HS/R167/81
(Revised)

Central Electricity Generating Board

Health and Safety Department

DESIGN SAFETY CRITERIA FOR CEGB NUCLEAR POWER STATIONS

March 1982

B-9

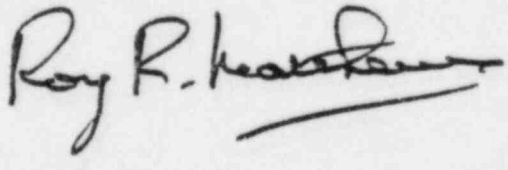
HS/R167/81
(Revised)

CENTRAL ELECTRICITY GENERATING BOARD

HEALTH AND SAFETY DEPARTMENT

Design Safety Criteria for

CEGB Nuclear Power Stations

Approved by: 

R.R. Matthews
Director of Health & Safety.

March 1982.

CONTENTS

		Page
	FOREWORD	
1.	INTRODUCTION	2
2.	GLOSSARY	3
3.	FUNDAMENTAL CRITERIA	5
	3.1 Normal Operating Doses	5
	3.2 Accidental Releases and Exposures	5
4.	FAULT AND HAZARD ASSESSMENT	6
	4.1 Faults Arising in the Reactor System	6
	4.2 Hazards Arising from within the Power Station Site	6
	4.3 Hazards Arising from Outside the Site	9
5.	ENGINEERING CRITERIA	11
	5.1 Initial Assumptions	11
	5.2 Determination of System Reliabilities	12
	5.3 Engineering Criteria for Reactor Protection Systems	14
	5.4 Dose Control	16
	5.5 Quality Assurance	18
	TABLES	
	1. Maximum Annual Design Doses for Occupationally Exposed Staff	19
	2. Permissible Frequency of Accidental Releases	20
	3. Emergency Reference Levels	21
	REFERENCES	22

FOREWORD

As an owner and operator of commercial nuclear power plant in the United Kingdom, the Central Electricity Generating Board (CEGB) is responsible for the safety of its employees and the public from any nuclear hazard arising from its installations. That responsibility is formally defined in the Nuclear Installations Acts 1965 and 1969, which control, by licence, the construction and operation of nuclear reactors, and impose an absolute liability upon the CEGB, as licensee, for any injury or damage caused by the release of radioactive material from its installations.

That responsibility is fully recognised by the CEGB and leads it to give the highest priority to the maintenance of nuclear safety standards in order to ensure the radiological protection of both personnel and the environment, and, in particular, to safeguard the public.

The policy adopted by the CEGB to achieve nuclear safety embodies certain fundamental principles, the main features of which are :-

- As a result of normal operation of a nuclear power station, no person shall receive doses of radiation in excess of the appropriate limits;
- The exposure of individuals to radiation shall be kept as low as is reasonably practicable;
- The collective dose equivalent to operators and the general public as a result of the operation of a nuclear installation shall be kept as low as is reasonably practicable;
- All reasonably practicable steps shall be taken to prevent accidents;
- All reasonably practicable steps shall be taken to minimise the radiological consequences of any accident.

The first three of these items are directly related to the design and layout of the plant and the provision of safeguards, the operating procedures for normal operation, and the policy adopted for the management of radioactive wastes. The fourth item is related to the integrity of the plant and to the provisions made for detecting abnormal conditions, for shutting down the reactor and cooling it after shutdown, and the fifth item is related to mitigating the consequences of nuclear accidents.

The dose limits referred to in the first of the features listed above have been set by reference to the recommendations of the International Commission on Radiological Protection (ICRP) (Ref.1), a body whose competence in this field is universally recognised. These recommendations are endorsed in the UK by the National Radiological Protection Board (NRPB) (Refs. 2 & 3). As a member of the European Communities, the UK has obligations under the Euratom Treaty and the practices adopted by the CEGB are required to conform to the appropriate Council Directive (Ref.4).

This document provides guidance on the interpretation and application of these principles in the design of future nuclear power stations.

1. INTRODUCTION

This document specifies the safety criteria against which future nuclear power stations should be designed so that they can be constructed and operated on sites near to urban areas. The criteria are design targets and not operational limits. If a particular reactor design does not meet the criteria in all respects it does not automatically follow that the design will be unacceptable from a safety point of view. Specific reactor designs or particular sites may have inherent safety features which cannot be taken into account until detailed proposals are available for assessment. However, whilst there is some latitude in both the releases and risk criteria quoted, the margins are such that these can only be exceeded in a small number of individual cases if the general safety objectives are to be met and an acceptable design produced.

The CEGB requires the use of numerical probability analysis in safety assessments wherever appropriate, as the technique ensures that a systematic approach is followed and that a balanced design is achieved in terms of safety performance. At the present time there are limitations which do not allow a numerical safety assessment to give an absolute indication of safety for some items of plant, although it can still form an important part of the safety demonstration. For example, it may not be possible to provide the necessary degree of assurance in the numerical reliability predictions for particular structural items of plant. In such cases the CEGB is prepared to accept non-numerical safety claim based on logical engineering arguments as a legitimate part of a safety case.

If the application of any particular criterion leads to undue complication of design or excessive cost, or if it proves impracticable to meet it for a particular reactor design, then the applicability of the criterion to that specific reactor will be reviewed. However, the overall standard of safety given in this document shall be the design objective in all cases.

In order to meet the basic safety objective of keeping doses to people as low as reasonably practicable, designers shall, in addition to meeting the criteria given in this document, take all reasonably practicable steps to this end without introducing unnecessary complexity into the design, operation, maintenance, inspection or testing of plant, particularly of protection systems, or without incurring unduly high costs.

These safety criteria take into account the Safety Assessment Principles of the Nuclear Installations Inspectorate (Ref. 5). For particular projects, the criteria are amplified by the CEGB's Generation Development and Construction Division into Design Safety Guidelines for issue to the CEGB's contractors. Typical of these Guidelines are those which have been issued for the Sizewell 'B' PWR Project (Ref. 6).

Where terms used in this document are intended to have a specific meaning they are defined in the glossary.

2. GLOSSARY

Accident - An event which leads to an unplanned release of radioactivity to the environment, or an unplanned operator exposure.

Control Points - The points from where local control may be undertaken of equipment, plant or plant items.

Emergency Control Centre - That room or area provided for the overall supervision of emergency actions.

Emergency Control Room - That room where limited reactor control is exercised in emergencies upon the unavailability of the main control room.

Emergency Reference Level (ERL) - The emergency reference level of dose is the radiation dose below which countermeasures are unlikely to be justified. When the dose seems likely to exceed the emergency reference level, countermeasures should be undertaken if a substantial reduction of dose is likely to be achieved and if the countermeasures can be carried out without undue risk to the community. The countermeasures appropriate to doses only moderately in excess of the emergency reference level should be such that they do not involve appreciable risk to the community. Countermeasures involving greater hazard should be called for only if radiation exposures would otherwise be considerable.

NOTE: The emergency reference level of dose (ERL) was originally defined by the Medical Research Council (MRC) (Ref.7) and subsequently endorsed by the National Radiological Protection Board (NRPB) (Ref.8). Further advice by the NRPB (Ref.9) now recommends ranges of dose equivalents in respect of the introduction of countermeasures.

In this document (the CEGB Design Safety Criteria), the emergency reference levels of dose are taken as the lower limits for evacuation as specified by the NRPB (Ref.9). These are detailed in Table 3.

Fault - a failure of equipment or plant item to perform its design function.

Incident - An event which causes an unplanned change in plant operating conditions.

Main Control Room - That room (or rooms) where centralised control is exercised for the reactor-generator unit, both in normal operation and most emergency conditions.

Protection Systems - All systems necessary to limit radiological hazards which may arise from any incident at the reactor site to within the design levels.

Protection Equipment - Equipment which forms part of a protection system.

Safety Related Equipment - Plant, equipment, structures or systems having a significant but not necessarily direct effect on nuclear safety. This is intended to include all equipment which is essential to nuclear safety and also such equipment as :-

a) Instrumentation, equipment, plant or systems whose failure would not cause an unacceptable radiological hazard but would cause a demand on a protection system;

b) Instrumentation used to warn of the imminent onset of conditions which could potentially cause an unacceptable radiological hazard;

c) Instrumentation used for monitoring the protection systems;

d) Communication systems.

Shall, should - Where shall is used in these criteria with no qualification, this indicates a mandatory requirement with no discretion permitted and no judgement to be made.

Where should is used in these criteria, the requirement is considered to be a sound recommendation for the achievement of nuclear safety but where discretion is permitted and where judgement may be necessary in interpretation.

ALARA, ALARP - It should be noted that ICRP 26 and associated health physics documents use the phrase, "as low as reasonably achievable, economic and social factors being taken into account." This is often shortened to the acronym 'ALARA'. This acronym is usually taken as being synonymous with the phrase, "as low as reasonably practicable," (ALARP) used in the NII document 'Safety Assessment Principles for Nuclear Power Reactors' (Ref.5) and in the Health and Safety at Work etc. Act 1974. In general this latter phrase or its acronym are used in this document.

3. FUNDAMENTAL CRITERIA

3.1 Normal Operating Doses

3.1.1 Public

Radiation dose to the public resulting from the operation of nuclear power stations can arise from three sources :-

(i) Liquid effluent discharges;

(ii) Gaseous effluent discharges;

(iii) Direct radiation from plant and buildings.

Authorisations for (i) and (ii) are granted by the Department of the Environment and the Ministry of Agriculture, Fisheries and Food taking account of the location and local conditions around the station. The relevant plant shall ensure compliance with the authorised annual limits which are based on the discharges being as low as reasonably achievable and the resultant doses being in accordance with the ICRP dose recommendations.

For design purposes the dose from (iii) should not exceed 5 mrem (50 μSv) per annum, taking into account local occupancy factors and any other station on the site.

Estimated doses to the public should be derived from the above considerations and should include any existing station sources on the site, for assessment against a level of 1/30th of the ICRP limits for the general public in any year (Ref.1).

3.1.2 Station Staff

The maximum design radiation doses for occupationally exposed staff are given in Table 1.

The station collective effective dose equivalent should not exceed 0.2 man-rem (0.002 man-Sv) per annum per MW(e) installed capacity.

3.2 Accidental Releases and Exposures

3.2.1 Public

(i) The predicted accident frequency for doses of 1 ERL (e.g. 10 rem (100 mSv) whole body dose) should not exceed 10^{-4} per reactor year. Accidents resulting in lower doses are acceptable at higher frequencies, in accordance with Table 2.

(ii) For any single accident which could give rise to a large uncontrolled release of radioactivity to the environment resulting from some or all of the protective systems and barriers being breached or failed, then the overall design should ensure that the accident frequency is less than 10^{-7}

per reactor year. This is to be interpreted as meaning that the product of the initiating fault frequency and the probability of failure to control the accident should be less than 10^{-7} per reactor year.

(iii) The total frequency of all accidents leading to uncontrolled releases, as in (ii) above, should be less than 10^{-6} per reactor year.

NOTE: If these targets cannot be achieved in all cases then in special circumstances some variation may be acceptable with the agreement of the CEGB. For example, releases giving doses up to several ERL (not exceeding 10) may be acceptable at frequencies somewhat higher than that in (ii).

Table 3 gives the ERL dose equivalent levels for the whole body and individual organs.

3.2.2 Station Staff

In the design of plant, steps should be taken to minimise, as far as is reasonably practicable, the doses to operators which might occur under accident conditions.

4. FAULT AND HAZARD ASSESSMENT

4.1 Faults Arising in the Reactor System

All potential faults arising within the reactor and reactor support systems shall be considered. Measures should be taken to keep the probabilities and consequences thereof as low as reasonably practicable. Protection systems shall be provided to meet the requirements of 3.1.1.

Faults to be considered include failure of reactor control, loss of cooling, loss of coolant, failure of internal structures, failure of mechanisms and failure of rotating machinery.

4.2 Hazards Arising from within the Power Station Site

All potential hazards originating from within the power station site boundary shall be considered. Those hazards to be considered shall include fires, explosions, releases of gases, water, steam or noxious substances, failure of pressure parts, supports, or other structural components, disruptive failure of rotating machinery and dropped or impacting loads.

It will be necessary to ensure that hazards considered within this category do not give rise to conditions which might invalidate the protective systems and lead to an unsafe situation.

Particular preventive and protective requirements associated with these hazards are detailed below.

4.2.1 Fires and Explosions

(i) Preventive Requirements

Non-combustible and heat-resistant materials shall be used wherever practicable throughout, particularly in locations such as the containment, control rooms and where any safety related equipment is located. Safety related structures, systems, cabling and components shall be designed and located to minimise, consistent with other safety requirements, the probability and effect of fires and explosions.

Where it is impracticable to use non-combustible materials then the use of installations and materials specifically designed to reduce the rate of propagation of fire shall be used.

(ii) Protective Requirements

Fire detection and fighting systems of appropriate capacity and capability shall be provided. They shall be designed to minimise the adverse effects of fires on safety related cables, structures, systems and components. Fire fighting systems shall be designed to ensure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems and components.

Unless special provisions are identified, the possibility that combustible material may be inadvertently deposited by operators in vulnerable areas shall be taken into consideration.

4.2.2 Release of Gases, Water, Steam or Noxious Substances

(i) Preventive Requirements

Structures containing gases, liquids, or noxious substances shall be designed so as to minimise as far as reasonably practicable the possibility of sudden failure.

Safety related structures, systems, cabling and components shall be designed and located so as to minimise, consistent with other safety requirements, damage due to the release of gas, water, steam or any noxious substance.

Special care shall be taken to ensure that the release of any of the above substances will not prevent any necessary operator action to control the incident or to safely shut down and cool the reactor.

The possibility of toxic gases or smoke entering the ventilation system and thereby affecting the operators should be minimised.

(ii) Protective Requirements

Notwithstanding the preventive measures, the possibility that any container of the above substances may fail and release its contents shall be considered and where necessary the means to control the effects of such releases shall be provided.

Suitable alarms shall where necessary be provided in the ventilating systems.

4.2.3 Failure of Pressure Parts, Supports or Other Structural Components

(i) Preventive Requirements

All safety related structures should, if possible, be sited such that they are not exposed to the risk of damage from impact loads, or be otherwise protected.

(ii) Protective Requirements

All reasonably practicable measures shall be taken to reduce to a minimum the possibility of damage to safety related structures, systems and components following failure of any structure.

(iii) Consequences of Failure

All consequential effects shall be considered and assessed using methods agreed by the CEGB. For pressure parts the following shall be taken into consideration:-

External Thermal Damage

Quasi-Static Overpressure

Drag Forces and Impulse Loadings in the Discharging Fluid Stream

Jets

Pipe Whip, Reaction Loads and Thermal Stresses on the Discharging Pressure System

Pressure and Rarefaction Waves

Missiles and Pipe Splits

Blanketing Effect of the Discharged Fluid

4.2.4 Disruptive Failure of Rotating Machinery

Attention shall be given to the need to minimise the risk to safety related plant arising from failure of rotating machinery. In particular, the possibility of disruptive failure of the main turbo-alternator shall be taken into account when considering plant layout.

(i) Preventive Requirements

Devices shall be provided to prevent the overspeeding of rotating machinery whose disruptive failure could potentially cause a safety hazard. Alarms shall be provided where practicable to warn the operator of incipient failure, e.g. excessive vibration alarms.

(ii) Protective Requirements

Any plant having an essential post-trip function should be sited such that it is not exposed to the risk of damage in the event of the disintegration of other plant notwithstanding any preventive measures that have been provided. The likely size, speed, and trajectory of potential missiles shall be assessed. Missile barriers of adequate integrity shall be provided.

4.2.5 Dropped or Impacting Loads

It shall be assumed that any load which may be required to be lifted or carried may also be inadvertently dropped and therefore the probability of the load being dropped and causing accidental damage shall be assessed. The following engineering measures shall also be taken:-

(i) Preventive Requirements

Adequate interlocks shall be provided to prevent the inadvertent release of any load whilst being transported.

(ii) Protective Requirements

Wherever practicable, protection systems and plant whose failure could cause a release of radioactivity shall be sited such that they are not exposed to the risk of damage from dropped loads. Adequate shields should otherwise be provided.

4.3 Hazards Arising from Outside the Site

The following external hazards shall be considered and, where appropriate, taken into account in the design. Requirements in respect of each hazard are detailed in the following sub-sections :-

(i) Earth Tremors

(ii) Extreme Winds

(iii) Extreme Temperatures

(iv) Site Flooding

(v) Aircraft Crash

(vi) Dangerous Substances

(vii) Sabotage

It will not be necessary to compute the probability of these hazards causing releases of radioactivity if it can be shown that no major damage will result to safety related structures and that the probability of failure to cool and shut down the reactor is not greater than 10^{-3} per demand for the hazards specified.

If it is not possible to demonstrate, for any individual hazard, that a particular design, or design feature, can meet these requirements, the safety case will, nonetheless, be acceptable if it can be shown that the summated probability criterion is still met.

The possibility of damage to protection systems and plant, where failure would result in a release of radioactivity, caused by the collapse of buildings or structures shall be taken into account in the accident analysis.

4.3.1 Earth Tremors

The station shall be designed to withstand the effects of the safe shut-down earth tremor (SSE) and the reactor shall be capable of being shut down and cooled to a safe state after such an event.

Free field ground motions associated with the SSE will be specified by the CEGB for each site.

4.3.2 Extreme Winds

All safety related structures shall be designed to conform with the British Standard Code of Practice 3, (CP3) Chapter 5, part 2 1972 using an agreed value for S_3.

The principal structures shall be classified in accordance with CP3 for design purposes.

4.3.3 Extreme Temperatures

The range of temperatures to be used for design purposes will be specified by the CEGB for each site.

4.3.4 Site Flooding

A design basis flood level will be specified by the CEGB for each nuclear power station based on historical tide recordings and taking into account tidal surges, wave heights, fresh water flows and any other local phenomena which could affect water levels.

4.3.5 Aircraft Crash

Attention shall be given to the station layout to minimise, as far as reasonably practicable, the effects of an aircraft crash on the station site.

Segregation and/or bunkering of protection systems should be carried out as far as reasonably practicable.

In addition to the above, specific criteria will be specified by the CEGB where appropriate, against which plant and structures should be designed.

It will be necessary to show that effective fire fighting services will still be available on the site following an aircraft crash.

4.3.6 Dangerous Substances

Detailed consideration shall be given to the possibilities of dangerous substances affecting the safety of the nuclear power station if the reactor site is within ten kilometres of any installation potentially using or storing such substances or any route used for transportation thereof.

Criteria appropriate to each site will be specified when necessary by the CEGB, taking into account the amount and type of substance, distance from the reactor, topography of the countryside, prevailing winds and any other relevant local factors.

4.3.7 Sabotage

Consideration shall be given during the design and layout phase of all nuclear power stations to the problem of site security. The aim shall be to provide protection against unauthorised entry, deliberate maloperation and sabotage.

5. ENGINEERING CRITERIA

5.1 Initial Assumptions

5.1.1 Reliability Criteria for Reactor Protection Systems

For the initial purposes of system design, it should be assumed that failure of a system occurs when the relevant fuel or plant design or test parameter is exceeded, and that such failure will result in a release of activity. It is accepted, however, that this approach will lead to an unnecessary level of conservatism in some cases, and in these cases, alternative arguments may be advanced.

System reliabilities are thus conservatively determined by :-

(i) For any single fault, the product of the initiating fault frequency and the probability of protection system failure should be less than 10^{-7} per reactor year.

(ii) For all faults, the sum of the product of each initiating fault frequency and corresponding probability of protection system failure should be less than 10^{-6} per reactor year.

5.1.2 Very Low Frequency Faults

The following requirements shall apply to those faults which have a sufficiently low probability of occurrence that they do not directly determine system requirements:-

(i) All initiating faults which are claimed to be of very low frequency shall be identified. A preliminary justification for such claims shall be agreed at the early stages of reactor design. The probabilities and consequences of each fault shall be examined in sufficient detail to judge the likely outcome and, where reasonably practicable, steps should be taken to limit the consequences if the fault occurs.

(ii) All very low frequency fault sequences should be followed to the extent necessary to demonstrate that the criterion 3.2.1 (iii) is not likely to be exceeded.

5.1.3 The Role of Containment and the Primary Coolant Boundary

The additional protection afforded by the primary coolant and containment boundaries may be invoked in determining system design reliabilities provided :-

(i) Any analysis of the fault is based on well-understood physical processes.

(ii) The number of faults in this category is limited.

5.2 Determination of System Reliabilities

5.2.1 Data

Data used in calculations which demonstrate the adequacy of reliability should be treated to take account of uncertainties. The methods and data used shall reasonably ensure that the estimates of system reliabilities are not optimistic. Sensitivity studies shall be performed to identify critical items.

5.2.2 Common Mode Failure

The probability of common mode or systematic failures affecting systems shall be considered. The probability of a common mode failure shall not be assumed to be less than 10^{-5} per annum post fault unless a lower figure can be justified.

If more than one system is needed in order to comply with the above requirement, it shall be shown that the additional system(s) is adequately diverse in design, function and segregation. The extent and depth of the justification of diversity shall be determined by the required overall reliability of the systems.

5.2.3 Maintenance and Testing

When considering the effects of the unavailability of plant items and systems during maintenance and testing a probabilistic approach is acceptable for those components where it can be shown that the probability of exceeding the assumed maintenance or test period is small. Adequate system functional performance shall be available during all times such performance may be required.

5.2.4 Human Factors

When human activities are required in the safety case such as maintenance, testing and pre- and post-trip operations, such activities shall be examined for their complexity, equipment interfaces, timescales, environmental influences, forms of instruction and staff availability, to justify the likelihood of human error being acceptably low and to show that :-

(i) Adequate corrective actions can be taken before system reliability has been significantly affected.

(ii) Adequate administrative control can be exercised.

(iii) Adequate post maintenance functional testing can be performed.

(iv) Failure in operator action following an incident is unlikely to lead to an irrecoverable situation.

5.2.5 Confirmation of System Functional Performance

In order that the systems are functionally adequate in design the following principles shall be adopted :-

(i) Where two or more mutually redundant or diverse systems are provided to achieve a given function, the functional performance requirements should be met when the least effective system is assumed to operate alone. When there are several systems provided in series (e.g. trip system and heat removal system), either the design requirements should be met when the combination of the least effective systems operates or the probability of this combination shall be shown to be insignificant. This should be shown for every possible combination of systems.

(ii) Experimental data used in calculations which demonstrate the adequacy of performance shall be treated statistically to take account of possible errors and uncertainties. The methods and data used shall reasonably ensure that the estimates of system performance are not optimistic. Sensitivity studies shall be performed to identify critical parameters.

(iii) Where it proves impracticable to obtain adequate data to justify the design requirement of functional performance of systems, then in-situ tests shall be performed on these systems to demonstrate their functional adequacy.

(iv) Confirmation of design system functional performance shall be demonstrated at an appropriate time by tests of representative equipment and plant items.

5.3 Engineering Criteria for Reactor Protection Systems

These criteria are additional and complementary to the requirements of 5.1.1.

Wherever practicable, systems shall be designed to be fail-safe in the event that a fault occurs in that system.

For those faults which originate in the control or protection equipment and which could lead to a release, no claim shall be made for the control or protection function provided by this equipment. Alternative protection systems of appropriate reliability shall be provided to ensure reactor safety under such conditions.

5.3.1 Separation of Function

In general, systems provided for protection purposes should not be used to achieve station control or operational functions.

If this cannot be achieved, protection systems may be used for control or other operational functions where control action can be demonstrated not to reduce the reliability below that required of the protection function and the control action does not seriously affect the operating lifetime of the equipment to the detriment of the assessed reliabilities. Adequate isolation arrangements should be employed to eliminate, as far as practicable, interactions between control and protection functions.

5.3.2 Segregation

To achieve satisfactory protective action in the event of external and internal hazards, the protection systems including all necessary pipework and electrical cabling shall be segregated as far as reasonably practicable. It will be necessary to ensure that the required functional performance is met at all times with the specified reliabilities.

5.3.3 Inspection, Testing and Monitoring

All safety related structures, plant and equipment shall be designed to permit inspection, testing, and where appropriate, on-load monitoring, to ensure that there has been no unacceptable deterioration in their performance or capability.

All plant items, except those whose operation would trip the reactor or produce an unacceptable plant state, shall be designed such that they can be functionally tested with the reactor at power and at shut-down. In those cases where full functional testing is not possible, equipment shall be designed so that testing can be carried out in stages without causing shut-down or unacceptable plant states, and tests should overlap so no components are left untested. Adequate functional testing should be possible at shut-down in all cases.

The frequency and method of examination and testing shall be determined by a proper consideration of the forms and rate of deterioration which can be foreseen, and by any requirement to confirm claimed reliability. These considerations may lead to a requirement for continuous monitoring of the condition of certain components, either because their performance is critical or because the nature and rate of deterioration cannot be accurately predicted. However, systems shall not be designed such that very frequent testing is used to compensate for intrinsic design weaknesses in the system.

Inspection, testing and monitoring procesures shall not result in an unacceptable degradation of reactor safety.

5.3.4 Maintenance

All equipment shall be designed to facilitate ease of maintenance and to minimise doses to operators.

5.3.5 Operator Actions

Sufficient control equipment should be provided to permit safe automatic reactor shut-down and cooling for 30 minutes post-trip for those faults where the main control room remains intact, and for 60 minutes post-trip when the emergency control room is required. Continuous operator surveillance during these periods shall be assumed, however, for the purposes of designing information display systems.

The design of control systems shall not prevent timely operator intervention at any time post-trip unless such intervention would be unsafe. Where practicable, systems shall be designed so that incorrect operator action does not lead to an irrecoverable situation.

5.3.6 Communications

Locations requiring operator manning during incidents (e.g. access control and emergency control points) shall be provided with installed means of communications with the main and emergency control rooms. Such communications systems shall be designed to operate throughout all credible faults (though accepting local damage). Where possible, the design and location of protection equipment and emergency control points shall permit the use of alternative communications methods (e.g. personal radios).

5.3.7 Emergency Control

For those hazards which could render the main control room uninhabitable, all control actions necessary to achieve a safe reactor situation shall be capable of being carried out in a controlled and co-ordinated manner from the emergency control points which are not affected by the original hazards.

The emergency control points shall be designed and located so that staff may take over control of reactor systems within 60 minutes of the start of the initiating incident. The design of reactor monitoring and control systems shall be such that destruction of either the main control room or any of the emergency control points does not prevent safe operation from the remaining intact control points.

An emergency control centre shall be provided at a position remote from the reactors where overall supervision and co-ordination of emergency actions can be carried out following an accident on the site. The centre shall be equipped with means of communication with essential personnel both inside and outside the power station site.

5.3.8 Damage Control Procedures

Consideration shall be given to means of applying damage control procedures to safety related systems. In addition to the normal fire fighting provisions, facilities for making temporary water and electrical connections should be provided as far as is reasonably practicable. The provision of these facilities shall not degrade the integrity of safety related plant or equipment.

5.4 Dose Control

5.4.1 Containment

The reactor structure, fuel storage and handling areas, active waste treatment plants and all other areas which may become contaminated with radioactive materials shall be enclosed by a structure or structures to minimise uncontrolled releases.

5.4.2 Controlled Discharges

The overall station design shall include systems such that for all normal operations, radioactive material within the station shall not reach the site boundary or beyond except in a controlled manner which allows an adequate assessment of the amount of activity discharged.

The design of ventilation systems shall ensure that, in general, air flows are from less to more contaminated areas. In general, similar principles shall apply to liquid collecting systems. Indications of the functioning of these systems shall be provided in the control rooms. These systems shall be designed so that any fault should not simultaneously release radioactive matter and cause failure of the discharge control systems.

5.4.3 Meteorological Measurements

Sufficient meteorological equipment shall be included in the design, such that if a release of radioactive material occurs, an assessment of the risk to the public in the surrounding areas can be made.

Displays of this equipment shall be available in the main control room and emergency control centre. These systems shall be designed and located such that any fault causing an uncontrolled release, or its consequences, shall not prevent operation of the meteorological equipment.

5.4.4 Operator Access

The design and layout of the station shall be such that access to contaminated areas and to areas with significant radiation dose rates can be controlled in accordance with the CEGB Safety Rules (Radiological).

5.4.5 Remote On-Site Surveillance

Environmental surveillance systems shall be designed to provide information on areas where damage control teams are most likely to require access following accidents. The displays from these systems should be at the appropriate emergency control points. Suitable installed systems shall also be included for environmental surveillance during normal operation. Where possible, equipments provided for normal conditions should also cover accident conditions.

5.4.6 Decontamination and Active Handling

Systems shall be included in the design to permit decontamination of plant items, and to permit work to be carried out on highly active plant items. Design measures shall be included to minimise levels of contamination during normal operation and following any credible accidents. Where practicable, systems shall be included to permit remote control of decontamination systems in areas requiring access following accidents.

5.5 Quality Assurance

All safety related structures, plant and equipment shall be designed, constructed, inspected and tested to technical standards commensurate with the importance of the safety functions to be performed. A comprehensive quality assurance programme shall be implemented.

The results of the quality assurance programme shall be fully documented and appropriate records shall be available throughout the life of the plant.

TABLE 1

Maximum Annual Design Doses for Occupationally Exposed Staff

Effective dose equivalent	1 rem (10 mSv)

Hands, feet, forearms, ankles	50 rem (500 mSv)
Skin (averaged over 100 cm^2)	50 rem (500 mSv)
Lens of eye	15 rem (150 mSv)

NOTES:

a) In the context of the above design doses it is not necessary to consider doses from external radiation to individual organs other than those listed in the above table.

b) In considering individual organ doses due to the additive effects of external and internal radiation, then the organ weighting factors of ICRP 26 should be used to assess the contributions to the effective dose equivalent. An overriding dose equivalent limit of 10 rem (100 mSv) will apply for organs with weighting factors less than 0.1.

c) The values specified above are intended primarily for use in the design of nuclear power stations. The target of 1 rem for effective dose equivalent is set at 1/5 of the annual limit recommended by the ICRP and is not therefore to be regarded as an operational limit. This design target provides a margin for unexpected operational requirements. Maximum operational doses will be controlled by procedures in accordance with current practice at CEGB power stations. The other values specified above are intended to prevent non-stochastic effects and are set at the annual limits recommended by the ICRP. These values will thus be actual limits during station operation.

TABLE 2

Permissible Frequency of Accidental Releases

Accidental Releases		Total Permissible Frequency per Reactor Year
ERL/1000	to ERL/100	10^{-2}
ERL/100	to ERL/10	10^{-3}
ERL/10	to 1 ERL	10^{-4}

TABLE 3

Emergency Reference Levels

	Dose Equivalent
Whole Body	10 rem (100 mSv)
Thyroid, lung or other single organs	30 rem (300 mSv)
Skin	100 rem (1.0 Sv)

NOTE: These emergency reference levels are equivalent to the lower limits for evacuation as specified by the National Radiological Protection Board. (Ref. 9)

REFERENCES

1. INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION

Recommendations of the ICRP (adopted 17 January, 1977) Pergamon Press, Oxford. Ann. ICRP, 1977, ICRP Publication 26.

2. NATIONAL RADIOLOGICAL PROTECTION BOARD

ASP 1 - Recommendations of the ICRP (ICRP Publication 26): Statement by the NRPB on their acceptability for application in the UK. HMSO, London 1978.

3. NATIONAL RADIOLOGICAL PROTECTION BOARD

ASP 2 and ASP 2, Addendum A - The application of the ICRP recommendations: Advice to the expert group reviewing the White Paper Command 884 "The Control of Radioactive Wastes". HMSO, London, 1978.

4. COUNCIL OF THE EUROPEAN COMMUNITIES

Council Directive of 15 July, 1980, amending the Directives laying down the basic safety standards for the health protection of the general public and workers against the dangers of ionising radiation. Official Journal of the European Communities, 1980, 23, 17 September, L246.

5. HM NUCLEAR INSTALLATIONS INSPECTORATE

Safety Assessment Principles for Nuclear Power Reactors. Health & Safety Executive, London, April 1979.

6. CENTRAL ELECTRICITY GENERATING BOARD

PWR Design Safety Guidelines.

7. MEDICAL RESEARCH COUNCIL

Criteria for controlling radiation doses to the public after accidental escape of radioactive material. HMSO, London, 1975.

8. NATIONAL RADIOLOGICAL PROTECTION BOARD

ERL 1, Emergency Reference Levels: interim guidance, HMSO, London, 1978.

9. NATIONAL RADIOLOGICAL PROTECTION BOARD

ERL 2, Emergency Reference Levels: criteria for limiting doses to the public in the event of accidental exposure to radiation. HMSO, London, 1981.