysis.

2.3.2.3 Some or all of the above factors contribute to the inaccuracies of the outputs received. One of the following methods should be adopted for combining the inaccuracies, depending on the conservatism required for a particular function:

- Square-root sum-of-squares method

  When two independent uncertainties, (±a) and (±b), are combined by this method, the resulting uncertainty is $(a^2 + b^2)^{1/2}$.

- Algebraic method

  The combination of two independent uncertainties, (+ a,-0) and (+0,-b), results in a third uncertainty distribution with limits (+a,-b).

- Probabilistic and statistical methods

  The interaction of dependent and independent uncertainties can be simulated by developing a stochastic model and inferring the combined uncertainties.

2.3.2.4 Sufficient margin/allowance shall be available between the trip set point and control system set points and control band. The above principles of determining the trip set points is to ensure that the safety systems are not demanded to act frequently because of uncertainties of the control system response and set points.

2.3.2.5 The dynamic performance of the safety systems after actuation, based on the set points, shall be assessed to get the transient response. This provides inputs for correction of set point of the protection systems to ensure that safety limits are not exceeded.

2.3.2.6 The testing of a system or a chain of equipment, with set points, must provide for testing the accuracy of the set point. Changing of set points for the purpose of demonstrating initiation of safety action shall normally not be done. Adequate technical/administrative procedures must exist for restoration of the set points to the original values after testing, in case such changes are done in set points.

2.3.2.7 As applicable, arrangements such as locking/administrative measures shall be provided for set points to safeguard against unauthorised tampering of the set points. Software locks, such as password, are normally provided for computer-based systems. In addition to this, a manual locking device should be provided for computer-based systems. Guidance for software systems is given in AERB/SG/D-25.

3. DESIGN REQUIREMENTS

3.1 Independence

Independence of a system/channel from other systems/channels is achieved by

- functional isolation,
- physical separation.

Certain areas in the plant tend to become natural centres of convergence for equipment or wiring. In these areas the extent to which independence might be lost following certain DBEs shall be carefully ascertained for establishing an overall design that shall meet the reliability requirements.

3.1.1 Functional Isolation

3.1.1.1 Functional isolation of a system/channel is required to restrict or prevent adverse interactions between equipment and components of other systems caused by electromagnetic interference, electrostatic pickup, short circuits, open circuits, earthing and application of the maximum credible AC or DC potential, mechanical interaction, etc. This is achieved by provisions such as electrical and optical isolating devices, cable shield, mechanical barriers or suitable devices.

3.1.1.2 The following equipment/channels of systems shall be functionally isolated from each other:

- Equipment, interconnecting cables and support features of a safety critical system, and those of a safety-related system.
- Equipment, interconnecting cables and support features of a safety-related system, and those of a system not important to safety.

In any of the above cases, if the same equipment is used for both the systems, then a functional isolation device (buffer) shall be provided at the connection between these systems. This isolation device (buffer) shall be classified as part of safety critical system or safety-related system, as the case may be. This need not apply for support features like compressed air supply in the latter case.

3.1.1.3 The power sources used to supply electrical, pneumatic or hydraulic power

shall meet the requirements given in section 3.6 to prevent the degradation or loss of functional isolation caused by failure of these power sources.

3.1.2 Physical Separation

3.1.2.1 The physical separation of systems/channels reduces the likelihood of common-cause failures resulting from events such as fires, missiles, high energy pipe breaks etc. (Ref. AERB/SG/D-3). This may also reduce the likelihood of errors committed inadvertently during operation or maintenance work in any portion of a system. The physical separation is achieved by distance, barriers or combinations of the two.

3.1.2.2 Physical separation shall be ensured amongst the equipment, cables and support features of the redundant channels of either safety-related or safety critical systems. However, equipment and cables of a redundant channel of a safety-related I&C system and that of a redundant channel of a safety critical system may be located in the same area. This area shall be physically separated from other redundant channels/equipment areas so that no criss-crossing of cables with different channels occurs. Similarly equipment and cables of a single channel safety-related I&C system may be associated with one of the redundant channels of a safety-related I&C system.

3.1.2.3 A single instrumentation cable shall not contain wires belonging to independent systems. A common junction box shall not be used for terminating wires belonging to independent systems.

3.1.2.4 Instrument cables and cable trays should be physically separated from power cables and power cable trays. For further details, refer to AERB/SG/D-11 on 'Emergency Electrical Power Supply Systems for Pressurised Heavy Water Reactors'.

3.2 Testability

3.2.1 I&C systems important to safety, particularly in-core equipment, should have test and calibration facilities, based on equipment function, expected drift and need for recalibration. This shall permit test and calibration at intervals as required and shall be capable of being performed in-situ with a minimum effort. Built-in test facilities for overall system checks from sensors, where appropriate,

are preferred. All the output functions of the system should be testable, for example, alarms, control actions and operation of actuation devices if these have a bearing on plant safety.

3.2.2 The frequency of testing of equipment/systems shall be determined based on reliability analysis and experience.

3.3 Maintainability

3.3.1 The equipment shall be designed for periodic surveillance and easy maintenance.

3.3.2 The mean time to repair (MTTR) and the frequency of inspection shall be defined in the design bases of the I&C systems. The effectiveness of the means for detecting and annunciating a failure shall be taken into account in evaluating the contribution to unreliability.

3.3.3 To facilitate maintenance, I&C systems shall, where practicable, be located so as to minimise risks to operating personnel. Enough room should be left around the equipment to ensure that the maintenance staff can fulfil its task under normal working conditions. Where practicable, equipment should not be located near points of high radiation level, or where conditions of extreme temperature or humidity normally exist. Wherever frequent removal of equipment/component from service is anticipated for maintenance or testing, an audio-visual annunciation of removal shall be provided in the control room. The indication shall identify the safety-related channel whose performance is affected, but need not identify the equipment removed from service. For those items whose removal from service is expected to be infrequent, administrative controls alone may suffice.

3.4 Electrical (Electromagnetic and Electrostatic) Interference

3.4.1 Electrical interference in a power plant could be due to switching transients and operation of power circuits, lightning strikes, leakage currents and the use of radio frequency communication apparatus. Such sources may be transient or of a continuous nature and may have a range of frequencies. I&C systems shall be designed for compliance to appropriate standards for electrical interference, such as MIL STD, 461.

3.4.2 Features such as screening, usage of specially shielded cables, physical separation of signal cables from power cables, filtering, optical coupling and earthing shall be incorporated within the I&C systems in order to reduce the effects of electrical interference to an insignificant level. Equipment operating at very low signal levels (like radiation detection sensors, thermocouples, resistance temperature detectors, etc.) are particularly vulnerable to interference. Ground loop currents between interconnected pieces of equipment with multiple grounding can cause unwanted voltage signals. To avoid this, all system equipment are so interconnected as to avoid ground loops. The I&C grounding shall be independent of grounding connections used for electrical power equipment and lightning protection. In the case of I&C systems, which are expected to be vulnerable to interference, tests shall be carried out to verify that they conform to design requirements.

3.5 Equipment Qualification

3.5.1 A qualification programme shall be provided to confirm that I&C equipment is capable of meeting, on a continuing basis, the design basis performance requirements (e.g., range, accuracy, response) needed for its function under the environmental conditions (e.g., temperature, pressure, vibration, radiation, humidity) likely to prevail at the time of the performance. These shall include the possible worst combinations of environmental conditions for periods of DBEs. Where the equipment is subject to natural phenomena or other external influences and is required to function during or following such an event, the qualification programme shall include the conditions imposed on the equipment by natural phenomena or other external influences. This will cover aspects like seismic qualification or LOCA qualification of respective identified pieces of equipment (refer AERB/SG/D-23 and AERB/SG/D-3).

3.5.2 In case where the design life of I&C equipment/components is less than the design life of the plant, mid-term, in-situ replacement of the I&C equipment/ components may be warranted. Adequate provisions should be made in the design, particularly for the in-core components, to facilitate such replacements. If the equipment function is still required beyond this qualification period, provision shall be made in design for removal and replacement with qualified equipment/components.

3.5.3 When protective barriers are provided to isolate equipment from possible environmental effects, the barriers themselves shall be subject to a qualification programme.

3.5.4 The following methods of qualification shall be used, either singly or in combination, to meet the above objectives:

- Performance of a test on the type of equipment to be supplied
- Performance of a test on the actual equipment supplied
- Use of pertinent past experience in similar applications
- Analysis based on reasonable engineering extrapolation of test data or operating experiences under pertinent conditions

3.5.5 The evidence derived from the chosen method of qualification shall be such that it shall provide a degree of confidence, commensurate with the importance of the equipment to nuclear safety.

3.5.6 All equipment shall undergo environmental chamber tests as per specified portions of IS-9000 or an equivalent standard and a burn-in test for a specified period to weed out infantile mortality. Shock and vibration tests should also be included to qualify for transportation and location of equipment.

3.5.7 Equipment required to be operable under seismic conditions shall be qualified to meet the requirements of AERB/SG/D-23 on 'Seismic Qualification' and IEEE -344 standard.

3.5.8 Equipment required to be operable under LOCA conditions in the plant shall be qualified by special tests or in special environmental chambers to meet the specified LOCA conditions. Cables used inside the containment and the cable penetrations should also be suitably qualified. Control cables used in containment building should similarly be qualified refer AERB/SG/D-11.

3.6 Control Power Supplies

3.6.1 Electric Power Supplies

The electrical power supplies shall meet the following.

- The quality of power supplies (frequency, voltage variation, voltage surges, ripples etc.) shall be compatible with the requirement of I&C

system and shall meet the same requirements as the I&C system they serve with respect to classification, qualification, isolation, testability, maintainability, etc.

- Each distribution system shall have sufficient capacity to supply the required loads under all operating conditions and to withstand the maximum credible overcurrent, during fault or transient conditions, without damage or adverse effect on any of its components.

- The characteristics of the DC and AC supplies required by individual loads shall have a margin on the values specified for the output of the power supply system to allow for deterioration in service and for the impedance arising out of connections between the load and supply.

- Standard distribution voltages shall be chosen to enable a wide range of equipment to be used. The number of voltage levels should be minimised to reduce system complexity.

- The following systems shall be provided with Uninterrupted Power Systems (UPS) :

  - systems important to safety and requiring continuous AC power for availability during operational states or accident conditions

  - systems, for which the interruption of power supply may cause actuation of the protection system.

- Systems having redundancy shall be provided with redundant power supplies meeting the independence requirements as stated in section 3.1. Where a safety critical and a safety-related I&C channel are supplied by the same power source, the reliability requirements shall be consistent with that of the safety critical system.

3.6.2 Pneumatic Power Supplies

Certain I&C systems may require non-electric power supplies, such as instrument air. These power supplies shall meet the availability requirements of the I&C systems they serve. Functional isolation and physical separation of these power supplies shall be applied as necessary to meet the independence requirements of section 3.1.

3.7 Field Instrumentation

3.7.1 The mechanical design of the I&C items which form direct part of pressure boundary shall be as given below:

- The design code/safety classification for in-line I&C items like venturies, thermowells, etc., shall be identical to the process system, wherever installed.

- The design code/safety classification of instrument impulse lines shall be identical to the corresponding process system. However, for impulse lines less than 25 mm. connected to class I system, class II system (NC) piping is permitted (refer AERB/SG/D-1). The design of tubing/piping systems for sensing lines should take into account all the forces and moments resulting from thermal expansion and contraction and the effects of expansion joints, if any.

- For the installation of instruments on the process equipment or in the process lines (i.e., venturi tubes, thermowells), effect of flow-induced vibrations for mechanical integrity as well as performance requirements shall be considered.

- In case of pressure retaining parts of sensors (e.g., bourden tube of pressure gauge, chambers of pressure transmitters and switches) mounted in the field, standard manufacturer's design can be accepted, provided compliance to the design intent of ASME code is demonstrated by analysis or type test.

- Separation between redundant instrument sensing lines should be provided by free air space or barriers, or both, such that no single failure can cause the failure of more than one sensing line. This shall conform to 'Nuclear Safety Related Instrument Sensing Line Piping and Tubing Standards for use in Nuclear Power Plants', ISA-S-67.02 or equivalent. In the absence of any barrier, separation distance should be at least 450 mm. As an alternative, a suitable steel or concrete barrier can be used.

- The redundant instruments shall be mounted on independent structures in the field having adequate physical separation.

- The pressure/differential pressure transmitters frequently used for different safety-related systems should have minimum moving parts and the fluid-retaining chambers should be so designed that structural integrity of the chambers is maintained.

- In differential pressure electronic transmitters, high pressure and low pressure chambers shall be isolated properly to ensure that inter-compartmental leakage does not occur during the operating life. Also, the design should be such that drift due to static pressure effect is minimum and repeatability of this effect should be periodically monitored. Provision shall be built in the sensor body for draining/venting to enable easy calibration checks.

3.7.2 It is recognised that intelligent/smart transmitters have unique programming advantages. However, such transmitters shall be used only after establishing their software reliability in addition to the above requirements.

4. CONTROL ROOM

4.1 Main Control Room

The design of a control room shall provide the operator with accurate, complete and timely status of the plant and the means for operating the plant safely under all DBEs.

4.1.1 Layout

4.1.1.1 The control room is the centre where redundant safety and safety-related channels of instrumentation from the plant converge. To maintain independence of these channels, separate control equipment rooms should be provided close to the control room to house the associated redundant channel instrumentation, meeting all the requirements of redundancy. Since the safety critical systems, safety related systems and systems not important to safety are all brought close together in the control room, the layout shall take into account the requirements for functional isolation and physical separation as stated in section 3.1 besides the ergonomic principles.

4.1.1.2 The location and layout of control room shall ensure adequate protection of occupants and equipment from hazards such as missile effects from turbine, crane movements in the vicinity, ventilation intake from contaminated plant exhausts, etc., which could jeopardise necessary operator action. A separate survival ventilation system for control room shall be provided to ensure its habitability in case of any failure or contamination of the normal ventilation system. Adequate and appropriate level of illumination in control room and on panel fronts is a prerequisite. The control room shall have direct access, independent of other plant areas, and have arrangements to guard against unauthorised entry to or unwarranted occupancy of the control room. In case of multiple units, control room for each unit should be independent in all respects as per section 3.1, including survival ventilation system and fire barrier requirements between the control rooms. Arrangement of panels, displays and controls should be similar in all the control rooms to facilitate operator familiarity. Mirror image concept shall not be considered.

4.1.2 Display

4.1.2.1 The display facilities shall cover appropriate parameters, consistent with the assumptions for safety analysis and with the information needs of the operator during DBEs.

4.1.2.2 Safety-related displays shall be located in the vicinity of the controls to effect the operator actions, such as control rod raise/lower switches and position indicators.

4.1.2.3 Displays shall be provided to indicate the status of all safety critical systems during normal and accident conditions. Parameters relevant to safety under abnormal or accident conditions should be grouped together for prominent display.

4.1.2.4 Where redundant displays are used, they shall be functionally isolated and physically separated to ensure that a single failure in this device would not result in a complete loss of information about a monitored variable, e.g., the use of multiple keyboards/CRT displays.

4.1.2.5 Displays shall be provided for indicating deliberately bypassed or inoperable conditions of safety channels or groups.

4.1.2.6 A single display channel with a clearly identifiable failure mode is adequate where the mean time to repair or replace it is less than the tolerable out-of-service time.

4.1.2.7 Where the trend of a parameter is essential to determine the required operator action, means shall be provided to display the trend.

4.1.3 Controls

4.1.3.1 Wherever any parameter can be controlled by an I&C system located in the control room and also from locations outside the control room, the currently acting control location shall be automatically indicated by visual means (e.g., annunciators, indicator lights) in the control room and at the outside locations of the safety-related equipment controls. Such transfer of control from control room to local areas or vice-versa shall be with permission from the control room operator and the transfer switch for the same should be located in the control room.

4.1.3.2 The control room should include all the controls necessary to deal with those accident conditions where

- performing of necessary controls outside the control room may be limited by the accident conditions; and
- time constraints for dealing with the accident conditions may prevent the operator from leaving the control room to operate controls in other locations

4.1.4 Alarms

4.1.4.1 Audio-visual alarm shall be provided in control room to attract immediate attention of operator. The annunciations and logging of alarms in the control room shall provide information on the key parameters required by the operator to identify any abnormal condition and to follow their trends. The selection of these key plant parameters and their display should take the following into consideration:

- identifying the particular abnormality.
- indicating that the required safety actions are being taken.
- monitoring the course of abnormality and effectiveness of safety actions.

4.1.4.2 The annunciations can be provided by hard-wired windows (window annunciators) or by CRT displays, etc.

4.1.4.3 Considering control panel space and operator fatigue, the number of window annunciations should be limited. Detachable engraved alarm plates, wherever used, should be so designed that unintended interchange is avoided, such as by labelling. All window annunciators should be latched and reset with only operator action.

4.1.4.4 Large number of annunciations may be covered on the CRT displays. In the event of a near simultaneous occurrence of alarms, the CRT displays or printouts facilitate logging the sequence of their occurrence and prove an aid to analyse the event.

4.1.4.5 The key parameters, which are important to plant safety, should be annunciated in the window boxes to facilitate an uninterrupted display. The parameters which are not directly related to the plant safety but are important from the point of view of certain equipment safety may be covered by CRT display only, so as to optimise the total number of window boxes in the control room.

4.1.4.5 Means shall be provided to permit the operator to acknowledge the alarms for abnormal states and clear the alarm when they return to normal state. Alarms may be muted before they are acknowledged.

4.1.4.6 The computerised alarm analysis method, if used, shall be qualified and should not result in suppression of information necessary for the operator to understand the location and potential consequences of the malfunctions.

4.2 Accident Monitoring

4.2.1 Information display for monitoring postulated DBEs in the plant shall be provided in the main control room and as necessary at the back-up control room/points, to verify

- that the reactor is shut down and remains shut down;
- that the decay heat is being removed;
- that any designated barrier in the containment isolation system (e.g., isolation dampers) for the release of radioactivity to the public is in place and continues to remain in place;
- whether conditions within the plant warrant emergency measures to be taken by authorities outside the boundary of the plant.

4.2.2 Means shall be provided for monitoring any off-normal radiological parameters inside the containment and also the iodine and tritium activities.

4.2.3 Accident monitoring equipment, including cables and accessories, shall be capable of operating in the environment present at the time of need and for the period of time needed. The ranges of measurement of selected key parameters shall extend to values which may be reached during events that challenge barriers to the release of materials from the fuel, primary system or containment or result in release of materials from one or more of these barriers.

4.2.4 The accident monitoring facility shall be designed to enable it to perform its role despite the failure of any single information display channel.

4.2.5 Where the accident monitoring facility utilises instrumentation for other purposes, e.g., for the protection system or for normal operation, the instrument

ranges and the equipment's environmental qualification shall be reviewed to confirm that the requirements established for these other purposes are also adequate for accident monitoring purposes.

4.2.6 Accident monitoring displays shall be specifically identified on control panels.

4.2.7 The accident monitoring system shall have provisions for printing out or otherwise recording the information relevant to accident analysis, so that it can be effectively used for accident control and emergency measures during and following accident conditions and may be retrieved for later use in the analysis of an accident.

4.2.8 Means shall be incorporated to provide adequate data to the emergency facilities without undue interference in control room activities during an emergency situation.

4.2.9 Station black out (SBO) is a unique situation, for which, means shall be provided for achieving the above objectives by manual operations, and if necessary, controlled by properly laid procedures. Adequate operator aids to indicate plant status and to monitor the plant safety- related parameters like plant power, PHT temperature, steam generator level, moderator level shall be provided under these conditions. Independent sensors and support I&C equipment for this purpose, as may be necessary, should be provided with dedicated battery backup to last the stipulated SBO.

4.3 Human Machine Interface

4.3.1 In design of control room, conditions for optimal human performance should be considered with due regard to general human characteristics and those specific to the operator population. The anthropometric and ergonomic considerations of the latter may be specific to a nation and may have to be evolved.

4.3.2 The following design goals shall be met taking human factors into consideration:

- Displays and controls should be arranged to optimise the operator's understanding of the plant status and minimise the movements required for him to control the plant.

- When parameters require redundant or diverse displays as a means for counter-checking the information, alternative sources of information should be located so that the operator can, with minimum movement, use all sources available in arriving at a conclusion.

- A simple convention should be established to provide consistency in the operation of controls that perform similar functions. For example, all pump switches could be arranged with rotary switches, which turn the pump 'on' when the switch is rotated clockwise. There should be a uniform convention in the use of colours, position indicators in the control room, push-button positions on instruments, and use of audio alarms. Where similar instruments or controls with related but different purposes are placed close together, means should be provided for the operator to readily distinguish one from the other, e.g., handles of different shapes, sizes or colours, distinctive labels, etc.

- Functional grouping of panel elements and appropriate mimic diagrams should be considered in laying out the panel.

- Audible or visual differentiation should be used to enable the operator to distinguish between various general classes of alarms.

- In the control room, the office of shift charge engineer/assistant shift charge engineer should be so located as to provide a clear vision of all the control room panels. A provision of operator information system computer terminal in the office to facilitate ON DEMAND display regarding the status of plant key parameters, is a desirable feature.

- Identified special tool-kits needed for specific operations should be kept in readiness, both in the main control room as well as in the back-up control room.

4.4 Back-up Control Room/Points

4.4.1 A back-up control room (BCR) shall be provided to accomplish the following safety functions, in the event of inability to carry out these functions from the main control room:

- safe shut down of the reactor

- removal of decay heat

- containment of radioactivity
- monitoring of plant parameters, including radiological parameters, to ensure that the above functions are being carried out

4.4.2 Such situations may arise because of

- equipment damage in the main control room, or
- inhabitability of the main control room.

4.4.3.1 It is preferable that all the required instrumentation and control equipment for the above be located in the BCR, which is physically and electrically separated from the main control room. Some of the identified control and monitoring facilities may also be distributed to identified areas of the plants like switch-gear area, motor control centre area, emergency DG room, etc., and called back-up control points (BCPs), from where safety tasks may be performed, based on the information available at the BCR.

4.4.4 The cause for non-availability of MCR shall not be a common cause for non-availability of BCR/BCPs.

4.4.5 The above monitoring and control functions from the BCR shall meet the requirements of single failure criteria.

4.4.6 It is not required to be able to perform from BCR all the control and monitoring functions, primarily carried out from the main control room during DBEs. As a minimum, the following facilities shall be available at BCR/BCPs:

- controls for :
  - diverse shut down systems;
  - steam discharge valves to atmosphere;
  - fuelling machine supply pumps and associated valves from BCP;
  - auxiliary boiler feed pumps and associated valves from BCP;
  - emergency diesel generator from BCP;
  - shutdown cooling pumps and associated valves from BCP.

- indications for :
  - neutron power;
  - PHT pressure and temperature;
  - PHT storage tank level;
  - moderator level and temperature;
  - steam generator level and pressure;
  - containment pressure and temperature;
  - containment radiation level;
  - containment isolation damper positions;
  - atmospheric steam discharge valves (ASDVs) state;
  - secondary shutdown system (SSS)/SDS-2 bank-in;
  - liquid poison injection system (LPIS) actuation;
  - channel trip status of both shutdown systems;
  - fuelling machine pump and associated valves state;
  - auxiliary boiler feed water pump and associated valves state.

4.4.7 Dedicated sensors and power supplies should be provided for monitoring the parameters necessary for ensuring the above in order to achieve functional independence from the main control room. Alternately, adequate isolation devices shall be used and the cable routing to the BCR/BCPs and location of the isolation devices should conform to requirements for independence from main control room.

4.4.8 Adequate physical separation between the main control room and BCR/BCPs shall be provided so that no common cause DBE renders both the controls ineffective at the same time.

4.4.9 The BCR/BCPs must be conveniently located so that the operators abandoning the main control room are able to move safely and easily to the BCR/BCPs. Two diverse access routes should be provided to the BCR, one of them for easy approach directly from the main control room.

4.4.10 The design shall allow adequate time for the operator to reach the BCR/BCPs and assess plant conditions for initiating necessary control actions.

4.4.11 The ventilation system for BCR/BCPs shall be independent of that for the main control room to avoid loss of habitability in both areas due to a common cause ventilation system failure.

4.4.12 A battery-powered emergency lighting system shall be continuously available to provide sufficient illumination for access and performance of the tasks by the operator, for a specified period.

4.4.13 Manual controls at BCR/BCPs should be accomplished by simple actions, e.g., operating a switch, pressing a button, etc.

4.4.14 Adequate displays shall be provided by means of indicating meters and annunciating lamps to cover the effectiveness of the functions performed from this area.

4.4.15 Arrangement of displays and controls on panels should be generally similar to that in the main control room to facilitate operator familiarity in an emergency.

4.4.16 In case a computer-based operator information system exists and the associated computer and functional hardwares are not located in the main control room, a CRT of this system may be provided in this area and adequately buffered from similar facilities in the main control room.

4.4.17 The design of BCR shall prevent unauthorised access and use.

4.4.18 The master control for putting into service of the BCR should be located in the main control room.

4.4.19 Whenever the control is transferred to BCR, it should be displayed both in the main control room and BCR.

4.4.20 For multiple units, separate BCRs shall be provided.

5. LOCAL ALARM AND VOICE COMMUNICATION SYSTEMS

5.1 Appropriate visual and/or audible alarms shall be provided at identified locations throughout the plant to warn site personnel about off-normal conditions, such as high radiation in local areas, shielding doors/valves status, etc., and to enable them to take proper actions.

5.2 Voice communications between the main control room, BCR/BCPs, other identified plant locations and off-site emergency services are vital to safety, particularly under anticipated operational occurrences or accident conditions. Communications between such locations shall be provided with two, preferably diverse, communication links (e.g., self-powered telephones, battery-operated telephones, hand-held portable radios). These communication links shall be routed in such a way that fires, electrical system failures and other applicable postulated initiating events (PIEs) cannot incapacitate both the systems simultaneously. It should also be ensured that such systems do not interfere with the functioning of other systems and equipment.

6. DOCUMENTATION

6.1 The design of the I&C systems shall be documented. In addition to the design features, design requirements of each system must be clearly specified. These should include functional requirements, performance requirements, requirements for interfaces with other plant systems, operator-interface requirements, fault tolerance requirements, behaviour under single failure/partial system operation (such as during testing and repair of a redundant equipment/channel), self-diagnostic features, requirements for equipment testing and maintenance, etc. The documentation shall also include the following:

- The design basis of each system, including its safety-related duties and the PIEs and plant conditions to which those safety-related duties apply.
- A list of applicable codes, standards or guides to be complied with when designing each system.
- A description of the range, accuracy and response time expected of each channel.
- The functions provided by each I&C channel including indicators, alarms and control characteristics.
- A description of the environmental conditions in which each component is required to operate, including normal conditions, anticipated operational occurrences and accident conditions.
- A specification of the power supply from which each system operates.
- Verification of the qualification of identified components for reliability.

6.2 These design documents should be suitably updated during all phases of plant life cycle, as in the case of design, fabrication, commissioning and operation.

ANNEXURE-I

PROGRAMMABLE DIGITAL SYSTEMS

I.1 Introduction

I.1.1 Programmable digital systems (or computer-based systems) are employed to perform control and operator information functions in a number of safety-related applications in the plant. The programmable nature of these systems, coupled with discrete logic implementation, raises additional issues, which are required to be considered during their design, implementation and use as well as for their assessment and licensing. The digital hardware implementation and software programmability of these systems can make them very sensitive even to minor programming errors or hardware faults. These systems require more rigorous analysis and testing because the concepts of continuity and interpolation are not applicable in the same way as for analogue hardwired systems. Because of the above reasons, for ensuring safety and reliability of these systems, a methodology that is different from that prevalent for hardwired electronic systems is required.

I.1.2 The faults, usually termed as 'software errors' in these systems, are the result of errors in communication of system requirements, by system designer and errors in the software architecture design implementation. Processes like wear out, degradation and environmental effects do not apply to software. Hence, reliability of programmable digital systems can only be demonstrated through a systematic, fully documented and reviewable engineering process during their design, integration and commissioning. There is, thus, an added emphasis on complete and total documentation for all software-based I&C systems to establish conformance to system requirements, as well as to enable verification and validation.

I.1.3 The documentation may fall under two categories, viz. system requirements and implementation methodologies.

I.1.4 The programmable digital systems implemented in the plant are parts of overall I&C of plant processes. The requirements of these systems are determined based on the overall requirements of the plant processes and their interfaces with other plant equipment, as well as for operation and maintenance. This

section concentrates on the process of determining requirements, which are used for their design and for validation of their implementation. The guidance for implementation methodology of computer-based systems are covered in safety guide AERB-SG-D-25 on 'Computer-based Safety Systems'.

I.2 Requirement Specifications of Programmable Digital Systems

I.2.1 An accurate and clear description of system requirements must be prepared as system requirements document (SRD) before design of the system. This description must be comprehensive and easy to use, in order to enable verification of the adequacy of the computer system, define the specifications of the tests and the software specifications for the required tasks, which validate the system when the design is complete. The elucidation of these requirements is an important early step of the design because errors and deficiencies at this level will have an impact on all later stages of the design and may prove too costly to correct.

I.2.2 The requirements enumerated in the SRD cover general system functions, system context and operating modes and deal with the computer-based system as a black box. These include functional requirements, performance requirements and interface requirements with other systems in the plant as well as human-computer interface. The requirements also cover safety, reliability and security aspects and provide fault tolerance, diagnostics and self-supervision, as also maintainability and environmental conditions. The SRD establishes the QA plan and provides requirements for verification and validation of the system as well as the acceptance criteria for the same. The system safety requirements are worked out depending on the results of plant safety analyses, which are based on postulated initiating events and safety criteria to be met. Detailed guidance for preparation of SRD is provided in safety guide AERB-SG-D-25.

I.2.3 Software should be well developed and documented through a controlled engineering process.

I.3 Types of Programmable Digital Systems

I.3.1 There are various types of implementations for programmable digital systems. Such systems can be employed in different categories of applications to perform functions such as data acquisition, information display and storage and closed

loop control. The design, implementation, assessment and licensing of these systems have to be commensurate with the special requirements of each category of application and type of the system selected.

I.3.2 The various types of systems can be broadly classified based on their implementation, as follows:

- Embedded systems
- Microprocessor-based custom-built systems
- Programmable logic controllers
- PC-based systems
- Distributed/networked systems.

I.3.3 One or a combination of the above types of systems may be chosen to meet a system function, with due consideration to the safety and reliability requirements. The generic requirements of I&C systems as outlined in section 3 of this guide are equally applicable for these systems also.

I.4 Embedded Systems

The embedded systems are generally microcontroller-based function modules, which have limited flexibility to select functional configuration and parameters. These are basically processing modules with embedded software, which have communication interfaces and/or analogue-to-digital and digital-to-analogue interfaces to connect to other modules. These modules are easier to test because of their limited functionality, if sufficient inner details are available. However, their self-diagnosis and fault tolerance capabilities are very limited, unless they are part of a distributed system.

I.5 Microprocessor-based Custom-built Systems

These systems are generally configured by using boards from a family of real-time industrial microcomputer boards. The hardware and software of these systems can be designed to be simple and specific to the requirements of the application, thus minimising chances of errors. It also enables availability of full functional and implementation details for review and analysis. Even though the individual cards used in these systems may be employed in several

applications, the specific architecture and software is custom-built and, hence, requires rigorous analysis and testing. In these types of systems, prototype testing using a dynamic simulator may become necessary.

I.6 Programmable Logic Controllers

The programmable logic controllers are general purpose, programmable process control and information systems which are available off-the-shelf (OTS). The hardware and software of these systems are modular and configurable for various types of applications. These modules may be proven by their sufficient usage in the process industry. However, since these modules have to cater to a variety of real-time applications, they often have extra functionalities, which are not required in the specific application, thus increasing complexity. In addition, for these modules, only overall functional and interface requirements are available and full implementation details are not available, thus restricting scope of review and analysis.

I.7 Distributed/Networked Systems

Plant-wide networked system configurations are being employed in most of the modern plants involving control and operator information. These systems can be built by using two types of architectures. In the first type, individual systems connected in the network perform specific plant system function including monitoring, control and/or operator information tasks. In the second type, individual modules in the network perform different system function such as acquisition, control or operator information and hence, a specific system function is achieved by interaction of these modules. The independence requirements as well as the types of failure modes and their consequences have to be thoroughly analysed for the type of architecture selected.

I.8 Design and Implementation Requirements

The design and implementation of programmable digital systems utilise SRD as the input and follow a systematic and well-documented multi-stage process. The stages in this process broadly cover architectural design, verification and validation planning, hardware design, software design, software coding, module level and integrated software testing, system integration, overall system commissioning and validation testing. Stage-by-stage verification and formal

validation based on system requirements, configuration management (i.e. version control) during all the stages of development as well as during use are some of the essential features of implementation. Since these aspects of programmable digital systems require a different and elaborate treatment, these are covered in the safety guide AERB/SG/D-25.

BIBLIOGRAPHY

1. ATOMIC ENERGY REGULATORY BOARD, code of practice on 'Design for Safety in Pressurised Heavy Water Reactors Basd Nuclear Power Plants', AERB/SC/D, Mumbai, India (1989).

2. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Safety Classification and Seismic Categorisation for structures, systems and components of Pressurised Heavy Water Reactors', AERB/SG/D-1, Mumbai, India (2003).

3. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Safety Critical Systems', AERB/SG/D-10, Mumbai, India (under preparation).

4. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Computer based Safety Systems', AERB/SG/D-25, Mumbai, India (under preparation).

5. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Fire Protection in Pressurised Heavy Water Based Nuclear Power Plants', AERB/SG/D-4, Mumbai, India (1999).

6. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Radiation Protection in Design', AERB/SG/D-12, Mumbai, India (under preparation).

7. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Primary Heat Transport System for Pressurised Heavy Water Reactors', AERB/SG/D-8, Mumbai, India (2003).

8. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Core Reactivity Control in Pressurised Heavy Water Reactors', AERB/SG/D-7, Mumbai, India (1998).

9. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Fuel Handling and Storage Systems for Pressurised Heavy Water Reactors', AERB/SG/D-24, Mumbai, India (2002).

10. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Protection against Internally Generated Missiles and Associated Environmental Conditions', AERB/SG/D-3, Mumbai, India (under preparation).

11. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Emergency Electric Power Supply Systems for Pressurised Heavy Water Reactors', AERB/SG/D-11, Mumbai, India (2001).

12. ATOMIC ENERGY REGULATORY BOARD, safety guide on 'Seismic Qualification', AERB/SG/D-23, Mumbai, India (under preparation).

LIST OF PARTICIPANTS

WORKING GROUP

Dates of meeting:	August 25, 1995	January 3, 1997
	November 15, 1995	January 17, 1997
	December 1, 1995	January 29, 1997
	April 9, 1996	February 25, 1997
	June 18, 1996	May 20, 1997
	July 2, 1996	August 21, 1997
	October 29, 1996	January 20, 1998
	November 19 & 20, 1996	February 26, 1998
	February 6, 2000	September 12, 2000

Members of the working group:

Shri K. Natarajan (Chairman)	:	NPCIL (Former)
Shri S.A. Bharadwaj	:	NPCIL
Shri Umesh Chandra	:	NPCIL
Shri B.B. Biswas	:	BARC
Shri Ravi Prakash	:	NPCIL
Dr. S. Thangasamy	:	NPCIL
Shri Murali Krishna	:	IGCAR
Shri R.K. Kulkarni	:	NPCIL
Shri S.N. Rao	:	AERB
Shri K.C. Subramanya	:	AERB (Former)
Shri A. Ramakrishna (Member-Secretary)	:	AERB

ADVISORY COMMITTEE ON CODES, GUIDES AND ASSOCIATED MANUALS FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD)

Dates of meeting:

June 27, 1996
September 29 & 30, 1997
November 3, 1997
July 20, 1998
February 7&8, 2000
September 14, 2000

Members of ACCGD :

Shri S.B. Bhoje (Chairman)	:	IGCAR
Shri S. Damodaran	:	NPCIL (Former)
Prof. N. Kannan Iyer	:	IIT Bombay
Shri V.K. Mehra	:	BARC
Shri Umesh Chandra	:	BARC
Shri Deepak De	:	AERB
Shri S. Sankar	:	BARC
Shri C.N. Bapat	:	NPCIL
Shri S.A. Bhardwaj	:	NPCIL
Dr. S.K. Gupta	:	BARC
Shri K. K. Vaze	:	BARC
Shri S.A. Khan (Member-Secretary)	:	AERB

ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS)

Date of meeting: 2 August, 2002

Members of ACNS :

Shri Ch. Surendar (Chairman)	:	NPCIL(Former)
Shri S.K. Sharma	:	BARC
Dr. V. Venkat Raj	:	BARC
Shri R.K. Sinha	:	BARC
Shri S.S. Bajaj	:	NPCIL
Shri S.P. Singh	:	AERB (Former)
Shri Ramesh D. Marathe	:	L&T, Mumbai
Shri S.K. Agarwal	:	AERB
Shri K. Srivasista (Member-Secretary)	:	AERB

Date of meeting: 28 April, 2001

Members of ACNS :

Shri S.K. Mehta (Chairman)	:	BARC (Former)
Shri S.M.C. Pillai	:	Nagarjuna Power Corporation, Hyderabad
Prof. U.N. Gaitonde	:	IIT Bombay
Shri S.K. Goyal	:	BHEL, Hyderabad
Shri Ch. Surendar	:	NPCIL (Former)
Shri S.K. Sharma	:	BARC
Dr. V. Venkat Raj	:	BARC
Dr. U.C. Mishra	:	BARC (Former)
Shri S.P. Singh	:	AERB (Former)
Shri G.K. De	:	AERB (Former)
Shri K. Srivasista (Member-Secretary)	:	AERB

PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUAL ON DESIGN OF PRESSURISED HEAVY WATER REACTORS

Safety Series No.	Title
AERB/SC/D	Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants
AERB/NPP-PHWR/ SG/D-1	Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors
AERB/SG/D-2	Structural Design of Irradiated Components
AERB/SG/D-3	Protection Against Internally Generated Missiles and Associated Environmental Conditions
AERB/SG/D-4	Fire Protection in Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/D-5	Design Basis Events for Pressurised Heavy Water Reactors
AERB/NPP-PHWR/ SG/D-6	Fuel Design for Pressurised Heavy Water Reactors
AERB/SG/D-7	Core Reactivity Control in Pressurised Heavy Water Reactors
AERB/NPP-PHWR / SG/D-8	Primary Heat Transport System for Pressurised Heavy Water Reactors
AERB/SG/D-9	Process Design
AERB/SG/D-10	Safety Critical Systems
AERB/SG/D-11	Emergency Electric Power Supply Systems for Pressurised Heavy Water Reactors
AERB/SG/D-12	Radiation Protection in Design
AERB/SG/D-13	Liquid and Solid Radwaste Management in Pressurised Heavy Water Reactor Based Nuclear Power Plants

PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUAL ON DESIGN OF PRESSURISED HEAVY WATER REACTORS

Safety Series No.	Title
AERB/SC/D	Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants
AERB/NPP-PHWR/ SG/D-1	Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors
AERB/SG/D-2	Structural Design of Irradiated Components
AERB/SG/D-3	Protection Against Internally Generated Missiles and Associated Environmental Conditions
AERB/SG/D-4	Fire Protection in Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/D-5	Design Basis Events for Pressurised Heavy Water Reactors
AERB/NPP-PHWR/ SG/D-6	Fuel Design for Pressurised Heavy Water Reactors
AERB/SG/D-7	Core Reactivity Control in Pressurised Heavy Water Reactors
AERB/NPP-PHWR / SG/D-8	Primary Heat Transport System for Pressurised Heavy Water Reactors
AERB/SG/D-9	Process Design
AERB/SG/D-10	Safety Critical Systems
AERB/SG/D-11	Emergency Electric Power Supply Systems for Pressurised Heavy Water Reactors
AERB/SG/D-12	Radiation Protection in Design
AERB/SG/D-13	Liquid and Solid Radwaste Management in Pressurised Heavy Water Reactor Based Nuclear Power Plants