GUIDE NO. AERB/NPP-PHWR/SG/D-10

GUIDE NO. AERB/NPP-PHWR/SG/D-10

GOVERNMENT OF INDIA

AERB SAFETY GUIDE

SAFETY SYSTEMS FOR PRESSURISED HEAVY WATER REACTORS

ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY GUIDE NO. AERB/NPP-PHWR/SG/D-10

SAFETY SYSTEMS FOR PRESSURISED HEAVY WATER REACTORS

Atomic Energy Regulatory Board
Mumbai-400 094
India

October 2005

Price

Orders for this guide should be addressed to:

The 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 of ensuring 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. While some of these documents cover aspects such as siting, design, construction, operation, quality assurance and decommissioning of nuclear and radiation facilities, other documents cover regulation aspects of these 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 top-level requirements for ensuring adequate safety in plant design. This safety guide is one of a series of guides, which are issued or are under preparation, to describe and elaborate the specific parts of the code. It identifies the safety systems, including engineered safety features which are required for the safety of pressurised heavy water reactor based nuclear power plants in India, under anticipated operational occurrences and accidents. This guide also provides design principles and graded application of the requirements to the different safety systems.

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. Footnotes and list 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 and Nuclear Power Corporation of India Limited 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.

(S.K.Sharma)
Chairman, AERB

DEFINITIONS

Acceptable Limits

Limits acceptable to the rregulatory body for accident condition or potential exposure.

Accident

An unplanned event resulting in (or having the potential to result in) personal injury or damage to equipment which may or may not cause release of unacceptable quantities of radioactive material or toxic/hazardous chemicals.

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.

Channel (Coolant)

The primary heat transport (PHT) coolant tube and accessories through which the reactor coolant flows in a reactor.

Channel (Instrumentation)

An arrangement of interconnected components within a system that initiates output(s).

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.

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 (ESFs)

The system or features, specifically engineered, installed and commissioned in a nuclear power plant (NPP) to mitigate the consequences of accident condition and help to 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

The ability of equipment, channel or a system 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 (IIS)

The items, which comprise:

- those structures, systems, equipment and components whose malfunction or failure could lead to undue radiological consequences at plant site or off-site;
- those structures, systems and components which prevent anticipated operational occurrences from leading to accident conditions;
- those features which are provided to mitigate the consequences of malfunction or failure of structures, systems, equipment or components.

Normal Operation

Operation of a plant or equipment within specified operational limits and conditions. In case of a nuclear power plant, this includes start-up, power operation, shutting down, shutdown state, maintenance, testing and refueling.

Operational Limits and Conditions (OLCs)

Limits on plant parameters and a set of rules on the functional capability and the performance level of equipment and personnel, approved by regulatory body, for safe operation of the facility.

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 a combination of both.

Postulated Initiating Events (PIE)

Identified events that lead to anticipated operational occurrence or accident conditions, and their consequential failure effects.

Protection System

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

Reactor Trip

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

Redundancy

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

Reliability

The probability that a structure, 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

The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of site personnel, the public and the environment from undue radiation hazards.

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 the safety system, which encompasses all equipment, required to accomplish the required safety action when initiated by the protection system.

Safety Function

A specific purpose that must be accomplished for safety.

Safety Related Systems

Systems important to safety which are not included in safety systems, which are required for the normal functioning of the safety systems.

Safety Support Systems

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

Safety Limits

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

Safety System

System important to safety and 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 (Examples of such systems are shutdown systems, emergency core cooling system and containment isolation system).

Safety System Settings

The levels at which protective devices are automatically actuated in the event of anticipated operational occurrences or accident conditions, so as to prevent safety limits being exceeded.

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.

CONTENTS

1. INTRODUCTION

1.1 General

1.1.1 Nuclear Power Plant (NPP) systems are broadly classified into two categories, namely,

1. Systems important to safety.
2. Systems not important to safety.

1.1.2 The fundamental safety functions that are required to be performed for the safe operation of a NPP, as given in the "Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants", AERB/SC/D are as follows.

- Reactor shutdown.
- Heat removal from core.
- Confinement of radioactive material to limit their release to the environment.

These functions are to be accomplished under all states of plant operation viz., normal operation, anticipated operational occurrence (AOO) and accident conditions.

1.1.3 The safety functions also include mitigation of the consequences of the accident conditions to reduce the activity release to the environment.

1.2 Role of Safety Systems

1.2.1 The systems important to safety are classified on the basis of their requirement during a particular state of plant operation to meet the above safety functions. These are divided into two categories, namely,

- Safety related systems.
- Safety systems.

1.2.2 The systems that are provided to meet the above safety functions during normal plant operation and maintain the relevant plant parameters within set limits constitute safety related systems. The safety related systems cover a broad range of systems from those having important safety functions to those with a less direct effect on safety.

1.2.3 The systems, either acting alone or in combination, which are provided to assure above three safety functions under AOO or accident conditions in the plant constitute safety systems. Safety systems mainly comprise shutdown system (SDS), emergency core cooling system (ECCS) and containment isolation system (CIS).

The AOO or accident conditions may arise because a fault has occurred within a control system, or because an event has occurred that changes process variables too rapidly for control system to act adequately, or because of failure of an item important to safety. In such situations, prompt and decisive action is required to prevent the situation from developing into a hazard.

1.2.4 SDS is called upon to act on the onset of AOO to prevent the AOO from developing into an accident. SDS is also initiated under accident conditions along with the action of ECCS.

ECCS is actuated under the accident conditions of loss of primary coolant to the fuel, to ensure the heat removal function.

CIS is actuated in case of release of activity to the environment from the plant to ensure confinement of activity within the plant.

1.2.5 Each of the above safety systems consists of protection system, safety actuation system and safety support systems.

The protection system is that part of safety system, which senses AOO or accident conditions and issues commands to associated safety actuation systems to ensure that specified design limits are not exceeded. The system extends from sensors, which provide signals that a particular process variable exceeded its limits, upto providing inputs to the safety actuation systems.

The safety actuation system consists of actuation devices and equipment associated with them, which get initiated by commands from the protection system and completes the process of safety action with the help of safety support systems.

The safety support systems provide the service facilities required by the protection system and the safety actuation system to complete the safety task. These include pneumatic and electrical power supplies of the safety systems and contribute to the uninterrupted availability of both the protection and safety actuation systems and maintain their operability.

1.2.6 Following the accident conditions, specially engineered systems/features may have to be initiated as required to mitigate the consequences of the accident conditions and to restore normalcy in the plant. These systems/features are called engineered safety features (ESFs).

The main safety systems and the ESFs have, thus, a graded impact on safety during AOO and accident conditions, in the order presented above and will have a bearing on the applicability or otherwise of the requirements of safety systems presented in this guide.

A schematic presentation of the plant systems is given in Fig.1.

1.3 Scope

The purpose of this safety guide is to outline the requirements and the design principles of safety systems. This covers the following aspects:

- Performance requirements.
- Design principles and requirements.
- Reliability requirements.
- Systems and plant status monitoring.
- Back-up control room / Back-up control points.
- Operator action.
- Documentation.

The classification of systems important to safety in a PHWR is given in "Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-1.

2. DEFENCE IN DEPTH

2.1 Concept of Defence in Depth

The safety in design is primarily based on the concept of defence in depth.

2.1.1 Defence in depth concept is implemented in the reactor design by means of a series of physical barriers and levels of protection. Physical barriers to limit radioactivity release are the fuel matrix, fuel cladding, the boundary of primary heat transport system and the containment systems. Apart from this, an exclusion zone around the plant site and a boundary fence are provided. Levels of protection include a combination of conservative design, quality assurance and safety culture, control of normal and abnormal operation and detection of failures, safety systems, accident management and off-site emergency response.

2.1.2 During normal operation, safety related process systems maintain the relevant plant parameters within set limits. This offers the first layer of safety for the three functions referred to in section 1.

2.1.3 During plant operation or AOO, the critical plant parameters may approach the trip set points. In order to avoid frequent demands on the safety systems, plant control systems also include set back and step back provisions to automatically reduce the plant power under the above conditions. This offers the next layer of protection in the defense in depth concept as applied to systems design.

When any of the safety system settings are exceeded, one or more of the safety systems come into play to achieve the safety functions. It is likely that the action of a safety system may have to be supplemented by one or more of the specially engineered safety features to complete/assist the safety task.

This forms a further layer of safety. The safety functions and the associated safety related and safety systems are covered in Table-1.

2.1.4 Inherent in the defence in depth approach to nuclear safety is the consideration that the consequences of a design basis accident shall not exceed the acceptable limits for dose, even in the unlikely event of one of the safety systems fails to achieve its safety function. To avoid consideration of anticipated transient without scram (ATWS), the reactor shutdown function shall be met by two independent and diverse shutdown systems so that any common cause failure would not disable both the shutdown systems at the same time.

3. PERFORMANCE REQUIREMENTS

The performance requirements and minimum allowable performance standards for the safety systems are arrived at by safety analysis with due considerations to postulated initiating events (PIE). The list of PIE requiring the safety analysis and their consequences is covered in "Design Basis Events for Pressurised Heavy Water Reactors", AERB/SG/D-5. These analyses, together with acceptable limits set by the regulatory body, should establish in quantitative terms, the overall functional performance requirements of the safety systems. These requirements are then applied to the protection system, safety actuation system and safety support systems as appropriate.

On demand, the protection system, safety actuation system and safety support system shall collectively perform the necessary safety task

- with stipulated reliability,
- with the assumption of a single failure, and
- with minimal spurious actions.

The general and the system specific requirements of the three main safety systems are given in this section. The design principles are covered in section 4.

3.1 Reliability Targets

The necessary functional performance requirements and reliability goals of the safety systems are stated in the design basis of the plant. The safety systems should be designed to meet the following reliability targets.

Each shutdown system failure probability	$< 10^{-3}$
Emergency core cooling system failure probability	$< 10^{-3}$
CIS failure probability	$< 10^{-3}$

3.2 Single Failure

The single failure criterion is based on the general experience that even components and equipment that are made to high standards of quality may fail to function in a random and unpredictable manner. The single failure criterion ensures safety even in that situation.

3.2.1 Each of the safety systems shall meet its performance requirements, in case of a single random, credible failure of a component occurring anywhere within the safety systems, under the following conditions.

i) The worst permissible configuration of safety systems performing the necessary safety function is assumed, with account taken of maintenance, testing, inspection and allowable equipment outage times.

ii) The consequential failures resulting from the assumed failure shall be considered to be an integral part of the single failure.

iii) Any potentially harmful consequences of a PIE and requiring the safety action be present.

3.2.2 Failure of components/equipment occurring anywhere in a safety system, which may affect the reliability of the safety system, should be automatically indicated in the control room or should be revealed by an accepted periodic testing programme. Failures, which are not covered above, are non-detectable failures for the application of this criterion. All credible, identifiable but non-detectable failures shall be assumed to exist, one at a time.

As an example, application of the above requirement will mean

- 2 x 100% design or 3 x 50% design will meet the single failure criterion only if provision exists for detection of failure of each equipment.
- 3 x 100% design or 4 x 50% design with a non-detectable failure, will meet the criterion.

In a group of shutoff rods in shutdown system, one rod failure should be postulated while assessing the reactivity worth, in case of detectable failures and two rods failure should have to be postulated in case of non-detectable failures, for the system to meet this criterion.

3.2.3 Single failure criterion should be met with the remaining portions of safety systems, even if a redundant channel/equipment is taken for maintenance.

Failure postulations need not be applied to passive components which do not change state and which do not depend on availability of safety support systems in order to perform their intended function, such as piping, storage tank, heat exchanger etc. provided they are designed, manufactured, inspected and maintained to acceptable standards.

3.2.4 Exemptions to the single failure criterion may arise depending on the credibility of postulated failure.

Non compliance to this criterion may be justified for

- very rare PIEs
- very improbable/low consequences of PIEs
- withdrawal from service for limited periods for maintenance, repair, or testing, backed up by adequate procedures and operator awareness.

Safety is the prime consideration in the application of single failure criterion. However, to the extent practicable, plant availability should also be considered such that a single failure should not lead to a spurious plant trip.

3.3 Spurious Operation

3.3.1 The primary requirement of the safety systems shall be to adequately carry out its specified safety tasks. However, spurious operation of this system shall also be considered in the design since it can

- lead to possible equipment failure because of needless frequent stressing of equipment,
- lead to the need for any other safety action,
- lead to a lack of operator confidence in the equipment and the possible disregard of valid signals, and
- cause loss of plant production capability.

3.3.2 Spurious operation may result from two causes, namely, failures within the equipment or inadequate trip set point margins on some parameters in relation to variations occurring in normal operation. The first results from unreliability of the equipment and the second from

- consideration of plant responses to operational disturbances and the consequential variations in the parameters being monitored,
- inadequate allowance for instrument inaccuracy, calibration uncertainties and drift or operator error in setting trip set points, and
- inadequate allowance for signal to noise ratio.

3.3.3 It is therefore necessary to design the protection system to meet its performance requirements while attaining a balance with the frequency of spurious operation. Adequate redundancy and majority coincidence should be introduced in the design such that a spurious output from a redundant channel should preferably not initiate a safety action. Suitable redundancy within safety actuation systems and safety support systems may be provided to reduce spurious operation.

3.4 Shutdown Systems

Each of the shutdown systems shall consist of equipment and means of introducing adequate negative reactivity into the reactor to shut it down when called upon by associated protection system. As explained in section 2, there shall be two independent and diverse shutdown systems which shall be independent from each other, from each of the other safety systems and also from the normal or abnormal functioning, or unavailability of, any safety related process systems. (Ref. “Core Reactivity Control in Pressurised Heavy Water Reactors”, AERB/SG/D-7).

3.4.1 The devices and equipment for the two diverse systems, acting alone shall individually meet the following requsirements.

- Reactivity worth of the shutdown system: The reactor is rendered subcritical and is maintained subcritical, with adequate shutdown margin for the most reactive state of the core.
- Rate of negative reactivity addition: The speed of shutdown system to insert negative reactivity into the core shall take into account the maximum positive reactivity addition rate by any accident to ensure fuel pellet integrity as assessed by fuel enthalpy limit under power ramp condition and maintenance of pressure tube integrity.

3.4.2 The above requirements shall typically be met under the following postulated situations.

- Loss of coolant accident (LOCA) signifying high rate/magnitude of reactivity addition.
- Loss of regulation accident (LORA) signifying uncontrolled power increase as a result of loss of bulk power regulation or loss of spatial power regulation.

3.4.3 Adequate consideration must be given in meeting the above requirements to:

a) Choice of trip parameters

Events requiring prompt shutdown action shall be identified in safety analysis and process variables signifying these events shall be used to select trip parameters. For illustration, a list of typical trip parameters and trip coverage is given in Table-2.

Any conceivable situation, which could lead to accident in the absence of prompt reactor trip, should have two independent trip parameters to the extent possible, one backed up by the other.[1]

b) Trip set points

This should take into account sensing and signal processing accuracies, delays, dead time in the initiation of the actuating mechanisms and the speed of insertion of negative reactivity by the system.

---

[1] Exemption can be taken for those events where the first (primary) trip signal is PHT high pressure. In such cases, the backup trip signal is not required to be credited (Ref: IAEA Safety Report Series No.29)

3.4.4 It is acceptable to meet the reactivity requirements for either system by the combined action of a fast acting system, followed by a slow acting system. In such a case, each of the fast acting systems shall be on its own capable of quickly rendering the reactor subcritical by adequate margin from operating and accident conditions. Also, the redundant/coincident output of at least one of the protection systems shall automatically initiate both fast acting and slow acting actuation systems to maintain the reactor subcritical under all conditions. A typical example will be quick filling of liquid poison tubes followed by liquid poison injection to moderator.

3.4.5 Diversity

Diversity is generally classified into functional and equipment diversity.

3.4.5.1 In functional diversity, two different means are used to accomplish a particular task when two different variables are used to detect a particular anticipated operational occurrence or accident conditions. This is the primary method of reducing the possibility that the protection system will not detect a departure from acceptable plant conditions in the case when one variable does not behave as predicted by the safety analysis.

In equipment diversity, either similar equipment from different manufacturers or equipment employing different principles of operation are used in the system. If carefully applied, equipment diversity offers protection against design, manufacturing and construction deficiencies as well as reducing the potential of cascading influences from other systems. The application of such diversity should take into account any potential for increased operational and maintenance errors, or other considerations due to the use of such equipment.

3.4.5.2 Diversity shall be applied to the two shutdown systems. Suggested means in the protection system are use of a computerised digital comparator system in one shutdown system and a different, discrete signal comparator in the other shutdown system for generating the trip signals.

3.4.5.3 The actuation systems should be of diverse design and should be physically, functionally and conceptually independent of each other. Examples of this diversity are the gravity fall of shut-off rods and liquid poison injection by pressurised fluid either in closed tubes or directly into the moderator.

3.4.5.4 In any application care must be exercised to ensure that diversity is in reality achieved in the implemented design. The designer should remain alert to areas of potential commonalty in the application of diversity, to materials, components, manufacturing methods, or subtle similarities in operating principles or common support features.

3.5 Emergency Core Cooling Systems

3.5.1 This system consists of various subsystems and components for emergency

coolant injection, supply, recovery and circulation for decay heat removal from the core. The system provides means of cooling the reactor fuel in the event that the inventory of normal fuel coolant is depleted to an extent that required fuel cooling is not assured. The system actuates when called upon by the associated protection system. The detailed performance requirements for ECCS are covered in "Primary Heat Transport System for Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-8.

3.5.2. ECCS carries out the following functions.

i) High pressure injection and

ii) Low pressure injection of light water/long term coolant recirculation.

3.5.3 The initiating logic and sensors required for detecting and identifying the nature of LOCA shall be incorporated for the above phases individually. In order to avoid spurious injection of light water, the initiating logic may have a suitable combination of the appropriate parameters such as:

- PHT system pressure very low;
- Containment system pressure high and
- Moderator level high.

3.6 Containment Isolation System

3.6.1 CIS is an operative part of the containment system. The objective of the system is to box up the reactor building containment to keep the release of radioactivity to the environment within acceptable limits, following postulated accident conditions. This system consists of a physical barrier, called the containment envelope and dampers and actuators on supply and exhaust lines of the ventilation system of reactor building. It also includes isolation devices provided for those containment penetrations of ventilation systems and lines of vapour recovery system, safety systems and various process systems, which are necessary for maintaining containment integrity.

The performance requirements of the system are covered in "Containment System Design", AERB/NPP-PHWR/SG/D-21.

3.6.2 All containment airlocks (main airlock, emergency airlock and fuelling machine airlocks, etc.,), though form part of the containment system, are provided with separate in-built logics and features to ensure that containment integrity is not impaired.

3.6.3 The containment isolation system is automatically initiated by closing all dampers and valves in the containment penetrating ducts and pipes, based on

- high reactor building pressure, or
- high release of radioactivity to the environment.

The sensing delays and actuation times of isolation devices shall be such that the permissible dose limits are not exceeded following an accident.

4. DESIGN PRINCIPLES

The system design should be in accordance with the safety classification and seismic categorization as stated in "Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-1. The general design principles and functional requirements of the safety systems are covered in this section.

4.1 General

4.1.1 The safety system shall:

- be simple and based on proven design principles,
- be latched after initiation, i.e., should not terminate automatically once initiated, before the completion of the task,
- provide for independence of the system for safeguard against credible common cause failures,
- incorporate fail-safe design, wherever practicable,
- be constructed from components of suitable quality as demonstrated by adequate qualification,
- be capable of being tested comprehensively and maintained to ensure its continuing ability to meet its performance requirements in service,
- minimise the potential for error by operating and maintenance personnel,
- be defined with clearly identified equipment and structures, and
- provide security against unauthorised access.

4.2 Independence

4.2.1 The effectiveness of defence-in-depth design is enhanced by maintaining system independence.

Independence comprises of

- functional independence including communication independence and
- physical independence.

4.2.2 Functional Independence

Functional independence between the systems is achieved by not having electrical interaction between the systems. No credible failure in one system shall prevent the other system from meeting its requirements. Examples of

credible failures include short circuits, open circuits, earth faults and the application of excessive voltage.

In case of electrical interconnection between systems requiring independence, functional independence is maintained by using isolating devices (buffers) such as electrical isolators, optical isolators etc.

Where the signal is transmitted through an isolation device (buffer) from one system to another, this device shall be classified as part of the system, with a higher level of safety. Failure of an isolation device shall be evaluated in the same manner as failure of other equipment in that system.

4.2.3 Physical Independence

This is ensured by physical separation by distance, provision of barriers etc.

The choice of physical separation by distance, barriers, or their combination may differ from location to location within the nuclear power plant and will depend on the need to provide protection against all the PIE considered in the design basis e.g. the effects of fire, chemical explosion, internal missiles and nuclear security. Reference should also be made to the safety guides, "Protection Against Internally Generated Missiles and Associated Environment Conditions", AERB/ SG/D-3 and "Fire Protection in Pressurised Heavy Water Reactor Based Nuclear Power Plants", AERB/SG/D-4.

4.2.4 There shall be total independence between safety systems and non-safety systems, including physical and functional independence.

4.2.4.1 There shall be total independence amongst redundant channels of protection system.

Functional independence shall be maintained

i) Amongst the different safety systems.

ii) Between safety systems and safety related systems.

4.2.4.2 Redundant channels equipment, cables, structures of safety systems and safety related systems may have the same physical location, while ensuring that such grouping of safety systems and safety related systems equipment, cables, structures etc do not violate independence amongst the redundant channels of safety systems and safety related systems.

4.2.4.3 Independence should be maintained to the extent possible amongst the protection systems of various safety systems by having individual, redundant protection system for the different safety systems.

4.2.4.4 Computer based signal processing techniques may be applied to handle, in a single equipment, protection system signals of more than one safety system. Functional independence shall still be maintained by using buffers. In addition,

redundancy and independence of this equipment is maintained same as in the redundant protection system channels and total independence between the two shutdown systems are maintained.

4.2.4.5 As an option, the four safety systems could be divided into two groups, one group consisting of shutdown system#1 and containment system and another group consisting of shutdown system#2 and ECCS. The two groups shall have total independence from each other.

Actuation system for each safety system shall be dedicated to that safety system and independent of other safety systems and related process systems. For example, the shutdown devices shall be independent from the regulating system control devices, liquid poison injection system shall be independent of boron addition to moderator for control purposes etc;

If provision is made for one common backup equipment to several redundant portions of protection system, design should ensure that the backup equipment be connected to only one of the redundant channels at a time. e.g., power supply back up for three protection channels.

4.2.4.6 Safety support systems may be shared by more then one safety system. In such a case, independence requirement amongst the safety systems be ensured such that safety function of any safety system will still be met even with a single failure in the safety support system.

As part of the requirements of independence, it shall be ensured that normal or abnormal functioning of any other system does not reduce the effectiveness of safety systems.

4.3 Fail-safe Design

4.3.1 Equipment with predictable failure modes should be used to the extent possible. For example, the predicted failure mode for an energised relay or a clutch holding a shut-off rod is the de-energised state. The design is fail-safe, if an equipment failure in the more probable modes of failure initiates a safe action. This concept should be followed in safety systems design, wherever practicable.

4.3.2 The less probable and unsafe failure mode may be the circuit not opening due to sticking/fusing of relay contacts, adhesive corrosion, creep etc. or a rod not dropping. The design shall nevertheless meet the single failure criterion, with the postulation of failure of the component in the less probable but credible other modes of failure.

4.4 Qualification

4.4.1 Equipment/components used in the safety systems shall be qualified to give assurance about its capability to meet design basis performance requirements

throughout their lives under all applicable design basis events including

- Dynamic effects such as jet impingement, pipe whip and internally generated missiles,
- Design basis earthquake (Ref. "Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-1 and "Seismic Qualification of Structures, Systems and Components of Pressurised Heavy Water Reactors Based Nuclear Power Plants" AERB/SG/D-23) and
- Environmental conditions (e.g. temperature, pressure, chemical sprays, high radiation fields, humidity) existing at the time of need.

4.4.1.1 These environmental conditions shall include the expected variations for normal operation, anticipated operational occurrences and accident conditions such as during LOCA or periodic containment leak rate testing.

4.4.1.2 When protective barriers are provided to isolate equipment from possible environmental effects, the barriers themselves shall be subject to verification of their adequacy.

4.4.1.3 Special emphasis shall be placed on the qualification of equipment that cannot be easily replaced.

4.4.1.4 Where computerised equipment are used in the protection system, these shall be subjected to qualification provisions as per safety guide for 'Computer Based Safety Systems of Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/NPP-PHWR/SG/D-25).

4.4.1.5 Quality verification of new and replacement equipment should be for the period during which the equipment will be used in the plant. In the qualification of safety systems, equipment in an integrated manner should preferably be qualified.

4.4.2 Methods of Qualification

The following methods of qualification may be used in combination as necessary to meet the objectives stated above.

i) Performance of type tests on equipment representative of that to be supplied,

ii) Performance of tests on the actual equipment supplied,

iii) Application of past experience in similar applications, and

iv) Analysis based on reasonable engineering extrapolation of test data or of operating experience under pertinent conditions.

4.5 Testability

4.5.1 All initiating parameters and logics for the safety systems shall be testable.

4.5.1.1 The preferred test method involves a single on-line test encompassing all components from the sensor to the actuating device. However, such tests are not always practical. In such circumstances, the test programme may combine on-line (operational states during which the safety function may be required) and off-line (during operational states when the safety function is not required) tests in a series of overlapping test steps to the extent necessary. Adequacy of overlapping test steps shall be demonstrated.

4.5.1.2 The testing of sensors and associated electronics may be done by perturbing the monitored variable, such as testing of the neutron ionisation chamber by movement of a boral test shutter. Other methods of injecting a signal to simulate the ionisation chamber response or application of high pressure air supply to transmitters are acceptable, provided the sensors are not disconnected and sensors response is ensured by some other means, on a different periodic interval and ensure reversion to normal operation.

4.5.1.3 All actuating devices, such as

- shutoff rods,
- valves in the liquid poison tubes / poison injection system,
- valves in ECCS, and
- isolation dampers

shall be tested. The frequency of testing of the safety actuation system components should be optimised in keeping with the overall performance requirements and the field conditions.

4.5.1.4 Exceptions for routine testing may be made for instruments monitoring rare events. An example is seismic switch. A feasible test programme must be evolved and accepted for such parameters.

4.5.2 Test Provisions

The design of the test provisions for the safety systems shall ensure the safety of the plant during the actual testing and minimise spurious initiation of any safety action. Conduct of the test programme shall not cause deterioration of any plant component beyond that provided for in the design.

The test sequences shall be capable of detecting failures in each redundant portion of the system.

The periodic test provisions shall provide system status information and should furnish trend data to assist in the determination of system degradation.

4.5.3 Control and Conduct of Tests

Human error affecting safety or availability is likely to occur at the time of conduct of tests. With a view to minimise this,

- Periodic testing shall be administered to the maximum extent possible from the control room. Adequate built-in facilities shall be provided for quick conduct of test for equipment in the control centre, in the local equipment areas of the plant, at the backup control points, or a combination of these.
- Indications of the state of the components (open or closed position of valves, position of shutoff rods etc) should be provided in the control room.
- Test procedures for periodic tests shall not require or allow makeshift test set-ups, use of temporary jumper wires, removal of fuses or opening of breakers etc.
- Testing arrangements shall neither compromise the independence of redundant portions of the protection system, nor increase the potential for common cause failure.

4.5.4 Removal from Service

4.5.4.1 The design of the protection system shall ensure that, during conduct of the periodic test, those portions remaining in service are able to accomplish any safety task, if required. The chosen test method shall minimise the time interval during which equipment is removed from service.

4.5.4.2 The preferred mode of withdrawal of a channel from service is to place that channel in tripped state. When a sensor is removed from service for a periodic test, visual crosschecking with the redundant sensors (or other equivalent means) shall be done to verify its subsequent successful restoration to service. In addition, the status of items (e.g. instrument root valve position, maintenance bypasses) that were disturbed to accommodate the periodic test shall be verified to ensure their return to the original operating state. In such instances, an indication shall be provided in the control room for items expected to be frequently removed from service during the conduct of the periodic test. Administrative controls alone may be used for those items expected to be infrequently removed from service.

4.5.5 Maintenance, Repair and Calibration

4.5.5.1 Safety systems equipment, with special reference to safety actuation system components, shall be located to permit timely access, easy diagnosis, and easy repair or replacement of faulty devices preferably even during plant operation.

4.5.5.2 If a protection system channel is bypassed during plant operation for purposes of maintenance, test, repair or calibration, the same channel should be kept in tripped state so that the remaining operable channels of the system will continue to perform the required safety function with majority coincidence.

4.6 Manual Backup

Operator action is not envisaged to fulfill a safety task of main safety systems as these are initiated automatically to accomplish necessary safety tasks. However, manual backup initiation shall be provided for rapid shutdown of the reactor and may be provided for the initiation of safety actions within other safety systems. Where manual backup is provided, the number of safety systems components common to both automatic and manual initiation should be minimised to the extent feasible.

4.7 Identification and Tagging

Safety systems equipment and its interconnections shall be suitably identified e.g., by tagging or color-coding, to differentiate this system from other plant systems. In addition, within safety systems, redundant channels/devices shall be suitably identified to reduce the likelihood or inadvertent maintenance, test, repair or calibration on an incorrect channel. Such identification should not require reference to drawings, manuals or other reference material. Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of the safety system do not themselves require identification.

4.8 Control of Access to Safety Systems Equipment

Access to equipment of the safety systems shall be appropriately limited, bearing in mind the need to prevent both unauthorised access and the possibility of error by authorised personnel. The methods employed shall include appropriate combinations of physical security (e.g., locked enclosures, rooms), and administrative measures (e.g., authorised work permits) according to the degree of supervision or remoteness of the equipment.

5. PROTECTION SYSTEM REQUIREMENTS

Requirements common to the protection system, safety actuation system and the safety support systems are covered in section 4 of this guide. This section includes additional requirements pertinent to the protection systems not specifically included in section 4.

5.1 Extent of Protection System Channels

Both functional and physical independence shall be maintained amongst the redundant protection system channels. For this purpose, the extent of a channel may include

a) Sensors, which may be

- Primary sensing devices used for measurement of plant variables, e.g., resistance temperature detectors, neutron ionisation chambers etc.
- Instrument sensing lines from the process up to and including the input transducers,

b) Signal conditioning equipment for the primary sensing devices,

c) Comparator circuits with preset limits,

d) Buffer isolation devices interfacing with operator information systems and other systems,

e) Panels, racks and enclosures containing protection system equipment, and

f) Cable trays including containment penetrations.

5.2 Redundancy and Coincidence

To ensure that the safety system achieves its reliability goals and conform to the single failure criterion, the principle of redundancy shall be applied. Independence is required for redundancy to be fully effective.

Taken alone, redundancy increases the reliability of safety action, but it may also increase the probability of spurious operation. Majority coincidence of redundant equipment signals is therefore used to obtain a proper balance of reliability and freedom from spurious operation. Coincidence is a feature of protection system design such that two or more overlapping or simultaneous output signals from more than one channel are necessary to initiate a safety action. Redundancy and coincidence are only two of the methods used to achieve higher reliability.

5.3 Sensing of Variables Indicative of PIE

5.3.1 The measured plant variables, either singly or in selected combination, must permit detection of all situations in which a safety task is to be performed. Safety action is initiated when the value of a plant variable, associated with safety, reaches a predetermined value.

5.3.2 Measurements of plant variables shall be unambiguous and shall meet the performance requirement specified in the design basis. To the extent practical, the plant conditions of concern should be monitored by a direct measurement rather than being inferred from indirect measurements. Selection of the sensing variables or combination or variables shall take into account the possible failures.

5.3.3 The selection of sensors shall take into account the conditions of the measured medium and the surrounding environmental conditions (e.g., temperature, pressure, radiation, humidity, vibration, corrosion effects, crud effects) to which the sensor may be subjected, and which may unacceptably affect their accuracy and ability to provide a signal in any of the circumstances in which they may be needed during the planned life of the equipment. The number and location of sensors required to monitor a spatially dependent variable shall be determined and included in the system design.

5.3.4 For each monitored variable, the selection of the measurement range shall take into account the accuracy, speed of response, and amount of over-range needed for the particular function and any required post-accident monitoring capability. If more than one sensor is required to adequately cover the entire range of the monitored variable, a reasonable amount of overlap from one sensor to another shall be provided at each transition point to ensure that saturation or fold-over effects do not prevent accomplishment of the required safety task.

5.4 Set Points

5.4.1 Thresholds for safety actions, in case the control systems fail, are to be set such that the safety action occurs before any significant damage is done to the plant. The bases for the selection of a trip set point shall be documented and shall include the data, assumptions and the methods used. The data used may be taken from operating experiences, equipment qualification tests, vendor design specifications, engineering analysis, laboratory tests and approved engineering drawings. Any assumptions used, such as ambient temperatures during equipment calibration and operation should 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 initiated and the safety limits are normally not exceeded. This takes into account the sensor/set point inaccuracies and the dynamic responses of process systems and actuation equipment.

5.4.2 The set point and measurement inaccuracies include:

a) Instrument calibration uncertainties caused by

- Calibration standard.
- Calibration equipment.
- Calibration method.

b) Instrument uncertainties during normal operations and also during specified design basis event

- Reference accuracy, including conformity to input-output relations, hysteresis, 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 setpoint 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 measurements, and process oscillations or noise or frequency change.

e) Calculation Uncertainties

The determination of the trip setpoint 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 setpoint allowance shall allow for response delays in the instrument channels. The instrument channel response time shall not be more than the limiting response time required by the safety analysis.

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

5.4.4 Safety system settings are chosen to have adequate margin below the safety limits.

5.4.5 Channel protective action set points are fixed depending upon plant parameter or conditions. The design of the system shall provide the operator with a means for ascertaining the set point values for each protection system channel.

5.4.6 The testing of a system or a chain of equipment, with set points, must provide for testing the set point. Changing of set points for the purpose of demonstrating initiation of safety action should normally not be done. Adequate technical/administration procedures must exist for restoration of the set points to the original values after testing, in case this is done.

5.4.7 Suitable locking arrangement for set points shall be provided wherever warranted to safeguard against unauthorised tampering of the set points. For computer based systems, software locks, such as password, are normally provided. A manual locking device may be preferred wherever possible.

5.5 Latching and Repoising

5.5.1 Latching

The process of the output signal of a component taking a new state and remaining in that state after the initiating signal or signals that initiated the new state have returned to their previous values. The action initiated by the protection system either automatically or manually shall be latched after a time interval established by the need to reject spurious signals and the need for timely safety system actuation.

Once the latching of a protection system takes place, the intended sequence of actions for that safety system will continue until the safety task of that safety system has been accomplished.

The latching shall be released by manual operator action for resetting subsequent to completion of the safety action. Such resetting of protection system shall be possible only when all the causative signals, which initiated the systems, are cleared. Following a latched action, the protection system shall continue to monitor the plant conditions automatically, providing information to the operator to support subsequent manual action, where permitted.

5.5.2 Repoising

While repoising the actuation system, system design should ensure that initiated safety action is not impaired and shall be available for safety action again.

5.6 Conditional Bypass

5.6.1 The provision, which protects the reactor in one mode of normal operation, may cause unwanted actuation of systems, when reactor is taken to other operational states. To achieve such changes, when required, it is necessary to inhibit the initiation of an unnecessary and unwanted safety action, by using a conditional or operational bypass. Bypass is an approved action or device which renders inoperable one or more portions of systems important to safety for the purpose of maintenance, test or repair.

5.6.2 An operational bypass may be used for example-

- to permit start-up by inhibiting a particular protective action that would otherwise occur. Whenever permissible conditions are not met, activation of an operational bypass, should be automatically inhibited,
- to inhibit certain trip parameters below a certain power level (referred as conditional trip parameters). The setting or removal of the bypass action shall be automatically done whenever permissible conditions for the safety of the plant are met. The equipment used for sensing such conditions shall also form part of safety systems for compliance with safety systems requirements, and
- ECCS blocking below a certain PHT temperature.

6. ACTUATION SYSTEM REQUIREMENTS

Requirements common to the protection system, safety actuation system and safety support systems are covered in section 4 of this guide. This section includes additional requirements pertinent to the actuation systems not specifically included in section 4.

6.1 Shutdown Actuation Systems

6.1.1 The actuation system should be designed to add fast negative reactivity into the reactor to meet the performance requirements given in section 3.4 of this guide.

6.1.2 The actuation system device should function on the concept of stored energy. For example, shutoff rods poised against gravity and gas pressure energy for liquid poison systems.

6.1.3 The actuation system design should aim at minimising the number of active components, required to operate during actuation.

6.1.4 The design of actuation device should incorporate features to ensure quick movement of rod/injection of liquid poison against resistance due to inertia or sticking.

6.1.5 Any retarding action (incorporated for safety of components) during the actuation of the device shall be effective only after the negative reactivity worth requirement is met.

6.1.6 Any failure of services such as power shall lead to actuation of shutoff devices to ensure safe shutdown of reactor.

6.1.7 The location of shut down devices should be based on the following considerations:

a) Maximisation of reactivity worth,

b) The minimum distance between two shutdown devices is such that the reactivity shadowing effect is minimised, and

c) Sufficient clear space around each device is available as per structural and mechanical considerations for handling and maintenance of drive mechanisms.

6.1.8 The shut-off rods may be grouped into number of banks, provided each bank has almost equal reactivity worth. The positive reactivity addition shall be such that reactor does not go critical when the shutdown devices are withdrawn after a reactor trip.

6.1.9 The minimum reactivity worth requirement of SDS shall be achieved even with the failure of a device (or a bank if used) with maximum reactivity worth.

6.1.10 Any actuation device performing the shutdown function should normally not be used for reactor regulation. The design of the device may however be similar/identical to regulating device.

6.1.11 The design shall be such that normal functioning of the process systems shall not affect the minimum performance requirements of the shutdown system as in section 3.

6.1.12 To the extent possible, the design should be such that all maintenance and availability testing can be carried out during reactor operation without reduction in the effectiveness of each of the shutdown systems below its minimum allowable performance standards.

6.1.13 The actuation system design should provide features for monitoring the performance of the system.

6.1.14 The absorber material for shutoff device should be selected based on following considerations:

a) Macroscopic absorption cross section,

b) Thickness/concentration of absorbing material required to ensure a black rod,

c) Stability against irradiation and other parameters,

d) Solubility and surface deposition characteristics for liquid poison, and

e) Compatibility with the chemistry of moderator water.

6.1.15 To the extent possible all components of actuation system may be replaceable.

6.1.16 The design of the pressure boundary of the system shall meet the requirements of ASME section-III sub-section NB for class-I Nuclear Power Plant components (Ref. "Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-1).

6.2 ECCS Actuation System

The actuation system should be designed to meet the performance requirements given in section 3.5 of this guide and "Primary Heat Transport System for Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-8.

6.3 CIS Actuation System

The actuation system should be designed to meet the performance requirements given in section 3.6 of this guide and "Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants", AERB/NPP-PHWR/SG/D-20.

7. SAFETY SUPPORT SYSTEMS REQUIREMENTS

The safety support systems are required for maintaining safety systems in normal state and also may be required for their operation. The support systems include the electrical and pneumatic power sources and systems essential for operation of safety actuation devices (e.g., lubricating oil). This section includes additional requirements pertinent to the support systems not specifically included in section 4.

7.1 Electrical Power Supply

7.1.1 The AC/DC power supply for safety systems shall have reliability requirements commensurate with reliability goal of safety systems. This requirement can be achieved by redundant (e.g., load sharing mode of DC.power supply), hot standby (e.g., standby UPS) power sources or from battery backup power sources for limited time.

7.1.2 The actuating systems of safety systems shall be designed to avoid spurious operation because of single failure in its power supply scheme. This can be achieved by providing redundant/hot-standby power supplies (e.g., DC power of shutoff rod clutches) or by connecting the devices to more than one power sources (e.g., valves in liquid poison injection system). The requirement of functional isolation, physical separation, single failure etc. described in section 3 and 4 are applicable to electrical power supply equipment, their location and power supply cabling.

7.2 Pneumatic Power Supply

The pneumatic power supply for safety systems shall have reliability requirement commensurate with reliability goal of safety systems. This requirement can be achieved by redundant or standby compressors. Additionally, local accumulators may be provided to specific devices of safety systems to improve availability. The general requirements of functional isolation, physical separation, single failure, etc. as described in section 3 and 4 are applicable. Pneumatic power supplies can be shared among safety systems and process systems.

8. ENGINEERED SAFETY FEATURES

8.1 Systems under ESFs

8.1.1 Additional systems and features over and above the main safety systems covered earlier, may have to be engineered to mitigate the consequences in accident conditions and to keep any radioactive release within the acceptable limits, subsequent to the action of one or more of safety systems. These are referred to as engineered safety features (ESFs) and may include

- Systems for gradual reduction of reactor containment pressure and temperature after an accident,
- Containment atmosphere clean up of fission products and filtration of radioactive particulates and iodine prior to discharge,
- Maintenance of negative pressure in secondary containment volume.

The above systems may use part of the safety related systems, if functional independence is established. The subdivisions of protection system, safety actuation system and safety system support features do not apply to ESFs and the system will be treated in an integrated manner for the specified safety task, to meet the requirements.

The classification of these systems may fall mostly under IB, based on their relative importance to safety, the time available for initiating the needed safety actions, the length of time for which the system is required once the safety function is initiated and the timeliness and the reliability with which alternate actions can be taken.

8.1.2 Manual initiation by operator action may be permitted for the above systems, with conditions stipulated in section 9. In all other respects, such systems and features should be designed to generally meet all the requirements of safety systems. Deviations may be permitted with adequate justification depending on the time available for such actions, laid out procedure etc.

9. OPERATOR INVOLVEMENT IN SAFETY ACTIONS

The requirements for design of safety systems include systematic consideration of human factors and the human-machine interface and integration of human factor processes into the overall design process. This will result in

- Adequate display of information needed to the operator for any safety action
- A structured design of controls to minimise operator mobility and to ensure that any single error on the part of the operator is inconsequential and detectable/correctable.

9.1 Manual Actions

Manual initiation or termination of certain systems or actions may be used only

- To supplement the safety actions to ensure that acceptable radiological limits are not exceeded.
- To place the plant in the long term shutdown state after the shutdown system has acted.
- To initiate certain safety actions that are not required until a later point in time subsequent to the PIE.
- For resetting and repoising the safety systems.

9.2 Operator Initiated Actions and Interventions

9.2.1 Operator initiated actions and interventions towards a safety task shall satisfy the following requirements.

- The operator is provided with written procedures to assist him,
- The required actions are simple,
- The operator is provided with sufficient means to accomplish the required actions, with due considerations to ergonomic factors,
- The operator has sufficient and clearly presented information to evaluate the status of the plant,
- The operator is allowed sufficient time to complete the required actions,
- The communication links between operators carrying out the actions are adequate to ensure correct accomplishment of these actions, and
- Magnitude of risk is low, if such manual actions are not taken.

9.2.2 Design for operator involvement shall be confined to actions that can be performed entirely in the control room or at specified backup control room / points. Information about the safety related effects of operator actions taken elsewhere shall be immediately available in the control room. Monitors displaying information required by the operator to initiate those manual safety actions that are not accomplished automatically shall be part of the safety systems.

9.2.3 The need for operator intervention on a short time scale of 30 minutes following a PIE should be kept to a minimum. The design should take into account that the credit for such operator intervention within 30 minutes of PIE is only acceptable where the designer can demonstrate that the operator has sufficient time to decide and to act, that the necessary information on which the operator must base a decision to act is simply and unambiguously presented, and that the physical environment following the event is acceptable in the control room and backup control room/points. However, even in such cases, the design shall not take credit for operator action within first 15 minutes of PIE.

9.3 Backup Control Room/ Backup Control Points

Sufficient instrumentation and control equipment shall also be located at points, which are physically and electrically separated from the main control room. This ensures that the reactor can be placed and maintained in a safe shut down state, residual heat removed, and the essential plant variables monitored should there be a loss of ability to perform these essential safety functions in the control room.

Backup control room/backup control points shall be provided as per guidelines given in safety guide, “Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants”, AERB/NPP-PHWR/SG/D-20.

10. SAFETY SYSTEM MONITORING

10.1 Requirements

10.1.1 Information about the state and availability of safety systems is essential in the control room. Information must also be available on systems and parameters required to initiate manual backup action as specified. While the former belongs to the category of safety related I & C (Category I-B, ref. "Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors", AERB/NPP-PHWR/SG/D-1), the latter shall meet the requirements of safety systems (Category I-A). Suitably designed safety systems monitoring system is therefore a required complement to the I&C of the reactor. For each safety systems, a set of parameters should be identified for monitoring, which indicate that the intended functional requirements of the system are met.

Such safety systems monitoring and display should be dedicated to those systems and may not form part of the general plant operator information systems to meet the independence and reliability requirements of the safety systems.

10.1.2 The safety systems monitoring shall:

i) monitor, at normal times, the availability of the safety systems to perform their desired functions, should a demand be made on them,

ii) inform the operator about the state of the safety systems when a demand has been made on them,

iii) identify and inform the operator about the initiation and subsequent functional performance of safety systems in bringing the plant to and maintaining it in a safe condition following an accident,

iv) monitor the plant variables that are indicative of the safe state of the reactor, and

v) record performances of the safety systems after a demand has been made to ensure compliance with performance requirements.

10.2 Design Principles

i) The monitoring system shall be simple in design by use of minimum amount of equipment that are adequate for its basic scope.

ii) The system should not be rendered inoperative by specific design basis events under which it is intended to perform the monitoring function.

iii) The information chain may share instrumentation provided for safety and process functions; but with adequate isolation/buffering such that failure anywhere in the system shall not affect the functionality of the systems it monitors.

10.3 Reliability

The system should be reliable to a degree commensurate with its classification. Functional separation shall ensure availability of monitoring even with a single failure.

10.4 System Status Displays

The status (viz., tripped or poised/energised condition) of protection system channels, states of the safety actuation systems (shut-off rod positions, poison tank/accumulator level, pressure, valve/damper positions) shall be indicated in the control room. If any part of a safety system has been deliberately rendered inoperative, by built-in design features, this state shall be automatically indicated in the control room. If any part of the safety systems has been rendered inoperative by administered means, the design of the information display equipment shall permit the operator to manually input this bypass status to the information display equipment.

10.5 Parameter Displays

Parameter displays mean the display of values of plant variables characteristic of the state of the plant. The displays may actually present the variable values in digital read out on, say, a visual display unit. For the sake of redundancy, additional discrete (i.e. variable specific) display modules may be optionally provided. The display design shall facilitate cross-checking between channels that bear known relationship to one another. Wherever the cross-checking is required to establish safety systems performance, the display design shall ensure immunity to common cause failures. The measurement range of instrumentation shall cover possible range of values of monitored variables during and following an accident situation. So, the range may extend well beyond the operational range of the variable.

10.6 Operator Comprehension

The design and physical arrangement of the information display readout shall be according to good ergonomic principles. The information displayed shall be clear, unambiguous, distinguishable and comprehensive so that the operator can quickly grasp the overall situation prevailing in the plant at all times of normal and abnormal operation. The distinguishability actually means that the normal state and abnormal state shall be indicated by different display attributes like colour, flashing, caption etc., wherever necessary. To enhance attention to visual information, audible alarms of distinguishable tones may be used.

11. DESIGN VERIFICATION

To ensure that high quality standards are attained, the safety systems, including all portions of the protection system, the safety actuation systems, the safety support system and ESFs should be designed, manufactured, qualified, inspected, installed, operated, tested and maintained in accordance with applicable quality assurance programme.

The quality assurance programme should include all the activities necessary to

a) verify the adequacy of design of the safety systems and

b) ensure that the safety systems meet all the requirements of this guide.

11.1 Failure Analysis

Analyses shall be performed at appropriate stages in the design of the safety systems to verify that the combination of the protection system, the safety actuation systems and the safety support system can meet, on a continuing basis, the requirements of this guide with regard to single failures, common cause failures, and any other reliability requirements established for the safety systems. These analyses shall be documented.

11.2 Analysis of Test Provisions

An analysis of the final design should be made to verify the adequacy of the test provisions of the protection system, the safety actuation systems and the safety support systems. The results of this analysis should be documented and the documentation shall identify areas of the design that are sensitive to either equipment failure or human error in all aspects of system and equipment testing.

11.3 Reliability Analysis

Reliability analysis of a safety system should be performed using relevant component failure rates. This analysis should

i) Encompass random failures and common cause failures and human errors.

ii) Establish the relative importance to reliability of portions (sub-systems /components) of the safety systems.

iii) Establish the initial required test intervals consistent with failure rates.

iv) Establish that the reliability goal is met in operation based on the observed failures during plant tests (ref. section 3.1)

v) Define the action to be taken if the actual failure rates exceed or fall short of, the assumed design failure rates, e.g. shortening or lengthening of the test interval or replacement of those components that prevent the attainment of the reliability goal.

The results of this analysis as well as the results of periodic tests, the inservice reliability assessments and any remedial actions should be documented.

12. SYSTEM DOCUMENTATION

When the safety system design is completed, the expected system functional performance and reliability shall be documented. For additional documents required for computer based systems, refer to "Computer Based Safety Systems of Presurised Heavy Water Reactor Based Nuclear Power Plants", AERB/SG/D-25. Assumptions made in any analysis required in the design verification should be included in the documentation of that analysis. Each assumption should be stated and justified.

The documentation should include, as a minimum, the following.

(i) The PIE with an identification of their corresponding safety tasks.

(ii) The variables, or combinations of variables, that are to be sensed to provide safety actions for each design basis event. These should include the minimum number and the locations of the sensors required to monitor adequately those variables that have a spatial dependence (where measurement of a parameter varies as a function of position in a particular region, e.g. neutron flux).

(iii) The calculated range and rate of change of the variables, or combinations of variables, mentioned in item (ii).

(iv) The safety system settings for each variable listed in item (ii) in each applicable plant operating mode, including all operational and maintenance bypass conditions, and the margin between the safety system settings and the level considered to mark the onset of unsafe conditions.

(v) The maximum permitted response times of the protection systems, the safety actuation system and the safety support system needed to accomplish all the safety tasks.

(vi) Any dependency upon the operating characteristics of the safety actuation systems and safety support systems.

(vii) The conditions which, when achieved, define completion of the safety task.

(viii) The expected response times of the protection system, safety actuation systems and the safety support systems.

(ix) The range, spans and expected accuracy for each item of the protection system equipment and the safety actuation systems.

(x) A comprehensive description of the system delineating the number and location of sensors, racks, cabinets, panels, set point adjustments, operator controls, operator displays, manual provisions and system test provisions.

(xi) The design verification analyses identified in section 11.

(xii) The documentation verifying the qualification, functional performance and any other special requirements on the safety systems equipment.

(xiii) A listing of that equipment in the safety systems, whose performance may not meet the functional requirements of the system for the full life of the plant; the criterion dictating the shortened life span and the expected life span shall be stated.

(xiv) A listing of codes and standards that may have been followed in the design of the safety systems and any other useful information.

(xv) The plant conditions during which bypass of identified safety tasks are permitted.

TABLE - 1

SAFETY FUNCTIONS AND ASSOCIATED SYSTEMS IMPORTANT TO SAFETY

Sr. No.	Safety Function	Associated Safety Related Systems	Safety System Meeting the Function when Demanded	Engineered Safety Features
1	Reactor Shut Down	i) Reactor Regulating System ii) Process Control Systems Associated with Trip Parameters	i) Shutdown System-1 ii) Shutdown System-2 iii) Liquid Poison Injection System.	
2.	Heat Removal from Core	i) Primary Heat Transport (PHT) System, Steam Generators (SG) And Associated Systems. ii) Shutdown Cooling System	Emergency Core Cooling System (ECCS)	
3.	Containment of Radioactivity	i) Ventilation System ii) Cooling Water System iii) Radiation Monitoring System	Containment Isolation System (CIS)	i) Primary Containment Clean-Up. ii) Secondary Containment Recirculation and Purge System. iii) Controlled Depressurisation System. iv) Containment Heat Removal System.
4.	System Status Monitoring	i) Safety Related Process System Monitoring ii) Safety System Monitoring	Portion of Safety Systems Monitoring System Required for Operator Actions for Plant Safety.	

TABLE - 2 TYPICAL TRIP PARAMETERS AND TRIP COVERAGE

S. No.	Event/Trip Parameter	LOCA			LORA		Loss of Flow	Loss of P/Supply	Loss of secondary H/Sink
		Large	Small	Incore	Low power	High power			
1.	HIGH NEUTRON POWER	X			X	X			
2.	HIGH LOG RATE	X			X	X			
3.	HIGH PUMP ROOM PRESSURE	X							
4.	HIGH PHT PRESSURE				X	X	X	X	X
5.	HIGH ACTUAL POWER TO DEMAND POWER RATIO				X				
6.	SG LEVEL VERY LOW (2 OF 4)								X
7.	NO PCP AND S/D PUMP RUNNING		X					X	
8.	PHT LOW PRESSURE	X		X					
9.	LOW PHT FLOW						X	X	
10.	PHT STORAGE TANK LEVEL LOW		X	X					
11.	SG DELTA T HIGH								
12.	NO PCP RUNNING ON ANY BANK							X	
13.	MODERATOR LEVEL HIGH			X					
14.	PRESSURISER LOW LEVEL		X	X					

Note: This table is only indicative.
X- indicates applicable trip parameters. A minimum of two trip parameters should appear for each event.

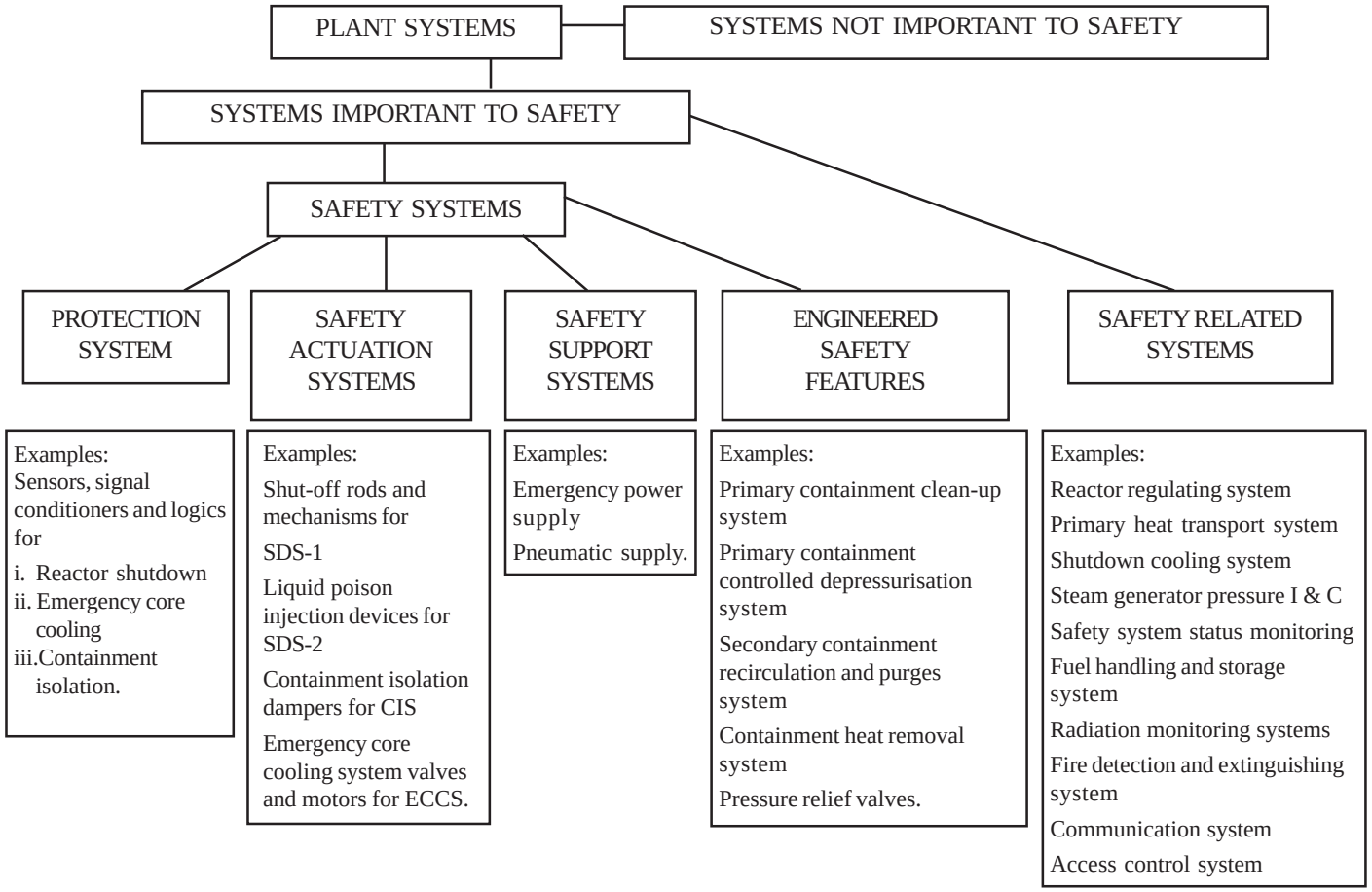

Fig.-1. CLASSIFICATION OF SYSTEMS IMPORTANT TO SAFETY

LIST OF PARTICIPANTS

WORKING GROUP

Dates of meeting:

November 16, 1995	January 16, 2002
April 9, 1996	January 29 & 30, 2002
January 29, 1997	February 19 & 20, 2002
February 25, 1997	March 15, 2002
September 06, 1999	August 05 & 06, 2002
February 7, 2000	April 10, 2003
September 13, 2000	May 10 & 12, 2003
February 13 & 14, 2001	December 11, 2003
March 13 & 14, 2001	January 15, 2004
	April 29, 2005

Members of the Working Group:

Shri. Umesh Chandra (Chairman)	:	NPCIL
Shri. K. Natarjan	:	NPCIL (Former)
Shri. B.B. Biswas	:	BARC
Dr. R. Srivenkatesan	:	BARC
Shri. Arvind kumar	:	BARC
Shri. R.Y. Apte	:	NPCIL
Shri. U.C. Muktibodh	:	NPCIL
Shri. D.K. Dave	:	AERB
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: September 06, 1999
February 13 & 14, 2001
March 13 & 14, 2001
August 5 & 6, 2002
May 10 & 12, 2003

Members of ACCGD:

Shri. S.B. Bhoje (Chairman)	:	IGCAR
Shri. S. Damodaran	:	NPCIL (Former)
Prof. N. Kannan Iyer	:	IIT-Bombay, Mumbai
Shri. V.K. Mehra	:	BARC
Shri. Umesh Chandra	:	BARC
Shri. Deepak De	:	AERB (Former)
Shri. S. Sankar	:	BARC
Shri. C.N. Bapat	:	NPCIL (Former)
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)

Dates of meeting:

September 30, 2004
October 15, 2004
October 28, 2004
November 18, 2004
February 18, 2005

Members of ACNS:

Shri. Ch. Surendar (Chairman)	:	NPCIL (Former)
Shri. S.K. Sharma	:	AERB
Shri. H.S. Kushwaha	:	BARC
Shri. R.K. Sinha	:	BARC
Shri. S.S. Bajaj	:	NPCIL
Shri. R.D. Marathe	:	L & T, Mumbai
Shri. S.P. Singh	:	AERB (Former)
Shri. P. Hajra	:	AERB
Shri. K. Srivasista (Member-Secretary)	:	AERB

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

Safety Series No.	Provisional 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 Systems for Pressurised Heavy Water Reactors
AERB/SG/D-11	Emergency Electric Power Supply Systems for Pressurised Heavy Water Reactors
AERB/SG/D-12	Radiation Protection Aspects in Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/D-13	Liquid and Solid Radwaste Management in Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/D-14	Control of Air-borne Radioactive Materials in Pressurised Heavy Water Reactors

PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUALS ON DESIGN OF PRESSURISED HEAVY WATER REACTOR (CONTD.)

Safety Series No.	Provisional Title
AERB/SG/D-15	Ultimate Heat Sink and Associated Systems in Pressurised Heavy Water Reactors
AERB/SG/D-16	Materials Selection and Properties
AERB/SG/D-17	Design for In-Service Inspection
AERB/SG/D-18	Loss of Coolant Accident Analysis for Pressurised Heavy Water Reactors
AERB/NPP-PHWR/SG/D-19	Deterministic Safety Analysis of Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/NPP-PHWR/SG/D-20	Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/D-21	Containment System Design
AERB/SG/D-22	Vapour Suppression System for Pressurised Heavy Water Reactors
AERB/SG/D-23	Seismic Qualification of Structures, Systems and Components of Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SG/D-24	Design of Fuel Handling and Storage Systems for Pressurised Heavy Water Reactors
AERB/SG/D-25	Computer Based Safety Systems of Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/SM/D-1	Decay Heat Load Calculations Pressurised Heavy Water Reactor Based Nuclear Power Plants
AERB/NPP-PHWR/SM/D-2	Hydrogen Release and Mitigation Measures under Accident Conditions in Pressurised Heavy Water Reactiors.

NOTES

NOTES

AERB SAFETY GUIDE NO. AERB/NPP-PHWR/SG/D-10

Published by : Atomic Energy Regulatory Board
Niyamak Bhavan, Anushaktinagar
Mumbai - 400 094.
INDIA

BCS