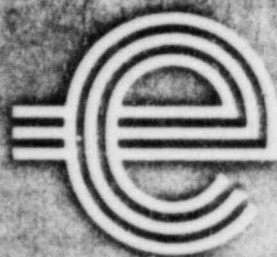


SEP 14 1982



## Central Electricity Generating Board

GENERATION DEVELOPMENT AND CONSTRUCTION DIVISION

Plant Engineering Department

Nuclear Plant Branch

PRESSURISED WATER REACTORDESIGN SAFETY GUIDELINES

Issue A      April 1982

8507180328 850606  
PDR FOIA  
SHOLLY83-619 PDR

B-17

CENTRAL ELECTRICITY GENERATING BOARD

Generation Development and Construction Division

Plant Engineering Department

Nuclear Plant Branch

PRESSURISED WATER REACTOR

Design Safety Guidelines



## CENTRAL ELECTRICITY GENERATING BOARD

Generation Development and Construction Division

Plant Engineering Department

Nuclear Plant Branch

PRESSURISED WATER REACTOR

Design Safety Guidelines

Issue	Date	Verified	Approved	Pages Amended
A	April 1982	<i>David S. / 1982</i>		

## PRESSURISED WATER REACTOR

## Design Safety Guidelines

Advice on general safety requirements for all types of new CEGB nuclear stations has been provided by the Board's Health and Safety Department in its publication "Design Safety Criteria for CEGB Nuclear Power Stations" HS/?. These Design Safety Guidelines amplify the Design Safety Criteria and are prepared by the Board's Generation Development and Construction Division specifically for the Pressurised Water Reactor in agreement with Health and Safety Department.

Each reactor and station shall be so designed and constructed that it can be readily maintained and operated economically without causing unacceptable risk to either the operators or members of the public. To this end all reasonably practicable steps shall be taken to reduce radiation doses in normal operation and maintenance work, to minimise the probability of accidental releases of radioactive material due to any cause whatsoever and, should such an accident occur, to minimise the consequential doses.

Although the attached Annexes contain a number of mandatory requirements they are in general intended to provide guidelines to designers for all significant safety related matters. Should any aspect of these guidelines prove difficult to interpret, or lead to unacceptable cost or complication, or result in an inadequate design or safety case then the designer shall draw immediate attention thereto so that timely agreement can be reached on any requisite changes.

Where the plant is to be built on a site on which there is a prior installation, possible interactions between plant shall be taken into account (e.g. credible hazards created by either plant shall not cause unacceptable consequences to the other).

LIST OF ANNEXESAnnex No.

I	Standards and Quality Assurance
II	In-Service Inspection, Testing and Monitoring
III	External Hazards
IV	The Prevention of and Protection against Internal Hazards
V	Trip, Shutdown and Essential Systems
VI	Reactor Safety System
VII	Specification for Reactor Safety Systems
VIII	Reactor Shutdown Requirements
IX	Reliability Guidelines for Post Trip Cooling and other Essential Systems
X	Safety Related Electrical Equipment
XI	Emergency Control
XII	Containment
XIII	Access to Containment
XIV	Not Used
XV	Design Targets for Doses and Dose Rates
XVI	Control of Contamination in Accessible Areas
XVII	Radioactive Waste Management
XVIII	Criticality Safety Requirements and Recommendations for the Design of the Fuel Route
XIX	Radiological limits for Accidental Release of Radioactivity to the Atmosphere
XX	Control Instrumentation and Alarm Systems

Standards and Quality Assurance

Standards and Quality Assurance

All safety related structures, plant and equipment shall be designed, fabricated, constructed and tested to standards commensurate with the importance of the safety functions to be performed. The enquiry specification will include appropriate CECB, national and international standards. Where appropriate standards are not available for particular components these shall be identified and the design bases and relevant standards justified.

Every contractor for safety related structures, plant and equipment shall work to an approved quality assurance programme and the implementation of these programmes will be monitored by the Board.

In-Service Inspection, Testing and Monitoring



In-Service Inspection, Testing and Monitoring

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

Systems shall be designed with a capability to test the operability and functional performance both of the components and the systems as a whole under operational conditions or, where this would lead to unacceptable plant conditions, under conditions as close to operational conditions as possible.

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.

Testing, inspection and monitoring procedures shall not result in an unacceptable degradation of reactor safety.

External Hazards

CONTENTS

1. INTRODUCTION
2. EARTHQUAKES
3. WIND
4. SITE FLOODING
5. AIRCRAFT CRASH
6. EXPLOSIVE SUBSTANCES
7. SABOTAGE
8. EXTREME AMBIENT TEMPERATURES
9. NOXIOUS SUBSTANCES

External Hazards1. INTRODUCTION

The station should be so designed that, in the event of any of the specified hazards, failure to shut down and failure to cool the reactor will each be no greater than  $10^{-3}$  per demand where failure is defined as the causation of doses in excess of an ERL.

If it is not possible to demonstrate that a particular design, or design feature, can meet the requirements for any individual hazard then an acceptable safety case can be made so long as the probability of any release is calculated and it can be shown that both the probability and the release are acceptably low. In addition to any essential safety plant damage caused directly by the accident, the possibility of damage to such plant arising from failure of non essential buildings or structures shall be taken into account in the accident analysis. In assessing the degree of protection and separation required for essential plant due account shall also be taken of possible fires and missiles that may result from the accident.

An Emergency Control Centre shall be provided to enable the reactor safety to be ensured if it cannot be shown that the main control room remains undamaged and tenable after any credible accident.

2. EARTHQUAKES

The station shall be designed to withstand the effects of ground motions corresponding to the safe shutdown earthquake (SSE) and the reactor shall be shown capable of being safely shutdown and cooled following such an event without causing an unacceptable release of radioactivity.

The SSE ground motions have been selected to correspond to the vibratory motion expected to occur at a site selected at random within the land area of Great Britain with a cumulative probability of exceedance less than, or equal to  $10^{-4}$  per annum. At present the ground motions corresponding to SSE have a peak free field acceleration of 0.25 gravity.

An extensive study of the characteristics of seismic ground motions for UK design has been completed and as a result ground response spectra have been derived which represent hard, medium and soft site ground conditions. In addition, artificial time histories have been constructed which are consistent with the response spectra. The spectra and time histories are given in CEGB/GDCD Specification of Ground Motion Data to be used for Seismic Design of Nuclear Power Plants (Ref. 1). This Specification provides design ground motion data for the SSE.

Validation of the seismic adequacy of the plant shall be demonstrated by analysis or testing.

The test methods, calculational routes, damping factors, stress categories and failure criteria used must be justified to the satisfaction of CEGB.

3. WIND

An assessment shall be made of the effect of abnormal wind loading on any safety related structure. Where appropriate, structures shall be designed to withstand the effects of abnormal winds taking into account the best available meteorological data on wind velocity and frequency for the location. As a design target wind speeds having a probability of  $10^{-4}$  p.a. should not cause an unacceptable radiological hazard.

4. SITE FLOODING

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

5. AIRCRAFT CRASH

Provided there is plant redundancy and separation incorporated for other reasons, no specific measures need be considered in plant designs for crashing aircraft so long as the reactors are sited at least 10 km from the nearest airfield or military low-level flying areas.

If the station is sited closer than 10 km then consideration shall be given to the need for the plant to be designed to withstand an aircraft crash by physical protection, segregation or appropriate means. The specific criteria to be used for design purposes shall be chosen to take account of all aircraft, up to and including the heaviest that the airfield is licensed to handle, and making due allowance for any foreseeable development that could occur over the planned lifetime of the nuclear station. For system assessment purposes it should be assumed that a crash can take place from any direction and that the crash may occur at any point on the site. For structural design purposes it should be assumed that the fuel carried by the aircraft is released and ignited. It will be necessary to show that effective fire fighting services will still be available on the site following an aircraft crash.

## 6. EXPLOSIVE SUBSTANCES

Detailed consideration shall be given to the possibilities of off-site explosions affecting the safety of the nuclear power station if the reactor site is within 10 km of any installation using or storing potentially explosive substance or any route used for the transportation of any such substances.

Detailed design criteria will be formulated by the CECB for the site 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.

## 7. SABOTAGE

Consideration shall be given to site security and layout requirements to provide protection against unauthorised entry and to minimise the effect of possible sabotage. The manner in which this is to be achieved shall be discussed with the Engineer.

## 8. EXTREME AMBIENT TEMPERATURES

The station shall be designed to be capable both of operation at power, and of being safely shut down, for all ambient temperatures deemed appropriate. The range of temperatures to be considered shall be specified following discussions with the Engineer.

## 9. NOXIOUS SUBSTANCES

Consideration shall be given to the possibility of releases of noxious substances from containers situated off-site and to the need for protective measures for plant and personnel on-site.

## REFERENCES

1. CECB/GDCD. "Specification of Ground Motion Data to be used for Seismic Design of Nuclear Power Plants.  
Ref. No. C/JI/SD/152.0. January, 1982



The prevention of and protection against internal hazards

CONTENTS

1. INTRODUCTION
2. FIRES AND EXPLOSIONS
  - 2.1 Preventive Requirements
  - 2.2 Protective Requirements
3. GAS, WATER, STEAM RELEASE, RELEASE OF ANY NOXIOUS SUBSTANCE
  - 3.1 Preventive Measures
  - 3.2 Protective Requirements
4. DISRUPTIVE FAILURE OF PRESSURE PARTS
  - 4.1 Preventive Measures
  - 4.2 Protection Requirement in Event of Failure
  - 4.3 Consequences of Failure
    - 4.3.1 External Thermal Damage
    - 4.3.2 Quasi-Static Overpressure
    - 4.3.3 Drag Forces and Impulse Loadings in the Discharging Fluid Stream
    - 4.3.4 Jets
    - 4.3.5 Pipe Whip, Reaction Loads and Thermal Stresses on the Discharging Pressure System
    - 4.3.6 Pressure and Rarefaction Waves
    - 4.3.7 Missiles and Pipe Splits
    - 4.3.8 Blanketing Effect of the Discharged Fluid
5. DISRUPTIVE FAILURE OF ROTATING MACHINERY
  - 5.1 Preventative Requirements
  - 5.2 Protective Requirements
6. DROPPED OR IMPACTING LOADS
  - 6.1 Preventative Requirements
  - 6.2 Protective Requirements
7. OTHER SAFETY RELATED STRUCTURES

## 1. INTRODUCTION

All potential hazards originating from within the station site boundary shall be considered including fires, explosions, disruptive failure of pressure parts or rotating machinery, flooding, releases of potentially damaging substances, dropped loads and failure of static structures.

Following any internal hazard the reliability requirements of Annexes V and IX should be met where appropriate.

## 2. FIRES AND EXPLOSIONS

### 2.1 Preventive Requirements

Non-combustible and heat resistant materials shall be used wherever reasonably practicable throughout, particularly in locations such as the control room and anywhere control equipment having a safety function is located. Structures, systems, cabling and components important to safety shall be designed and located to minimise, consistent with other safety requirements, the probability and effect of fires and explosions.

### 2.2 Protective Requirements

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

Notwithstanding the preventive measures and fire detection and fighting systems defined above, it should be assumed that anywhere combustible material is, or may be, present a fire may start and the reliability requirements of Annex IX met. Note that, unless special provisions are identified, the possibility of operators (inadvertently) transporting combustible material cannot be ruled out. Barriers may be claimed to isolate and contain fires within defined fire zones. Fire fighting equipment within the zone may be claimed in arguing the effectiveness of the barriers provided that such equipment is designed to the appropriate standards of reliability and has the requisite integrity. However, all essential plant in the fire zone, other than fire fighting equipment, should in general be assumed to be incapacitated by the fire and due account shall be taken of the potential effect on any passive component (e.g. pipework).

### 3. GAS, WATER, STEAM RELEASE, RELEASE OF ANY NOXIOUS SUBSTANCE

Note, noxious substances include chlorine, CO<sub>2</sub>, ammonia, caustic soda, etc. This clause also covers the release of any substance from a gas container, although any mechanical or thermal damage following failure of a gas container is covered by clause 4.

#### 3.1 Preventive measures

Careful attention shall be paid to the design so as to minimise the possibility of release of any noxious substance.

Structures, systems, cabling and components important to safety shall be designed and located 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 shall 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 shall be minimised.

#### 3.2 Protective requirements

Notwithstanding the preventive measures, it should be assumed that any container containing any of the above substances may fail and release its contents. (Exceptions may be made by agreement of certain failures of the primary circuit). Means to control the effects of such release, including flooding, shall be provided. The reliability requirements of Annex IX should be met. In deriving the reliability as required by Annex IX due account may be taken of measures specially provided to control the situation.

Notwithstanding the preventive measures, the possibility of any of the above substances including toxic gases entering the ventilation system shall be recognised. Suitable alarms shall wherever practicable be provided. Suitable breathing apparatus shall be provided in key locations including the control room.

### 4. DISRUPTIVE FAILURE OF PRESSURE PARTS

#### 4.1 Preventive Measures

Appropriate standards shall be adopted in the design of all pressure parts (see Annex 1).

All pressure parts\* should be sited so that they are not exposed to the risk of impact loads, or should be otherwise protected.

So far as is reasonably practicable all pressure parts\* should be located in areas free of fire risk.

#### 4.2 Protection Requirement in Event of Failure

All reasonably practicable measures shall be taken to reduce to a minimum the possibility of damage to safety related systems or structures following failure of any pressure component. This should be achieved by locating such equipment, and by designing such structures, so that any damage is avoided. The possible consequences of failure of a pressure component are detailed in section 4.3. The extent of damage may be limited by providing suitable barriers or suitable restraints.

The requirements for essential systems operation following such failures are itemised in Annex IX.

An assessment of the extent of damage possible shall take into account separately or in combination any or all of the effects listed in 4.3.

Note that it is to be considered credible that any non-redundant pressure barrier can fail suddenly except where an adequate justification of incredibility can be advanced. An incredibility claim will not be acceptable unless it can be shown that all mechanisms of sudden failure e.g. fast fracture, fire, dropped loads and sabotage can be excluded. Each claim of incredibility will need to be individually negotiated with the CEEB.

#### 4.3 Consequences of Failure

The following consequential effects shall be considered and assessed using methods to be agreed with the CEEB.

##### 4.3.1 External Thermal Damage

The discharging fluid may contain substantial stored heat having the potential to cause external objects, instruments and safety system components to rise to temperatures beyond their design limits.

##### 4.3.2 Quasi-Static Overpressure

Discharging fluid may cause a significant quasi-static overpressure differential to be exerted on external structures. If within the breached pressure system there is a fluid reservoir local to the breach in addition to more distant reservoirs, there may be a substantial short term transient component to the overpressure.

---

\* Certain small pipes, fracture of which is of no consequence, might be excluded.



#### 4.3.3 Drag Forces and Impulse Loadings in the Discharging Fluid Stream

A substantial fluid velocity may exist along the discharge route. Drag forces will be produced on the walls of the route and on obstructions in the path of the fluid. Changes in direction of the fluid stream can produce momentum loads.

#### 4.3.4 Jets

A breach of a pipe or a hole in a vessel may lead to a strongly directional discharge of the contained fuel. If the discharging fluid is a gas, pressure differentials will usually be such that at the point of choking the gas flow will be sonic. Supersonic jet flows can in theory be developed by expansion downstream of the point of choking but unless the orifice were appropriately shaped (which would be an extremely unlikely eventuality in the case of an accidental fracture) shock fronts would repeatedly occur in the jet stream which would reduce the flow to sonic or sub sonic velocities, accompanied by a pressure recovery. This process continues until sufficient of the surrounding air has acquired a share of the momentum of the jet to preclude the possibility of supersonic velocities.

Very large local loadings may be produced by jets. There may be substantial energy input to structures, producing resonance vibrations taking them beyond the yield point and additionally there is a local concentration of the heating effect of the fluid, if applicable. Hence there may be a tendency towards thermal lancing.

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

The breaking of a pipe or vessel may lead to a strongly directional discharge of the contained fluid and therefore a violent reaction load on the container. Additionally a flow pattern is set up within the pressure system which may produce internal reaction/friction loads very much greater than those it experiences during normal operation. Vibrational movements which could stress components beyond their yield point may be set up. There may also be rapid and very localised internal temperature changes.

#### 4.3.6 Pressure and Rarefaction Waves

The sudden rupture of a pressure barrier generates a succession of airwaves whose leading edge precedes and eventually outstrips the fluid expansion. The front, when free of the expanding fluid, travels at sonic or supersonic velocity through the surrounding air. Waves which follow it are travelling through somewhat heated air and therefore tend



to catch up and intensify the front. This is a process known as 'shocking up'. At a few feet from the burst, the shock profile can become comparable with that produced by a high explosive detonation.

In confined areas the blast effect is intensified both in magnitude and in duration. Venting of the enclosure does not appear to be greatly helpful unless the vent area subtends a large fraction of the total solid angle viewed from the point of burst.

In the enclosed blast situation, energy is contained within the volume of the chamber, exerting an equivalent steady pressure on the walls of the chamber and any object within it. This energy is gradually dissipated by venting, transfer to the walls of the enclosure and losses producing heating. If the energy input continues after the initial blast, as it would for instance in the case of a discharging pipe, this contribution also can enhance both the magnitude and duration of the equivalent steady pressure. Very short duration peaks can exceed the equivalent steady pressure.

It is to be noted that a pressure barrier's rupture can be non symmetrical, generating a shock wave with a degree of directionality. This may be more important at small distances from the rupture than at large distances. It is to be noted that if a rupture occurs off-centre in an enclosure, the blast may be substantially enhanced locally.

The ability of a structure to withstand a blast wave is dependent on whether it can withstand the total impulse and whether it can absorb the total energy input. The transmission of a blast wave through a structure can cause the production of missiles from the back face ('scabbing').

In addition to the external overpressure wave, a rarefaction front travels back into the pressurised system from the point of rupture at sonic velocity in the pressurised fluid.

#### 4.3.7 Missiles and Pipe Splits

Test and accident reports show that the sudden rupture of a pressure barrier may generate energetic missiles. An unacceptable escalation of the accident as a result of consequential damage to other adjacent barriers must be prevented. If there is a defined route for the discharging fluid it is important that this is not disrupted by missiles.

A vessel burst can either be visualised as symmetrical or non-symmetrical. Small or large fragments may be produced, or there could be a mixture. There is no clear way of predicting what might in practice occur for a particular vessel.

Judgement shall be exercised as to what plausible missiles could prove troublesome, e.g. an end cap or coverplate. Analysis of vessel failures indicates that frequently 20 to 30% of the available energy can go into the translational energy of missiles, and exceptionally can be significantly greater.

It appears to be impossible to arrive at the shape of the missile, or its attitude when impacting on a barricade, other than by exercising engineering judgement. For a missile which takes the approximate shape of a flat plate, the conservative assumption is that it hits the barricade edge-on. It would not be conservative to assume that any of the energy of impact is necessarily absorbed in the buckling of the missile.

Depending on the thickness of a barricade, secondary missiles may be generated by scabbing from the rear face.

In the case of pipe work failure the failed part itself can cause consequential damage to other parts without necessarily becoming a missile, e.g. pipe splits.

#### 4.3.8 Blanketing Effect of the Discharged Fluid

Unless steps are taken to prevent this, accumulation of the discharged fluid may occur.

### 5. DISRUPTIVE FAILURE OF ROTATING MACHINERY

Attention shall be given to the need for minimising the risk to safety related plant arising from failure of any rotating machinery and in particular the possibility of disruptive failure of the main turbo-alternator must be taken into account when considering plant layout.

#### 5.1 Preventive Requirements

Where necessary 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.

#### 5.2 Protective Requirements

Wherever possible any plant having an established function post trip shall be so sited as to be invulnerable in the event of disintegration notwithstanding any preventive measures that have been provided. The likely size, speed and trajectory of potential missiles shall be assessed. Alternatively, missile barriers of adequate integrity shall be provided.

## 6. DROPPED OR IMPACTING LOADS

It should be assumed that any load that is lifted or transported (including the equipment for the lifting or transporting) may be inadvertently dropped or cause impacting damage unless it can be demonstrated that the probability of so doing is so low it can be ignored. If a claim of prevention of failure is to be made adequate redundancy and/or inspection or early detection of incipient failure of the whole lifting/carrying system (including its supports and the carried load) shall be demonstrated and it shall be shown that all mechanisms leading to unacceptable sudden failure (e.g. fast fracture, fire) can be excluded.

### 6.1 Preventive Requirements

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

### 6.2 Protective Requirements

Wherever practicable essential plant should be so sited that it is not exposed to the risk of dropped loads. Adequate shields should otherwise be provided.

## 7. OTHER SAFETY RELATED STRUCTURES

Appropriate standards shall be adopted in the design of all other safety related structures\* whether normally stressed (e.g. floors, core support and restraint structures and static load bearing structures) or unstressed (e.g. anti-seismic devices or missile barriers) in accordance with Annex I. If a claim of incredibility of failure is to be made, adequate strength margins, redundancy, inspection or early detection of incipient failure shall be demonstrated in respect of both cyclic and static stresses and it shall be shown that all mechanisms leading to unacceptable sudden failure e.g. fast fracture, fire, sabotage, corrosion and impact can be excluded.

---

\* Note: a structure is safety related if its failure can either directly or indirectly affect the integrity of any essential system.

Trip, Shutdown and other essential systems

CONTENTS

1. INTRODUCTION
2. BASIS OF RELIABILITY TARGETS
3. GENERAL RELIABILITY REQUIREMENTS
4. SIMPLIFICATION OF GENERAL EQUATION FOR DESIGN PURPOSES
  - 4.1 Fuel and Plant Constraints
  - 4.2 Incredible Initiating Faults
  - 4.3 Reliability Targets for Systems Other Than Containment System
  - 4.4 Reliability Targets for Containment Systems
5. FAULT CLASSIFICATION AND DERIVATION OF INDIVIDUAL REQUIREMENTS
  - 5.1 Confidence Levels for Transient Calculations
6. ADDITIONAL RADIOLOGICAL REQUIREMENTS

## 1. INTRODUCTION

This document derives reliability targets for trip, shutdown and essential cooling systems.

These targets are derived from the basis that the probability of an uncontrolled release of radioactivity is to be kept acceptably low. The quantification of what is judged acceptably low is detailed in Section 2.

In outline the approach is to group faults into various classes, and then by ascribing an initiating event probability for each class of fault to derive the reliability with which systems should operate.

In applying the approach it is recognised that it is not always possible to derive rigorously probabilities of certain faults such as failure of structural plant items. In such cases, probabilities have to be assigned on the basis of engineering judgement. However, the probability approach is still of significant value in that it defines in a logical way target reliability requirements for the systems. It is also recognised that certain faults may be excluded from the probability analysis and treated in a deterministic way. Such faults include external hazards; it is judged that provided the requirements of Annex III are met that these faults can be excluded from the probabilistic approach of this Annex.

It is emphasised that, although the desirability of keeping the guidelines as simple as possible is recognised, the subject is complex involving as it does many variables. Because of the complexity the interpretation of the targets derived in this Annex are detailed in separate Annexes elsewhere (Annex VI for the trip system, VIII for reactor shutdown systems, and IX for post trip essential systems). However, in order to derive separate targets for the trip, shutdown and cooling systems certain pessimistic assumptions have to be made. Such assumptions may prove too pessimistic for certain faults. These cases may be studied instead against the general approach of this Annex. Similarly alternative approaches, covering all faults, which meet the general guidelines are permitted.

These targets have been proposed to ensure that a disciplined approach is made to the design of systems and that adequately reliable systems are developed. However, any targets laid down in this document are not to be confused with the ultimate safety claim. It is not essential that these guidelines be met in all respects in order to ensure adequate safety.

It is noted that the numerical/probability treatment can only form part of the safety case and then only when adequate evidence is available. Regardless of numerical targets, the protective systems shall be designed and constructed throughout to high engineering standards and integrity of operation bearing in mind the importance of the functions to be carried out, particular regard being paid to the principles of diversity and segregation detailed in Annexes VI, VII, VIII, IX, X and elsewhere. Items should be conservatively rated for duty and environment (normal operation and incidents). Where the numerical approach is adopted additional guidance is given in Annexes VI to X inclusive to cover:-



## Diversity requirements

The distributions applied to failure data

The confidence levels of the frequencies and probabilities

The treatment of common mode failures

How operator and maintenance errors will be handled.

In particular, Clauses 5.1, 5.3, 5.4 and Clause 6 of Annex IX shall apply generally, except to Annexes VI and VII where rules are separately defined. Also, the single failure criterion of Annex IX (see overriding requirement) shall apply generally to all safety related systems and not only to post trip cooling systems.

In those cases where relevant data cannot be obtained alternative arguments may be adopted by agreement with the C.E.G.B. Such areas where this arises shall be identified as early as possible.

The minimum amount of operational protection system equipment for which reactor operation will be permitted shall be defined.

## 2. BASIS OF RELIABILITY TARGETS

It has always been the endeavour of the nuclear industry to ensure that the risks from nuclear plant are lower than the everyday risks of life that currently exist, and can be compared favourably with other risks for similar types of activity that society finds reasonable. Some authoritative opinions on the acceptability of risk by society have been published, e.g:-

- (a) ICRP Publication 26 in para. 18 indicates that risk of death in the range of  $10^{-6}$  to  $10^{-5}$  per year would be likely to be acceptable to any individual member of the public.
- (b) Lord Ashby in his book "Reconciling Man with the Environment" on page 71 states that as a very rough generalisation it can be said that risks (of death per annum) of 1 in 1 million are of no concern to the average person.
- (c) The Sixth Report of the Royal Commission on Environmental Pollution in para. 171 also states that risks of death for an individual below 1 in 1 million per year are generally accepted without concern.
- (d) The First Report of the Health and Safety Commission's Advisory Committee on Major Hazards in para. 19 expresses the view that a  $10^{-4}$  risk per year of a serious accident in a non-nuclear process plant causing death or injury might perhaps be regarded as just on the borderline of acceptability.

Consideration of such opinions and surveys of international nuclear practice and hazardous non-nuclear industries lead to the following targets:-

- (i) The predicted accident frequency for doses of 1 ERL (e.g. 10 rem whole body dose) should not exceed  $10^{-4}$  per reactor year. Accidents resulting in lower doses are acceptable at higher frequencies, as specified in Annex XIX.
- (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 CEEGB. For example, releases giving doses up to several ERL (not exceeding 10) may be acceptable at frequencies somewhat higher than that in (ii).

### 3. GENERAL RELIABILITY REQUIREMENTS

Of the targets identified in Section 2, the one covering all incidents is possibly the most severe. This can be expressed:-

Total probability of an uncontrolled release

$$< 10^{-6} \text{ p.a.}$$

Following any initiating fault, an unacceptable release can occur as a result of the trip, shutdown, cooling or containment systems failing to work effectively (either because they did not work as designed or because inadequate allowance had been taken of random variations in reactor parameters or of uncertainties in physics predictions of fault behaviour).

Given any particular initiating fault there are many different fault sequences. For each sequence a probability of a release to the environment in principle can be evaluated. Each sequence can be constructed as follows:-

Following the fault the reactor may trip via the first or second line of protection. It is most likely that a trip will occur via the first line however (with a probability of virtually 1) but there does remain a small probability (typically around  $10^{-4}$ ) that the first line fails. Similarly, following the trip, although it is most likely that all the shutdown devices will operate, there is a certain probability that one or more components

will fail. There is also a possibility, however remote, that due to some completely unforeseen event there could be a systematic failure of a large number of similar components in the shutdown system(s). In principle one can ascribe a probability to any particular combination of shutdown system component failures. Also, following reactor shutdown, although there is a high probability that the post trip cooling systems will work as designed, there is a possibility that certain faults will make cooling less than 100% effective.

It may thus be seen that one can construct various fault sequences depending upon line of trip, effectiveness of shutdown and cooling and derive a probability for each sequence.

Finally, for each sequence one can calculate a temperature transient, evaluate the probability of any activity release from the reactor and from this evaluate the probability of a release to the environment (taking into account the available barriers including containment).

By summing over all such sequences and all initiating events one can arrive at an overall probability of an uncontrolled release.

Mathematically, the above can be expressed as follows:-

$$\sum_i \sum_N \sum_M \int_C \int_R \left\{ P_i \cdot \text{prob}(N/i) \cdot \text{prob}(M/N,i) \cdot \text{prob}(C/N,M,i) \times \right. \\ \left. \text{prob}(R/N,M,C,i) \cdot \text{prob}(U/R) \right\} dC dR \\ + \sum_j P'_j < 10^{-6} \quad \text{-----} \quad (1)$$

Where,

$P_i$  = initiating frequency of fault  $i$ , having a frequency greater than or equal to  $10^{-7}$  p.a.

$P'_j$  = initiating frequency of fault  $j$  having a probability smaller than  $10^{-7}$  p.a., against which no protection is claimed.

$\text{prob}(N/i)$  = probability of tripping on  $N$ th line of protection given fault has occurred.

$\text{prob}(M/N,i)$  = probability that  $M$  components fail in the shutdown system(s) given tripping on  $N$ th line of protection and fault  $i$ .

$\text{prob}(C/N,M,i)$  = probability of a given degree of cooling,  $C$ , following fault  $i$  and given an  $N$ th line trip with the particular  $M$  components failing in the shutdown system(s). This should be interpreted as a given degree of safeguards operation if operations in addition to cooling are required.

$\text{prob} (R/N, M, C, i)$  = probability of release R from fuel given fault i, with Nth line trip, M components failing in the shutdown systems and cooling C.

$\text{prob} (U/R)$  = probability of an uncontrolled release from the site given a release R from fuel following fault i etc. Due benefit can be taken for the effect of the pressure circuit barrier and containment.

#### 4. SIMPLIFICATION OF GENERAL EQUATION FOR DESIGN PURPOSES

In principle it would be possible to assess a reactor design against the general criteria as represented by equation 1. Depending on the proposed design, it may be possible to make simplifying pessimistic assumptions. The approach set down below includes certain assumptions which may not be appropriate for a particular design. Alternative approaches are not precluded providing system reliabilities are compatible with equation 1. It is also necessary that initiating fault frequencies used for system design meet the requirements set down in Section 5.

##### 4.1 Fuel and Plant Constraints

In order to get a significant release R from the reactor gross fuel failure has to occur. However, for design purposes it is convenient to adopt fuel limits sufficiently conservative that below the limits fuel behaviour can be predicted with confidence. Such limits need not necessarily preclude clad failure provided this is shown to be compatible with the requirements of Annex XIX (see Section 6 below). Similarly, limits on plant components should be conservatively defined. In practice, of course, exceeding such limits would not necessarily lead to an uncontrolled release of radioactivity. Thus, the probability of exceeding these design limits need not be kept as low as  $10^{-6}$ . Some degree of flexibility is permissible in meeting targets for not exceeding the design limits, especially for those cases where it can be shown that the containment provides an additional barrier to an uncontrolled release. Systems necessary to containment effectiveness must be shown to have an appropriate reliability.

However, in the analysis that follows,  $10^{-6}$  has been retained as a target for not exceeding the design basis, but it is emphasised that this does not preclude a more relaxed target being adopted.

##### 4.2 Incredible Initiating Faults

Faults  $P'_i$  can be regarded as the so-called "incredible" initiating faults. The Board's Health and Safety Department have agreed that a fault may be deemed "incredible" if inter-alia either adequate forewarning of the events which may lead to the accident can be guaranteed and adequate preventive

action can be demonstrated, or the probability can be proved to be less than 1 in  $10^7$  reactor years. A fault can also be regarded as "incredible" if it can be discounted by engineering judgement based on appropriate preventive measures.

All initiating faults which are claimed to be "incredible" shall be identified and the consequences of each fault, should it occur, shall be examined in sufficient detail to judge the likely outcome. Where it is practicable at an acceptable cost steps should be taken to ensure that, if the fault occurred, the consequences will be acceptable.

For the purposes of developing system reliability targets, "incredible" faults will now

be omitted since no meaningful value can be put to  $\sum_j P_j$

#### 4.3 Reliability targets for Systems Other Than Containment System

The essential systems other than containment systems, i.e. trip, shutdown and cooling, should, therefore, ensure, to a reliability now to be determined, that specified fuel and plant limits are not exceeded. It should be demonstrated, or argued, that, provided these limits are not exceeded the fuel and plant will remain in a safe, definable state. The reliability is given by,

$$\sum_i \sum_N \sum_M \int_C \left\{ P_i \text{prob}(N/i) \text{prob}(M/N,i) \text{prob}(C/N,M,i) \times \right. \\ \left. \text{prob}(\text{limits}/N,M,C,i) \right\} dC < 10^{-6} \text{ ----- (2)}$$

where,

$\text{prob}(\text{limits}/N,M,C,i)$  = probability of exceeding specified fuel or plant limits given in  $N,M,C,i$ .

Equation 2 may more conveniently be written,

$$\sum_i \left\{ P_i \sum_S \text{prob}(S/i) \text{prob}(\text{limits}/S,i) \right\} < 10^{-6} \text{ ----- (3)}$$

where  $\text{prob}(S/i)$  = probability of combination of Nth line tripping, M failures in shutdown systems given fault i

and,  $\text{prob}(\text{limits}/S,i) = \text{prob}(\text{limits}/N,M,C,i)$

Although it is possible to deal with equation (3) considering separately the various possible combinations  $S = S(C,N,M)$  it is desirable for design purposes to adopt a simplified approach. However, should this approach prove impracticable either as a whole or for certain limiting faults then the basic reliability target given by equation 2 may be applied directly.



Equation (3) may be simplified by noting, given a combination of tripping, shutdown and cooling  $S^* = S^*(N^*, M^*, C^*)$ , say, that for every combination,  $S$ , of tripping, shutdown and cooling which is less effective than  $S^*$  then.

$$\text{prob}(\text{limits}/S^*, i) \leq \text{prob}(\text{limits}/S, i) \leq 1$$

and for every combination,  $S$ , which is more effective than  $S^*$  then,

$$0 \leq \text{prob}(\text{limits}/S, i) \leq \text{prob}(\text{limits}/S^*, i)$$

Equation (3) may now be written, pessimistically,

$$\sum_i P_i (\text{prob}(S \leq S^*/i) + \text{prob}(\text{limits}/S^*, i)) \leq 10^{-6} \text{ ----- (4)}$$

where,

$\text{prob}(S \leq S^*/i)$  = probability that combination of systems  $S$  is less effective than combination  $S^*$ ,

assuming that  $\text{prob}(S^* \leq S/i) \approx 1$

Further simplification may be achieved by noting that  $S$  can only be less effective than  $S^*$  if any one or any combination of the following apply:-

$$(i) \quad N > N^*$$

$$(ii) \quad M > M^*$$

$$\text{or } (iii) \quad C < C^*$$

Let  $f_T$  =  $\text{prob}(N > N^*)$ , the failure probability to sense fault and trip guard lines.

$f_R$  =  $\text{prob}(M > M^*)$ , the failure probability to insert sufficient reactivity.

$f_C$  =  $\text{prob}(C < C^*)$ , the failure probability to cool following reactor shutdown.

Then equation (4) reduces to,

$$\sum_i P_i (f_{T_i} + f_{R_i} + f_{C_i}) + \sum_i P_i \text{prob}(\text{limits}/S^*, i) \leq 10^{-6} \text{ --- (5)}$$

ignoring terms such as  $(f_{T_i} f_{R_i})$  etc.

The objective, therefore, becomes one of choosing, for each fault, a combination of tripping, shutdown and cooling,  $S^*$ , such that the probability of not having a combination as good as  $S^*$  satisfies equation 5.

It will be appreciated that in order to arrive at values of  $f_{T_1}$ ,  $f_{R_1}$ ,  $f_{C_1}$ , which satisfy equation (5) the

minimum system response will involve a combination of second line tripping; minimum reactivity take up; and minimum cooling response.

Ideally each term in the L.H.S. of equation (5) would have equal value. However, it is proposed that for purposes of system design

$$\text{prob}(\text{limits}/S^*, i) \ll (f_{T_1} + f_{R_1} + f_{C_1})$$

so that we only require,

$$\sum_i P_i (f_{T_1} + f_{R_1} + f_{C_1}) \ll 10^{-6} \text{ ----- (6)}$$

The application of equation (6) to system design is discussed in Section 5.

Dependent on the probability of the initiating fault, it may be necessary to show protection against a systematic or common mode failure of similar components. Possible approaches to common mode failure in the shutdown system(s) are considered in Annex VIII. The use of inherent reactor characteristics to promote shutdown may impose requirements on the post trip safety related systems different, or additional, to those where the shutdown system operates. The reliability with which these requirements are met should be such that the total approach is in accord with the fundamental target given by equation 2.

#### 4.4 Reliability targets for Containment Systems

The systems required for containment effectiveness (eg. cooling, isolation) shall have a reliability compatible with the reliability targets described in section 2.

### 5. FAULT CLASSIFICATION AND DERIVATION OF INDIVIDUAL REQUIREMENTS

Faults may be grouped in various ways, and systems considered separately. However, in defining the post trip cooling requirements the transient analysis should be carried out using the minimum requirements assumed in the reliability assessment of the tripping and shutdown systems (e.g. 2nd line tripping and minimum reactivity insertion).



The fault classification shown in table V-1 , detailed more fully in Annex IX, is an example of that which could be adopted for the first design iteration. Other classifications are not precluded. Also included are suggested permissible failure probabilities  $f_{T_i}$ ,  $f_{R_i}$ ,  $f_{C_i}$ .

#### Initiating Fault Frequencies

To be certain that the design of post-trip essential systems will be adequate it is important to ensure that the values used for initiating fault frequencies are not optimistic.

The attached table sets down for certain categories, proposed minimum claimable total frequencies for purposes of system design. It is considered that the frequency of faults in these categories is unlikely to be strongly influenced by reactor design.

For categories where frequencies are not specified, the designer should present justification of the frequencies to be used in system design to the Engineer at the initial stage of design development. An overriding requirement which should, however, be met is that following any single credible initiating fault the probability of failure to adequately shut down and cool is compatible with the overall requirements and in line with good engineering practice.

Table V-1

## Example of fault classification scheme

Fault Classification $i$	Minimum claimable total frequency for purposes of system design, $P_i$ (per reactor) (p.a.)	Corresponding max. permissible system unreliability			$P_i(f_{T_i} + f_{R_i} + f_{C_i})$
		$f_{T_i}$	$f_{R_i}$	$f_{C_i}$	
A. Spurious reactor shutdown/guard line trip	10	-	See note below	$10^{-8}$	$10^{-7}$
B. All pressurised faults which do not affect integrity of essential systems	1	$10^{-7}$	$10^{-7}$	$10^{-7}$	$3 \times 10^{-7}$
C. Loss of Grid supply which initiates a trip	See Annex IX	$10^{-7}$	$10^{-7}$	See Annex IX	$10^{-7}$
D. Small LOCA	)	)	)	)	$10^{-7}$
E. Large LOCA	)To be specified by the designer	)To be established on the basis of the designer's fault frequencies	)	)	$10^{-7}$
F. Faults originating within an essential system	)	)	)	)	$10^{-7}$
G. Internal hazards	)	)	)	)	$10^{-7}$
H. External hazards	-	As specified in Annex III			-

$$\sum_i P_i (f_{T_i} + f_{R_i} + f_{C_i}) < 10^{-6}$$

Note on Table

The table above assumes that no reactivity insertion is necessary following a guard line trip. If this is not the case - e.g. if a spurious signal also initiates certain post trip actions which require a reactor shutdown - then the permissible reactivity insertion failure probability could become  $10^{-8}$ .

5.1 Confidence Levels for Transient Calculations

If for a given fault the system unreliability

$(f_{T_1} + f_{R_1} + f_{C_1})$  is F, say,

then the probability of the postulated fuel and plant limits being exceeded when the systems are deemed to have worked must be of a similar order of magnitude.

It is recognised however, that methods have not been developed for performing such calculations. Instead, in order to achieve this objective, calculations should be performed using current practices of worst bound data and appropriately pessimistic assumptions to be agreed with the Engineer.

It is required that all modelling assumptions in fault analyses are systematically examined against all available experimental and theoretical data with the intent of developing a demonstrably conservative calculational route.

In addition, sensitivity studies shall be carried out for each part of the calculational model to establish that the simulation of plant in the computer codes, nodal representation and timestepping and the methods of linking codes are sufficiently well developed and understood to give confidence that the definitive calculational route is conservative.

Sensitivity studies are also required to identify dominant assumptions both in input data and plant and component response and to support the conservatism of the assumptions in the definitive approach. The aim should be to demonstrate that, should the assumptions be incorrect, the consequences are acceptable.

6. ADDITIONAL RADIOLOGICAL REQUIREMENTS

The general requirements derived in section 3 have been based only on the need to avoid an uncontrolled release. Although this is a necessary condition, it is not a sufficient one for defining successful system operation. Annex XIX defines other requirements which should also be met.

For those faults not involving a breach of the primary pressure circuit these criteria are unlikely to significantly affect system design (even although, for frequent faults, permissible releases to the environment will be small).

Reactor Safety System

CONTENTS

1. GENERAL
2. PERFORMANCE
3. ACCESS AND MAINTENANCE

1. GENERAL

- 1.1 A safety system shall be provided which shall be designed to prevent conditions arising which would seriously damage the reactor plant and/or cause a hazard to the public or personnel.
- 1.2 The safety system shall be engineered to meet the detailed requirements of Annex VII. It shall be an independent system and entirely automatic in operation.

2. PERFORMANCE

- 2.1 The safety system shall be designed and constructed throughout to the highest engineering standards and integrity of operation bearing in mind the importance of the functions to be carried out. Particular regard should be made to the principles of diversity and segregation as described in Annex VII.
- 2.2 In principle only the general requirement of Annex V need be met but, unless it is shown to be impracticable, the safety system should meet the following criterion:

$$f_T \ll 10^{-7}$$

where  $f_T$  is the peak value of probability of failure of the safety system to initiate a shut down on demand (excluding maintenance etc. - see 2.3 below).

No single line of protection should have a probability of failure of worse than  $10^{-3}$  per demand.

A detailed theoretical analysis shall be presented during the design stage to substantiate in detail that the criterion has been met. The reliability data used in this analysis shall be agreed in advance with the Board.

- 2.3 Taking into account maintenance, the removal of equipment for test, the application of vetos and other factors which may cause temporarily reduced integrity, the instantaneous value of  $f_T$  should at no time be increased by more than a factor of 10 greater than the value required in 2.2 and then for no more than 2% of the total maintenance interval.
- 2.4 The probability of the safety system causing restriction in station operation (allowance being made for maintenance and testing) should be less than 0.1 per annum.



3. ACCESS AND MAINTENANCE

- 3.1 No routine access to the containment should be necessary for safety system checking except at fuelling intervals. Access may be permitted for simple maintenance procedures.
- 3.2 All equipment, including sensors, shall be testable with the plant on load or shutdown.
- 3.3 The mounting of components within the containment shall be such as to minimise any maintenance time, radiation dose and risk to maintenance staff.

Specification for Reactor Safety Systems

CONTENTS

1. SCOPE
2. DEFINITIONS
3. SYSTEM DESIGN PRINCIPLES
  - 3.1 Introduction
  - 3.2 General
  - 3.3 Rules for System Calculations
4. SYSTEM REQUIREMENTS
  - 4.1 General
  - 4.2 Guard Lines
  - 4.3 Power Supplies
  - 4.4 Alarms
5. EQUIPMENT REQUIREMENTS
  - 5.1 General
  - 5.2 Cabling
  - 5.3 Cubicles and cubicle wiring
  - 5.4 Sensors
  - 5.5 Relays and Contactors
  - 5.6 Solid State Devices

## 1. SCOPE

1.1 It should be particularly noted that this specification applies to all the equipment provided to prevent conditions arising which could seriously damage the reactor fuel and/or cause a hazard to the public or personnel: it extends from the sensors to the electrical terminals of the final plant items involved, e.g. control rod clutch terminals or trip solenoid terminals, and includes monitoring devices essential to ensure the correct operation of the reactor shutdown systems. Where emergency cooling services need to be initiated from reactor parameters, the initiating circuits shall comply with this Specification. Engineered Safety Features Actuation Systems shall also comply with this specification.

1.2 This specification is not intended to be exhaustive, but is complementary to the following specifications:

US 76/10\* Instruments and Control Equipment General Technical Requirements.

US 12/50\* General Technical Requirements for Ancillary Electrical Equipment.

Electronic equipment specification EES (1980).

I.E.C. Publication 231, 231A, 231D.

B.S. 4877: 1972.

\* Issue numbers pertaining to the particular power station.

The equipment supplied shall comply with the above specifications, unless these are specifically overruled by the requirements of this specification.

## 2. DEFINITIONS

### Safety System

All equipment provided to meet Section 1 from the sensing devices to the electrical power terminals of the final items of plant concerned.

### Safety Channel (or Safety Monitoring Assembly)

All equipment associated with a single measurement of any parameter required for the safety system including all necessary sensors, cabling and electronic equipment.

### Safety Trip Group

A group of identical safety channels measuring the same parameter arranged to feed reactor trip signals into the guard lines, e.g. rate of change of pressure trip.

Shutdown System

The equipment used to produce a sub-critical condition in the reactor when required by the guard line (e.g. control rods).

Safety Initiator Group

A group of safety channels arranged to initiate an emergency service required to prevent or minimise conditions defined in Section 1, e.g. start emergency generators, circulators or feed system.

Safety Interlock Group

An interlock consisting of a group of safety channels to prevent conditions defined in Section 1 arising.

Guard Line (or Safety Line)

The physical equipment used to assemble the logic of several safety trip groups to produce a reactor trip actuation.

Demand

The requirement of the safety system to perform an action, e.g. trip reactor, to prevent unsafe action or operation, initiate emergency cooling.

Incorrect Operation

The inability of the system to meet a demand.

Restriction in Station Operation

Inability to operate the station at the designed, permitted and safe output power due to a cause arising in the safety system, e.g. reactor trip, control rod withdrawal, interlock applied.

3. SYSTEM DESIGN PRINCIPLES3.1 Introduction

All credible faults on the reactor unit and associated plant which can cause fuel damage or a personnel hazard shall be listed in a schedule.

Each fault shall be protected against to the standard specified in Annex VI either by the provision of safety channels to interlock against the condition or to trip the reactor or a combination of both.

The protection achieved against each fault shall be calculated in accordance with Section 3.3 of this specification.

In the same manner the probability of the complete safety system causing a restriction in station operation, due allowance being made for maintenance and testing, shall be shown to meet the requirement of Annex VI.

### 3.2 General

- 3.2.1 Unless otherwise agreed, the safety system shall be exclusively for this purpose, and shall be independent of all other systems and shall not require operator action for effective operation.
- 3.2.2 The design of the complete system including power supplies shall be such that any two independent concurrent faults in the system shall not prevent the correct operation of the system and no single fault shall restrict the station operation. Connection together of any two conductors within a cubicle or common cable run shall be considered as one fault.
- 3.2.3 Unless otherwise agreed the safety system shall be actuated for each demand by two different physical parameters via channels of different design.

### 3.3 Rules for System Calculations

Probabilities of incorrect operation of the safety system and restriction in station operation should be met by calculation using the following rules.

- (a) Assume all equipment is set up in rotation at 0.25 year intervals.
- (b) An unrevealed unsafe failure would exist until the next maintenance.
- (c) Any failure brought to the operators attention by a persistent alarm in the M.C.R. will be repaired in 5 hours: allowance must be made for the reliability of the alarm system.
- (d) Each channel will be considered to be in an unsafe failed condition for 1 hour whilst being repaired or checked as in (a) above.
- (e) The failure rate of each item of equipment shall be established either by:
  - (i) Observation to 95%, single sided, confidence level on identical equipment under similar operating conditions.
  - (ii) Calculated from component data established to a 95% single sided, confidence level under similar conditions, the source of data to be previously agreed with the Engineer.

Except that:

- (iii) No single safety channel shall be regarded as having a fail-danger rate better than 0.1% per 1,000 hours.
- (iv) Failed danger rates for components lower than the following shall not be used:

Laddic unit 0.01% per 1,000 hours.

Safety relay/contactors (per contact) 0.01% per 1,000 hours.

Inverter 0.01% per 1,000 hours.

Limit Switches 0.1% per 1,000 hours.

Pressure switches 0.3% per 1,000 hours.

- (f) Due allowances shall be made in the reliability calculations for each system or sub-system for the risk of common-mode failures; the CMF limit to claimed reliability for each system or sub-subsystem shall be agreed with the Board.

- (g) The probability of incorrect setting of equipment during maintenance should be taken as  $10^{-3}$  per setting.

#### 4. SYSTEM REQUIREMENTS

##### 4.1 General

- 4.1.1 Segregation of the safety system shall be such that no credible internal or external hazard shall result in its incorrect operation.
- 4.1.2 As far as is practicable all equipment shall be in the safety equipment rooms.  
  
All safety equipment shall be housed in suitably segregated cubicles which shall, with the exception of power supplied, be locked by a unique key system.
- 4.1.3 The key locking system should permit the maximum access for maintenance at any one time; the only limitation being that it shall not be possible to cause an unsafe condition, nor produce a reactor trip, by the access permitted at any one time.
- 4.1.4 Due allowance shall be made in safety-room layout and guard-line cubicle layout for possible safety system extensions up to 20%.
- 4.1.5 Maintenance shall be possible on every item of equipment with the system in operation and without the use of veto facilities. The time taken to check correct operation of the whole system shall be minimised by the provision of adequate installed test equipment and facilities.



- 4.1.6 The safety system test equipment should enable one man in the safety room area to check and calibrate all complete safety channels from the open fronts of the cubicles and check all logic circuits with the system in operation and the reactor at power or shut-down. The system shall not permit testing of more than one channel of a group at a time. The test gear may be trolley mounted or installed. Facilities shall be provided for response time testing of sensors and equipment where necessary.
- 4.1.7 The system should be designed to eliminate the operational adjustment of trip/interlock parameters by the operator; where unavoidable the controls shall be on the reactor unit desk and excess margin trips shall be fitted.
- 4.1.8 The system shall be designed as far as possible to obviate the need for manual operational veto arrangements. Where unavoidable they shall be actuated in the C.C.R. by suitable locked switches separately alarmed to show discrepancy between switch position and plant state. Operation should not cause any significant delay to plant operating procedures. The operational vetoes shall be interlocked to prevent an unsafe reactor condition arising.
- 4.1.9 All position and level signals shall be obtained directly from the functions being monitored by a system unique to the reactor safety system and shall not be derived by inference from measurement of a different parameter. Recorder contacts or contacts derived from indicating devices shall not be used for reactor safety purposes.
- 4.1.10 Facilities shall be provided to allow the operator to manually trip the reactor. Where two or more modes of trip are available separate facilities shall be provided for each mode, with clear and unambiguous indication to the operator as to which mode is controlled by which switch. Only one facility will be regarded as the emergency trip, and the facility so designated will be clearly identified. The manual trip facilities shall be provided on the reactor unit desk, tripping as close as possible to the control rod release circuits and breaking the circuit at 2 points. The manual trip shall only be reset by the use of a key. Push-buttons must have a positive 'follow through' to permit correct operation with broken springs.
- 4.1.11 A direct telephone facility shall be provided between all locations at which safety system equipment is installed. The facility may take the form of suitable outlets for self-powered hand sets.

An adequate number of hand sets shall be provided for use with this telephone facility.

- 4.1.12 The use of relays shall be avoided where possible for all primary safety system applications other than alarms and interlocks, except that subsidiary inputs such as unit faults (e.g. E.H.T. failure in the S.D.A.s) may be included as relay contacts in series with the laddic hold current generated by the main parameter trip function.
- 4.1.13 Where two safety interlock groups are claimed against the same fault they shall be of diverse design and be subject to specific approval by the Board.
- 4.1.14 Units which provide a rate of change trip shall be designed to lock out on a trip, with manual reset facilities being provided on the front of the unit.

#### 4.2 Guard Lines

- 4.2.1 All primary guard line logic shall be performed without the use of interposing relays in the guard lines or safety channels by solid state elements of established and repeatable performance except as provided for in 4.1.12 above. The laddic element is preferred and is available from the C.E.G.B.

Alternative systems may be considered by the Board on presentation of full supporting evidence.

- 4.2.2 The guard lines shall be entirely within the safety system equipment rooms.
- 4.2.3 The safety trip channels and guard lines shall be arranged such that all guard lines operate when any combination of the minimum number of safety channels required to produce a trip operates.
- 4.2.4 Each guard line shall lock out when operated and only be reset manually, without the use of keys, from the safety equipment rooms.
- 4.2.5 The guard line system when operated shall cause all required reactor shutdown systems to operate. Each shutdown system operation shall be initiated by two distinct breaks using different equipment. Where electromechanical circuit interruption is used, different contact materials should be employed for each break (see 5.5.5).
- 4.2.6 Only sufficient delays shall be incorporated into the guard line end circuits to prevent spurious tripping from safety system internal causes such as surges.
- 4.2.7 The guard line end logic system and shutdown system trip circuits shall be fitted with an earth fault detection system for use during periodic testing.

#### 4.3 Power Supplies

- 4.3.1 Sufficient independent "no break" power supplies shall be provided to meet the requirements of Section 3.2. A further identical standby supply is required together with a facility for interconnecting to a further standby supply.
- 4.3.2 The range of voltage and frequency of the no break supplies, measured at the equipment terminals, shall not exceed +3% and +1% respectively over all load and battery conditions.
- 4.3.3 The regulation system and filtering devices shall be such that transients and electrical interference cannot actuate or prevent correct operation of the safety system.
- 4.3.4 The supplies shall be monitored so that an alarm is initiated for voltage or frequency errors of +7% and +3% respectively.

#### 4.4 Alarms

- 4.4.1 The final action of the safety system shall be indicated via prominent alarms independent of the D.P.S. In addition mimic panels shall be provided in the main control room and the safety rooms to indicate the state of the guard lines, individual trip units (including trip approach and equipment fault alarms), safety interlocks and operational vetoes.

Alarms shall be provided in the central control room, via the data processing system, to indicate the state of each safety channel and guard line, to automatically record changes and to enable the cause of safety system operation to be determined.

- 4.4.2 Where a trip function is vetoed its associated alarm shall also be vetoed except where it will perform a useful function.
- 4.4.3 If an alarm has direct safety significance it shall be of fail safe design.
- 4.4.4 In addition to the alarms specified above, sufficient alarms shall be provided in the safety system equipment rooms to enable all equipment faults to be located quickly.
- 4.4.5 The safety system equipment indicator panel in the safety system equipment rooms shall be located so that it is in view while carrying out maintenance on all cubicles; an alarm bell shall be fitted.
- 4.4.6 All supplies to the safety system and to the safety system alarms shall be monitored by a reliable system and an alarm raised in the C.C.R. in the case of failure.
- 4.4.7 All alarms indicating the state of a safety channel shall operate concurrently with the main output logic signal.

- 4.4.8 Alarms shall be provided to remind the operator of any action required in the safety system, e.g. remove E.H.T. from low power detectors.
- 4.4.9 Where an operational veto is unavoidable the fact that a veto is applied shall be alarmed individually to the operator in the C.C.R.
- 4.4.10 A facility shall be provided on every safety channel to enable all its alarms to be vetoed during maintenance. A separate alarm in the control room shall indicate that the facility is in use.
- 4.4.11 Every trip/interlock function on a continuously variable parameter shall have an associated approach alarm provided if corrective action can be taken by the operator.
- 4.4.12 Alarms shall be provided in the main control room and safety rooms to indicate the removal of a unit or module from its operating position.
- 4.4.13 Where routine testing is necessary at locations remote from the safety rooms, indicator lamps shall be provided at these locations to show the state of trip units in the appropriate trip group.

## 5. EQUIPMENT REQUIREMENTS

### 5.1 General

- 5.1.1 All items of safety equipment shall be of fail-safe design to individual approval. The designs shall be the simplest and most reliable consistent with the fail-safe requirement and shall either have been proved in similar service or be subjected to thorough type-testing. The equipment should not require adjustment for 0.25 year periods.

The Board reserve the right to undertake independent tests on contract equipment during the contract. The Contractor shall co-operate with the Board in carrying out such tests.

For equipment mounted in plant areas outside the safety room, the design temperature and humidity ranges and the type-test requirements shall be individually agreed.

- 5.1.2 All safety equipment components or sub-assemblies shall operate within specification for any combination of:

Temperature	0 to 55°C
Relative Humidity	0 to 95%
Supply Voltage	+ 10% nominal
Voltage Step Change	+ 10% within band
Supply Frequency	+ 5% nominal
Total Harmonic Voltage Distortion	5% (10% for new designs)

Type tests shall be carried out to Class B3 of EES (1980) but a damp heat test is required. Tests shall be carried out at the following conditions:

Dry heat - 55°C, Low temperature - 0°C

Damp heat - 40°C 95% R.H.

- 5.1.3 All components used in the safety system shall be professional quality standard items with readily available equivalents unless otherwise agreed. The requirements of EES (1980) for components should be noted.
- 5.1.4 The equipment shall be capable of withstanding radio transmissions producing a field strength of 10V/M and covering a frequency range of 20 to 500 MHZ without deviating from the agreed performance limits for the equipment. For the test procedure to check for equipment susceptibility to R.F.I. reference must be made to the Engineer.
- 5.1.5 All channels used in the safety system shall be designed so that trip and alarm settings can be secured in a set position. If it is necessary to impose a fixed maximum setting on any device, which normally operates at a point below this maximum setting and on which facilities for day-to-day adjustment are required, the maximum setting shall be fixed by means of pre-set control, separate from the facility for day-to-day adjustment.
- 5.1.6 All means of adjustment for detectors and monitoring assemblies used in the safety system shall be enclosed within cubicles, locked in accordance with the safety line locking system requirements. Controls used for any adjustment shall be accessible from the front of the cubicle when the appropriate access door is unlocked.
- 5.1.7 On all items of plant, e.g. circuit breakers, auxiliary switches, terminal blocks, plugs and sockets, there shall be complete segregation of the safety system equipment from all other equipment; different safety channels shall also be segregated.
- 5.1.8 All relays including those for alarm use within the safety equipment shall be fitted with adequate arc suppression devices. The method chosen should ensure high reliability and be such that failures are 'fail safe'.  
  
All contacts should nevertheless be rated for use without the suppression device fitted.
- 5.1.9 Plug-in apparatus shall be so arranged that only the correct items of equipment can be mounted in the appropriate position.
- 5.1.10 Plugs and sockets shall be so designed that it is impossible to insert a plug into an incorrect socket.



- 5.1.11 Where a plug and socket is used to make connections within the safety system the following rules shall apply:
- (a) Separate plugs and sockets shall be provided for power supply and trip and alarm circuits.
  - (b) Where leakage between 2 leads could be dangerous the leads shall not be connected to adjacent pins but segregated to the approval of the Board.
- 5.1.12 The earth connection to individual items of equipment shall be arranged so that continuity is maintained when any item is removed from its mounting position.
- 5.1.13 Where a plant contact is being monitored for use in a safety system the go and return leads shall be separated by earthed screens.
- 5.1.14 Connectors for printed circuits should where possible, use separate board-mounted connectors and shall be to Board approval. Where edge connectors are used they must comply with EES (1980).
- 5.1.15 Facilities shall be provided for testing of multiple contact hammocks without requiring the system to be tripped.

## 5.2 Cabling

- 5.2.1 All safety system cabling shall be segregated from all other cabling; the cables of one guard line or group of safety channels shall be so segregated from the cabling of others that no single hazard, e.g. fire, flood, severance, etc., shall result in incorrect operation of the safety system.
- 5.2.2 All safety trip system cabling shall be segregated from all other cabling through the use of earthed armouring (or earthed metal conduit or trunking to the Board's specific approval) in conjunction with the following minimum requirements:
- (i) Between safety trip system cabling and power cabling/earthing strip - 600mm separation distance.
  - (ii) Between safety trip system cabling bearing very low signal levels, e.g. neutron flux measurement signals etc, and control cabling - 300mm separation distance.
  - (iii) Between safety channels within the same trip group, between guard lines, and between safety groups where diversity is claimed for safety - where possible 2 M separation distance plus one hour fire protection enclosure.

- (iv) As a safeguard against the occurrence of any possible incident leading to an unprotected reactor situation due to its affecting more than 2 guard lines or safety channels in a 2004 system, then Class I segregation (external and internal incident proof enclosure) shall be provided between two groups of 2 guard lines or safety channels.

- 5.2.3 All cabling associated with the safety system shall be in accordance with the electrical section of the main Enquiry Specification except where conflicting with this specification. All cables shall be subject to individual approval with regard to type, routing and method of running.
- 5.2.4 All safety system cabling external to cubicles shall be carried out in cable having multi-strand conductors of minimum cross-section 0.75 sq. mm except for conductors carrying thermocouple or neutron flux instrument signals which shall be to the Board's specific and individual approval.
- 5.2.5 All power supply cables shall be protected by fuses rated at not more than the cable rating.
- 5.2.6 All safety system cabling shall be marked on each core at each termination with an orange ferrule in addition to other identifying symbols. All such cables shall have orange sheaths. Cable runs shall be identified by orange bands at not more than 1 metre intervals. This requirement includes:
- (a) Thermocouple cabling from marshalling cubicles to the safety system equipment rooms.
  - (b) Shutdown system final circuits.
  - (c) Electrical Supplies
- 5.2.7 Separate screened cables shall be provided for the shutdown system trip signals.

### 5.3 Cubicles and Cubicle Wiring

- 5.3.1 The cubicles shall be arranged so that the equipment mounted therein is kept within its temperature operating limits without the use of individual ventilating fans for each cubicle. The cubicles shall be designed such that with an external ambient temperature of 40°C the cubicle internal ambient does not exceed 50°C.
- 5.3.2 Instruments shall be grouped logically by function in cubicles. Vertical segregation is preferred. Guard lines shall be contained in mechanically separate enclosed compartments or cubicles with separate access.
- 5.3.3 Apparatus shall be laid out in cubicles in such a manner that testing, adjustment and removal of individual items of equipment can be carried out without disturbing other equipment or cabling. It is preferred that no equipment should be mounted on the sides of cubicles



- 5.3.4 All equipment in the safety system shall be mounted behind doors locked in accordance with Section 4.1. Glass or similar quality panels shall be provided in doors enclosing equipment carrying meter scales, controls or indicators to enable these to be read without opening the doors.
- 5.3.5 All cubicles and housings shall be clearly and unambiguously labelled with their function and the reactor with which they are associated. All equipment within cubicles shall be clearly labelled and its function and circuit reference. The mounting position and equipment shall both be labelled where the equipment is removable.
- 5.3.6 All cable entries into cubicles, apparatus boxes etc. shall be dust and moisture proof. Cable glands and cable clamps of the Board's approved pattern shall be used.
- 5.3.7 Cables and cable forms shall be terminated in such a manner that the cable, cable form and terminal are under no mechanical stress.
- 5.3.8 All terminals shall be shrouded, irrespective of voltage.
- 5.3.9 All terminations and terminal blocks shall be subject to specific and individual approval. Terminals which if they become electrically connected together would inhibit any part of the safety system, shall have special provision made to ensure that these terminals shall remain electrically separate during all ambient operating conditions for the life of the station. This provision shall be subject to the specific approval of the Board.
- 5.3.10 Terminations shall be grouped in terminal blocks according to functions. Barriers shall be used between groups of terminations associated with separate functions.
- Terminal arrangements shall be such that the requirements for external cabling set out in Section 5.2 are met.
- 5.3.11 Internal wiring within cubicles should, where possible, be carried out in 24/0.20mm PVC insulated cable to B.S. 6231: 1969, type B insulation or to DEF 61-12 (Part 6). All wiring within safety cubicles should be of flame resistant type.
- 5.3.12 Separate cable forms shall be made within cubicles for:
- (a) Sensor input signals.
  - (b) Trip circuits.
  - (c) Alarm circuits.
  - (d) Power supply circuits.

5.3.13 The following minimum spacing shall be provided between cable forms:

- (a) Between separate channel or guard line forms - 15cms.
- (b) Between safety channel and other cable forms - 5cms.
- (c) Between power supply and other cable forms - 5cms.
- (d) Between power supply cable forms - 5cms.

In lieu of the above spacings an earthed metal barrier may be used to segregate cable forms.

5.3.14 All wires shall be terminated with approved claw washers or crimped tags in approved terminal blocks.

5.3.15 Thermocouple cables shall be run directly from the marshalling cubicles to the cubicle which contains the equipment into which their signals are to be fed.

The flexible tails connecting to the equipment shall be replaceable.

All thermocouple cables used for safety purposes shall be marked in orange in the marshalling cubicles.

#### 5.4 Sensors

5.4.1 All sensors which feed signals into the safety system shall be unique to this function and operate from separate measurement points. The application of flux measuring equipment may be considered separately, subject to specific approval. Sensors used for safety purposes shall not be used for control purposes or for indication. Where signals are fed into the safety system from auxiliary contacts and other items of plant, e.g. gas valve limit switches, circuit breaker auxiliary switches, the contacts used shall be separate from those used by other functions, and separate auxiliary switches shall be provided exclusively for use in the safety system.

5.4.2 Where a failed sensor cannot be replaced within approximately 5 hours with the reactor at power an installed spare or alternative sensor shall be provided. Spare neutron flux detectors shall be provided, as detailed in the flux measuring specification.

5.4.3 Cables and connectors for sensors shall be subject to individual approval.

5.4.4 All necessary test facilities shall be provided at sensors (e.g. test valves, tappings, pressure supplies).

- 5.4.5 Where necessary, plant mounted sensors shall be protected against potential environmental hazards, e.g. gas or liquid at temperature or pressure, to the Board's approval.

## 5.5 Relays and Contactors

- 5.5.1 Relay and contactor contacts shall be protected from the effects of fault currents, which could cause welding. This protection may take the form of fuses or series resistors depending on the contact size and material.

If fuses are used type tests shall be carried out to demonstrate the protection. If resistors are used the fault current should be limited to less than half the rated contact current or one quarter the contact limit current, whichever is lower.

Any series resistors shall be of an approved type and shall be mounted as close to the contacts that they protect as possible.

- 5.5.2 All relays shall be fitted with separate transparent, flame retardent dust covers.

Plug in relays and contactors shall be oriented by duty and non-interchangeable with those of different duty.

- 5.5.3 All relays shall comply with B.S. 142: 1966. "Specification for Electrical Protective Relays".

Contactors shall comply with the requirements of B.S. 5424 Part 1 except as qualified below.

- 5.5.4 All relays and contactors for safety purposes shall be subject to specific and individual approval.

The following specific requirements shall be met by all relays and contactors.

- (a) Relays and contactors shall be designed for continuous energised operation at 120% of rated voltage.

The temperature rise of the coil, measured by the self-resistance method shall not exceed the values in the following table:

<u>Class of Insulation</u> <u>(B.S. 2757)</u>	<u>Maximum Coil</u> <u>Temperature Rise</u>
A	30°C
E	45°C
B	55°C

Temperature rises greater than 55°C are not acceptable.

- (b) Relays shall have the following operating characteristics:

Test Operate	- 75% of nominal voltage
Test Non-Operate	- 40% of nominal voltage
Test Hold	- 37% of nominal voltage
Test Release	- 10% of nominal voltage or where this voltage leads to a coil current of less than 2 mA the voltage appropriate to a coil current of 2 mA shall be used.

- (c) The coil impregnation shall be non-migratory.

- (d) Any remanence pin fitted shall be non-adjustable.

- (e) Relays and contactors shall withstand a 2 kV test voltage between contacts and all other metal parts of the relay which are insulated therefrom, and between coil connections and earth. For equipment designed to operate at 50V, the above test voltage may be reduced to 500V.

- 5.5.5 The preferred contact materials for relays are either one contact silver and the other graphite or silver graphite, or both contacts silver cadmium oxide. Consideration will be given to other materials with a high inherent resistance to welding.

For some low current applications the use of Post Office K3000 relays is acceptable provided that the contact material is either platinum or palladium.

#### 5.5.6 Specific Requirements for Contactors

- (a) The preferred contact materials are either one contact silver and the other graphite or silver-graphite, or both contacts silver cadmium oxide.

If silver cadmium oxide contacts are provided the mechanism of the contactors shall ensure that the contacts close with a definite wipe and roll action.

- (b) Arc chutes and magnetic blow-out action shall be provided.
- (c) There shall be two independent means of opening the contacts when the contactor is released.
- (d) Contactors with graphite or silver-graphite contacts need not be overload tested in accordance with B.S. 5424 Part 1. A test schedule based on the load carried will be agreed at the submission stage.

## 5.6 Solid State Devices

### 5.6.1 Laddic System:

The detailed system proposed shall be by agreement between the Board and the Contractor. The following shall be noted;

- (a) The laddic module shall be encapsulated by specific approval only.
- (b) All windings shall be isolated from earth.
- (c) An earth fault detection system shall be provided for use during periodic testing.
- (d) Means shall be provided for testing logic without removing leads.
- (e) All safety channels feeding the laddic shall give direct electrical outputs, one for each guard line. The outputs may be taken by a single plug and socket, but open or short circuits on one output should not effect the others by more than 20%.
- (f) Where a hold winding is fed from a source outside the safety room a static interposing device shall be provided in the safety room to give electrical isolation.
- (g) No winding shall be operated from a source at greater than 15 volts above earth.
- (h) Veto signals, where applied by relays, shall be subject to specific approval by the Board.

### 5.6.2 Semiconductor Devices:

- (a) Any MOS devices shall have input protection circuitry provided to prevent failure due to statically-induced electrical charges. Any circuit card incorporating an MOS device shall have a suitable warning incorporated into the card.
- (b) Reliability data for integrated circuits shall be subject to specific approval.
- (c) No specially designed integrated circuits (e.g. "Custom built" large scale integration) will be accepted.
- (d) The use of plugged-in integrated circuits is not permitted; all components shall be soldered-in.
- (e) Plastic encapsulated integrated circuits and transistors shall be subject to individual approval.

Reactor Shutdown Requirements



CONTENTS

1. INTRODUCTION
2. FUNCTION OF SHUTDOWN SYSTEMS
3. DIVERSITY REQUIREMENTS
4. RELIABILITY REQUIREMENTS
  - 4.1 Calculation of Reliabilities
5. OPERATOR ACTIONS
6. REACTIVITY SHUTDOWN CAPABILITY
7. SHUTDOWN FAULTS
8. TESTING
9. ADDITIONAL REQUIREMENTS

1. INTRODUCTION

This specification applies only to reactivity insertion systems termed shutdown systems. It excludes the requirements of the safety system and sensors which are covered in Annexes VI and VII. It includes any devices (e.g. valves) whose operation is initiated by the safety system.

2. FUNCTION OF SHUTDOWN SYSTEMS

Following any credible transient or incident, sufficient reactivity shall be taken up to terminate the transient and to leave the reactor in a safe shutdown state so as to prevent any fuel or plant limitations being exceeded.

Sufficient reactivity shall also be capable of being taken up to adequately shut the reactor down in the long term to a cold state. Ideally the reactor should stay shutdown even if loss of cooling occurs. The presence of the shutdown systems and their modes of operation shall not jeopardise the safety of the plant.

3. DIVERSITY REQUIREMENTS

The possibility of a common mode or systematic failure affecting similar components in the shutdown systems shall be considered and taken into account where necessary in plant design. As an overriding limit, the possibility of such a failure shall not be assumed to be less than  $10^{-5}$  failures per demand. Both short and long term shutdown shall be considered.

The designer shall identify those faults or fault sequences which have a sufficient frequency to require protection against common mode failure.

For each such fault either:

A Two or more diverse shutdown systems shall be provided each individually capable of ensuring that any release will meet the requirements of Annex XIX.

or B it shall be shown that inherent reactor characteristics are sufficiently effective that the activity release requirements are met despite the common mode failure of the shutdown system. In this case, the provision of a single shutdown system would be deemed adequate.

4. RELIABILITY REQUIREMENTS

The basic reliability requirements are given in Annex V.

4.1 Calculation of Reliabilities

1. The method of calculating reliabilities shall be agreed with the Engineer.
2. The reliability requirements should be met at all times including during maintenance and testing.
3. Only components of proven reliability shall be used unless otherwise agreed with the Engineer. Data shall be agreed with the Engineer.

5. OPERATOR ACTIONS

No operator actions shall be required to meet the targets set out in sections 2, 3 and 4 other than on an extended timescale. The timescale and circumstances for any operator intervention shall be agreed with the Engineer.

6. REACTIVITY SHUTDOWN CAPABILITY

Adequate shutdown margins shall be proposed by the designer for agreement by the Engineer.

7. SHUTDOWN FAULTS

Faults during refuelling or shutdown conditions should have the equivalent of at least two lines of protection.

8. TESTING

In-situ testing of the effectiveness of each system should be possible.

The operational status of each shutdown system shall be capable of being monitored at all times.

9. ADDITIONAL REQUIREMENTS

Notwithstanding the results of any reliability analysis, shutdown as defined in Section 2 shall be achieved by each diverse system even assuming a single credible failure in that system.

Where inherent reactor characteristics are claimed to provide a diverse shutdown argument, any safety related systems required to operate to support this claim shall also be able to withstand any single credible failure. These systems shall also meet the requirements 9.1 and 9.2 below.

- 9.1 The shutdown systems shall be designed so that their capability to shutdown the reactor (as defined in section 2) and meeting the requirements of section 4 is not impaired in the event of any of the hazards defined in Annex III.
- 9.2 The shutdown systems shall be designed so that their capability to shutdown the reactor (as defined in section 2) and meeting the requirements of section 4 is not impaired in the event of any of the hazards specified in Annex IV (fires, internal explosions, missiles, gas, steam or water releases).

Reliability Guidelines for Post Trip  
Cooling and Other Essential Systems

CONTENTS

1. INTRODUCTION
2. FUNCTION OF POST TRIP COOLING SYSTEMS
3. RELIABILITY TARGETS
4. APPLICATION OF RELIABILITY TARGETS
5. CALCULATION OF RELIABILITIES AND PERMITTED FAILURES
6. OPERATOR ACTIONS
7. VENTILATION SYSTEMS

## APPENDIX



## 1. INTRODUCTION

Post trip essential services or systems include those necessary for the removal to a guaranteed heat sink of fission product decay heat and other residual heat - termed the post trip cooling systems. During the pre-tender stage these requirements will be reviewed by the Engineer as design details evolve. If it turns out that the requirements are unnecessarily stringent in some areas - or on the other hand insufficiently restrictive - then the requirements may be changed. A satisfactory safety design requires an iteration between design principles and design development.

## 2. FUNCTION OF POST TRIP COOLING SYSTEMS

The systems should be designed to remove fission product decay heat and other residual heat from the reactor core following any credible fault or accident condition at such a rate and with such reliability and diversity as laid down in this specification. The specification is concerned, however, only with safety requirements. There may be further requirements to protect economic investment.

The heat shall be removed at a rate such that specified fuel criteria are met, and that any plant and structures which are necessary to prevent the radioactivity release limit given in Annex XIX from being exceeded are maintained within the temperature and stress limits which enable this integrity to be claimed.

This specification applies to all plant items, structures or equipment of all types\* (including system initiation signals and controls) which are essential to the heat removal function, whether they be the prime heat removal system or a supporting system. All such systems will be referred to collectively as post trip cooling systems.

The heat shall be removed to a guaranteed heat sink.

## 3. RELIABILITY TARGETS

The basic reliability targets are given in Annex V. General requirements involve the reliability of the tripping, shutdown and cooling systems.

The appropriate method of detailed application is likely to be design dependent. The approach detailed below is to be seen as illustrative of an acceptable approach. It does not preclude other approaches where the design makes this necessary or desirable providing the guidelines of Annex V are met.

In order to identify a unique reliability required from the cooling systems, following any given fault, pessimistic simplifying assumptions have to be made. These result in the requirement that cooling systems have to be designed to be effective, with a reliability required depending upon the initiating fault frequency, assuming:

- (a) the reactor trips via the less effective of the two lines of tripping.

---

\* Including mechanical, electrical, hydraulic systems etc and any operations associated with the control of radioactive releases.

- (b) where two diverse systems are provided, the more effective of the two shutdown systems has completely failed.

Furthermore it is proposed that all faults be divided into various broad classifications, having a defined frequency for the totality of all faults within each class. For each fault within a given classification, the permitted system unreliability is related to the classification frequency.

Annex V proposes a possible classification, but it is emphasised that the designer may choose to suggest an alternative division of faults. He may also sub-divide various classifications. Whatever classification is ultimately adopted certain minimum claimable frequencies will be applied for certain groups of faults, in order to ensure adequate redundancy/reliability in the design. Certain minimum claimable frequencies are detailed in the table, in Section 4 below, which is based on Annex V, Section 5.

In the event of the designer wishing to further sub-divide any given classification, the additional constraint is imposed that, following any credible initiating fault the cooling system unreliability should always be less than  $10^{-3}$  per demand.

#### 4. APPLICATION OF RELIABILITY TARGETS

The contractor shall compile a schedule of all initiating faults and fault sequences within each classification. The frequency assumed for each sequence shall be assessed and justified to the satisfaction of the Engineer.

The philosophy shall be adopted that, unless justified to the contrary, any single plant item, including pressure vessels or any pressure component may fail. Any exclusion shall be fully justified to the satisfaction of both the C.E.G.B. and the Licencing Authority.

If any post trip cooling system is required to operate with the reactor at power, combinations of faults could lead to system failure to an extent which requires the reactor to be tripped or shutdown. Such cases shall also be considered in defining the various initiating faults.

The various faults can then be divided into various broad classifications as described in Section 3 above. It is recognised that the final classification adopted will require a degree of iteration. For the first iteration the classification given in the table below is proposed as an example. Other classifications are not precluded. As noted in Annex V, and shown in the Table, for certain categories of faults minimum claimable total frequencies are specified for the purpose of system design. Total fault frequencies for other categories are recognised as being design dependent. In these cases the designer shall present justification for the values he intends to use as a basis for systems design.

A degree of flexibility is permissible in the target maximum cooling system unreliabilities especially for those cases where it can be shown that the containment system provides an additional barrier to an uncontrolled release.

Table IX-1  
Example of Fault Classification Scheme

Fault Classification	Examples of faults within classification	Minimum claimable initiating frequency for the totality of all faults in classification p.a. (note 12)	Corresponding maximum cooling system unreliability. See Annex V (notes 12 & 13) (per demand)
A Spurious reactor shutdown/guardline trip	See classification	10	$10^{-8}$
B All pressurised initiating faults which do not effect integrity of essential systems (note 2)	Reactivity faults, Pump failure faults, Spurious operation of engineered safeguards	1	$10^{-7}$
C Loss of grid supply which initiates a trip or requires a shutdown (note 1)	See classification	$10^{-1}$ (note 8)	$0.8 \times 10^{-6}$
D Small LOCA (note 3)	Minor leak, accidental slow depressurisation, Small pipe fracture	(note 10)	) ) ) ) )
E Large LOCA (note 3)	Any LOCA not in D including double ended pipe fractures	(note 10)	) ) ) )
F Faults originating within an essential system	Failure of any single item e.g. any single pipe failure (other than one causing LOCA), Circumferential failure of any valve, CW blockage	(notes 5 & 10)	) )To be )established on )the basis of )the designers' )assessed fault )frequencies ) )
G Internal hazards	Fires (note 6), T/A disintegration (note 7), Dropped Load (note 7), Disruptive failure of any pressure component (not causing LOCA)	(notes 6, 7 & 10)	) ) ) ) ) ) ) )
H External hazards (notes 4 & 14)	Aircraft crash, Earth tremors, Sabotage, Main Control room destruction (note 9)	-	(note 11)

NOTES

- (1) Ideally, the system design should be able to accommodate loss of external supplies to the station for the duration of the post trip period. Should this prove impracticable some credit may be claimed for grid restoration providing suitable justification can be provided. However, the following limiting probabilities shall be applied:

<u>Duration of grid loss</u>	<u>Probability of initiating event</u>
0 - 2 hours	$3.5 \times 10^{-2}$ p.a.
2 - 12 hours	$10^{-2}$ p.a.
>12 hours	$2 \times 10^{-3}$ p.a.

The above probabilities have been derived only for Sizewell 'B' Power Station and are subject to revision.

- (2) All such pressurised initiating faults have been assumed to place more or less the same minimum demand on essential systems performance. The minimum essential system performance used in reliability analysis shall be taken as the most onerous demand following any fault within the classification. If it so happens that a high demand is only required for a few low probability faults, further sub-division may be permitted provided the same  $\sum pf$  is maintained for the classification.
- (3) The allocation of LOCA faults within these two classifications shall be by discussion with the Engineer.
- (4) See Annex III for requirements.
- (5) It should be assumed that complete loss of cooling either due to blockage of the CW intake can occur, or complete system contamination by an oil slick.
- (6) It should be assumed possible for a fire to start in any area where combustible material is present or could be present.

All practicable steps shall be taken to limit the consequences of a fire or internal flooding, and recourse may be made to claiming low fault probability only if it is impracticable to do otherwise.

- (7) Recourse may be made to claiming a low fault probability for the case of a dropped load or turbine disintegration only if it is shown to be impracticable to site or protect the plant to render it invulnerable to such faults. It should be assumed that disintegration of any turbo-generator can occur due to overspeeding, thus creating missiles which could potentially damage adjacent plant.
- (8) This frequency will need justification and may depend upon the particular electrical system design.



- (9) See Annex XI for emergency control requirements not in Table.
- (10) Values to be ascribed and justified by the designer to the satisfaction of the Engineer.
- (11) Following any single accident, be it an aircraft crash, or control room damage, the system unreliability should not exceed  $10^{-3}$ .
- (12) An overriding requirement which should be met is that following any single credible initiating fault, the system unreliability is not greater than  $10^{-3}$ .
- (13) The system unreliability will be determined by constructing all possible sequences following the initiating fault. In constructing such consequences, a probability for loss of grid supplies may be used providing suitable justification is made. However, the probability of such a loss may not be assumed smaller than  $10^{-3}$  per trip. For such sequences, involving loss of grid, the basic philosophy shall be that the post trip cooling systems shall be sufficient without having to rely upon the restoration of grid for at least 3 hours. Furthermore for sequences involving grid loss such loss shall be assumed at the most disadvantageous time. In addition to meeting Annex V targets, the shutdown and cooling systems should also have a maximum unreliability not greater than  $10^{-2}$  failures per demand following any credible initiating fault accompanied by such grid loss.

Due account shall be taken of any consequential damage or consequential incident. Consequential effects can include:

Pipe whipping  
 Water hammer  
 Water, steam, gas release including temperature, pressure, shock wave and jet.  
 Flooding  
 Missile propagation.

- (14) The plant shall be designed to be unaffected by external floods of the nature described in Annex III.

#### OVERRIDING REQUIREMENT

Even though systems may be shown to meet the reliability requirements given above, the aim should be to make the credible failure of any plant item tolerable. This is regarded as part of the basic philosophy.

Thus, following any trip or credible fault, and taking due account of plant out on planned or permitted maintenance or undergoing testing, the post trip cooling systems should at all times perform adequately their overall function, with or without offsite power available, assuming a single credible failure.

This clause shall be interpreted as follows:

- (i) All reasonable measures should be taken in the design to avoid features, the failure of which during an accident could prejudice the functioning of the reactor engineered safeguards.
- (ii) Compliance with (i) above may in some cases of failure of passive components be impracticable or lead to unacceptable complications of the design and agreement may be sought to a small number of exceptions to this requirement provided it can be shown that the occurrence of such failures is sufficiently unlikely for them to be acceptable in relation to the safety hazard that might follow. It will be necessary, however, to show that the component undergoes no significant change in its operational or environmental state from before the initiating event until after the end of the period of required operation.

#### 5. CALCULATION OF RELIABILITIES AND PERMITTED FAILURES

Calculations shall be performed to show the system failure probabilities are less than those specified for the various initiating faults, when all possible component failures of the post trip cooling systems are considered. If any post trip cooling system is required to operate with the reactor at power, combinations of faults could lead to system failure to an extent which requires the reactor to be tripped or shutdown. In such cases, the fault combination becomes a reactor trip initiating fault and is additional to those specified in section 4. The reliability then required post trip may be determined by application of the approach given in section 3.

All data and methods of calculating system failure probabilities shall be agreed with the Engineer. It is desirable that this be done before design work commences. The following rules will be applied:

- 1. Only components for which sufficient reliability data already are available shall be used in the design unless agreed otherwise with the Engineer.
- 2. The treatment of maintenance and testing in reliability analysis is outlined in the appendix.
- 3. The possibility of a common mode or systematic failure affecting similar plant items shall be considered. Common mode failures can occur for all types of plant (not necessarily similar). Diverse equipment shall be provided unless it can be argued to the satisfaction of the Engineer that common mode failures or systematic failures can be discounted. As an overriding limit, however, the probability of a common mode failure affecting plant items of one type shall not be assumed to be less than  $10^{-5}$  failures per demand.
- 4. The calculations shall take into account the probability of any plant being in a failed condition, taking into account any alarms or other indications that might bring such failed plant to the attention of the operator. The possibility of maintenance errors shall be included in the analysis.



## 6. OPERATOR ACTIONS

For all faults not involving destruction of the control room, the post trip cooling systems shall be designed so that operator actions are neither required nor claimed within 30 minutes of the reactor trip. After 30 minutes operator action involving simple switching actions in the control room may be claimed providing suitable indication is available. Any local actions which might also be required and the timescales for such actions shall be consistent with the indication provided of actions required, the complexity of actions involved, staff availability and possible hazards from steam, water, gas or any other noxious material. Required reliabilities of the plant should be met without having to claim repair of failed items for at least 12 hours. Thereafter, arguments may depend on permissible interrupt times in cooling and the time to repair.

Furthermore, failure of the operator to take the correct action after 30 minutes shall not lead to any immediate safety hazard, although some plant damage or a limited activity release might be permissible. It should still be possible to re-establish cooling and contain the effects of any damage even if correct operator actions are delayed for hours.

To cater for the case of main control room damage, (see Annex XI), as a result of which a reactor trip may occur, operator action shall not normally be claimed for at least 60 minutes even allowing for spurious signals being sent out from the control room. See Annex XI for further details and for emergency control requirements.

The effect of the operator taking an incorrect action at any time shall be assessed.

## 7. VENTILATION SYSTEMS

Ventilation systems may be invoked in the nuclear safety case for any of the following reasons:

- (a) ventilation is required or must be isolated in order to keep safety related equipment within acceptable conditions during normal operation or during an emergency;
- (b) ventilation is required or must be isolated in order to permit operator essential access or occupation during normal operation or an emergency;
- (c) ventilation is required or must be isolated in an emergency in order to prevent escalation of the accident;
- (d) ventilation is required in order to permit essential monitoring equipment (e.g. air borne activity monitoring) to function adequately;
- (e) ventilation is required for contamination control, where failure might lead to an unacceptable spread of activity.

A ventilation system invoked in any of these ways shall be defined as a safety ventilation system and shall satisfy the Design Requirements of this and other Annexes as appropriate.

Safety ventilation systems shall include positive means of dealing with smoke, fumes and high temperature atmospheres which might result from any fire or other incident of safety significance, where these effects might otherwise escalate the incident, disable essential plant or jeopardise essential operator action. There shall be positive provisions of suitable integrity to avoid the spread of fire via ventilation systems. Any essential monitoring equipment shall be designed to withstand the environment produced by the fire. The fresh air supply intakes to any fire zone\* containing safety related equipment shall be located away from the exhaust air outlets and smoke vents from the same and all other fire zones. There shall be no common ventilation equipment shared between the Main Control Room and the Emergency Control Room.

Provisions shall be made for adequate in-service inspection, test and maintenance of ventilation systems, with regard to both electrical and mechanical aspects.

---

\* Fire zone is defined in Annex X

APPENDIX TO ANNEX IXThe Treatment of Maintenance and Testing in Reliability Analyses

Ideally the reliability requirements should be met at all times even when plant is out on maintenance, planned or unplanned, or is undergoing testing. However, since the basic criterion given in Annex V is probabilistic then maintenance and testing can also be treated in a probabilistic manner when demonstrating that the basic criterion is met. Nevertheless, when plant is out on maintenance or is undergoing testing it is desirable that the actual system unreliability at that particular point in time is sensibly limited. It would be undesirable for the cooling system unreliability at any point in time to be worsened by more than one decade when the permitted unreliability lies between  $10^{-4}$  and  $10^{-5}$ , or by two decades when the permitted unreliability is  $10^{-6}$  or less. For cases where the permitted unreliability lies between  $10^{-3}$  and  $10^{-4}$  the point unreliability should never be increased above  $10^{-3}$ .

Thus, concurrent with demonstrating that the overall reliability target can be met on a probabilistic basis, the designer shall also discuss with the Engineer a maintenance strategy. To assist such discussions the designer shall produce point-in-time reliability calculations to cover all envisaged maintenance and testing conditions. Following such discussions the designer shall propose a maintenance strategy to the satisfaction of the Engineer and shall also propose envisaged operating rules and restrictions on maintenance and testing (e.g. designer shall specify minimum plant to be available). Only in exceptional circumstances will rules which limit permissible maintenance outage be considered acceptable.

Wherever reasonably practicable maintenance procedures proposed shall be straightforward to minimise the risk of assumed maintenance outage times being exceeded. Maintenance by replacement would be considered acceptable in certain circumstances.

Only those maintenance outage times approved by the Engineer shall be used.

### 3.3 Testing

Where it is necessary for testing to disconnect or remove elements of a system, this shall not cause signals or changes in plant state that may be detrimental to safety.

### 3.4 Operational Constraint

The minimum available set of instrumentation, alarms and control facilities with less than which continued operation is not permitted shall be defined in the Operating Rules or IOI's.

### 3.5 Hazards

Essential Control, Instrumentation and Alarm systems shall be so designed that:

- (a) Following damage to any part of the essential control systems, the effects of any resultant spurious signals, open and short circuits should not prejudice nuclear safety.
- (b) Where an indication or alarm could be rendered suspect by a particular hazard affecting plant or the information routes between plant and the MCR or ECR, this fact should be made clear to the operator.
- (c) Instrumentation provided for purpose (d) of 3.1.2.1 should enable the operator to differentiate between hazards where the subsequent actions required are different.

### 3.6 Security

Enclosed unmanned areas containing essential control facilities, instrumentation and alarm equipment shall be provided with security measures to prevent or warn of unauthorised entry.

## 4. RECORDS

Records shall be made of selected safety parameters to show the trends leading up to a fault or accident, and the effectiveness of the actions carried out.

Records shall also be made (not necessarily of the same parameters) to enable the ECR personnel, who may not have been in the MCR previously during the incident, to acquire sufficient familiarity with its circumstances for them to formulate a strategy for the maintenance or recovery of safety.

The methods used for the capture, storage and presentation of recorded data shall meet the requirements of 3.1.2.2 above. The accumulation period, after which data are discarded or no longer immediately retrievable, and the frequency of update of the records shall be adequate for the above purposes during and following all credible faults.

It should be ensured that sufficient records exist and can be retrieved following an incident (including one in which the MCR or ECR is damaged) for determination of the nature and cause of the incident, the performance of the essential systems and the magnitude and duration of any release of radioactive materials. A schedule should be compiled detailing the recorded parameters needed for this purpose. The recordings should have adequate accuracy and frequency of up-date for post-incident analysis, and should include accurate timing markers.

## 5. CONTROL ROOMS AND OPERATOR ACTION

### 5.1 General

#### 5.1.1 Main and Emergency Control Rooms

In addition to the Main Control Room, from which the normal day-to-day running of the station and the great majority of faults and incidents are managed, there shall be an additional location where limited monitoring and control can be carried out. Annex XI sets out the reasons behind this and gives the monitoring and control requirements in full.

#### 5.1.2 Local Control

In situations where, irrespective of which control room is in use and manned, plant control using local control facilities is claimed, the manpower requirements, manual actions and their timescales shall be consistent with the complexity of the task involved, the possible presence of hazards from steam, water, gas or other noxious material, and the local indications provided. Local actions may not be claimed immediately post trip.

#### 5.1.3 Operation Action

All operator actions claimed shall be identified on a schedule which shall show the control facilities used and their location, the allowable timescale, the instrumentation and alarms that provide the cues for action and those that provide confirmation of its correct execution. The reliability of the control equipment claimed for safety shall be consistent with the demands made upon the operator. Account shall be taken of the



probability of human error to the extent that the design shall not make unacceptable demands upon operator action in critical situations, and should tolerate an individual failure of the operator to act correctly. (Where this is not so, the actions should be performed by redundant automatic systems). Justification will be required that the demands made upon the operator are reasonable in terms of both function and implied reliability. The system design shall take full account of human performance shaping factors and best ergonomic practice so as to result in reliability of operator action.

#### 5.1.4 Control Room Design

The following are requirements upon the design of the MCR and ECR:

- (a) To maximise operator perception and response the design of the MCR and ECR should embody the best available ergonomic principles. This should include environmental design and layout as well as the design of the desks and panels and the control facilities, information displays, instrumentation and alarms.
- (b) The environment should be controlled so as to be suitable for continuous occupation. Adequate protection shall be provided against internal and external hazards, including hazards such as released radioactive material from any adjacent reactor. See Annexes III, IV and XI for details.
- (c) Following damage to any part of the MCR or ECR, the effects of any resultant spurious signals, open and short circuits should not prejudice nuclear safety.

#### 5.2 Main Control Room

The Main Control Room shall contain all control facilities, instrumentation and alarms necessary for the reactor to be operated safely (i.e. those serving purposes (a) to (e) of section 3.1.2.1), together with means of gaining access to the recorded information provided under section 4. The instrumentation and alarms shall enable the operator to identify any trends, disturbances or faults which could potentially lead to an unsafe situation, and the control facilities shall enable him to take appropriate action to ensure safety is maintained. The MCR shall also contain instrumentation and alarms necessary to monitor the situation fully following any trip or incident (i.e. serving purposes (f) to (l) of section 3.1.2.1).



Automatic essential control systems should be provided so that operator action is neither required nor claimed as part of the safety case within 30 minutes following reactor trip. However, in the event of extensive failure either of these control systems or in the reactor system, the intention is that the operator will be allowed to take (or to regain and then to take) control during this period. He will also be allowed to reinforce the automatic systems by manually repeating their (simple switching) actions where it is clear that some elements of a redundant system are not in their correct state. This should not be claimed as part of the formal safety case. It is therefore especially important that the reliability of the instrumentation and alarm systems is such that the operator will not be misled into taking action. The design shall reduce to a practicable minimum the likelihood of the operator inadvertently or mistakenly inhibiting the correct functioning of the post trip systems. In the event of partial failure of a system, the operator must not be misled into intervening while its performance remains sufficient and adequate for safety.

30 minutes after a reactor trip operator actions involving simple switching in the MCR may be claimed provided that the actions form part of a check list which is followed through after each and every trip. This check list may "branch" depending upon the states of certain plant items or the values of certain parameters, etc., but it is not permissible to claim a unique operator action for a specific fault without including that fault and the action amongst those covered by the checklist.

### 5.3

#### Emergency Control Room

The Emergency Control Room should contain all control facilities, instrumentation and alarms necessary to ensure safety in the event of the MCR being damaged or rendered unusable or uninhabitable. Instrumentation and alarms necessary for safety in this event should be provided (ie. those serving purposes (f) to (l) of section 3.1.2.1), together with a manual means of tripping the reactor. The provision of other controls in the ECR will depend upon the system requirements and the adequacy of local control facilities. The ECR should contain means of gaining access to the recorded information provided under section 4.

If the ECR is permanently manned then operator action from there may be claimed in the same manner as for the MCR, subject to the conditions laid down in Annex XI. If it is not so manned then operator action may be claimed not less than 60 minutes after reactor trip. This action may be performed from the ECR or locally depending on whether the ECR is provided with controls (other than reactor trip) or not.

The ECR should be provided with adequate external communications facilities, and with internal communications facilities to the MCR and to any local control points. It should also be adequately accessible from the Station perimeter.

If the ECR is unmanned it should be provided with security measures that will prevent or warn of unauthorised entry.

#### 6. TECHNICAL SUPPORT CENTRE

A room should be set aside which can be used as a Technical Support Centre for specialists and advisers brought to the site in the event of an incident or emergency. It should be separated from but within easy reach of the MCR and should have adequate communications with the On-Site Emergency Control Centre. It should contain facilities to allow the state of the reactor and essential plant to be monitored adequately without having to involve the MCR operators.

APPENDIX

Within the context of this Annex the following words have been used with the defined meanings which follow them.

<u>Essential</u>	A system is essential if it operates to prevent the uncontrolled release of radioactive material by ensuring the continuity of the barriers to such a release, or by intercepting the material before it passes beyond the final recognised barrier.
<u>Control Facility</u>	Equipment provided, in the control room or elsewhere, for the express purpose of allowing manual control.
<u>Manual</u>	Involving intervention or action by the operator or others, via remote control systems or directly at the item controlled.

Safety Related Electrical Equipment

CONTENTS

1. INTRODUCTION
2. DESIGN PRINCIPLES
  - 2.1 Principles Drawn from Annex IX
  - 2.2 Additional Principles Specific to Essential Electrical Systems
  - 2.3 Calculation of Reliabilities and Permitted Failures (Drawn from Annex IX)
  - 2.4 Operator Actions
  - 2.5 Segregation
3. IDENTIFICATION OF SAFETY-RELATED ELECTRICAL (AND MECHANICAL) EQUIPMENT
4. RELIABILITY REQUIREMENTS OF ESSENTIAL ELECTRICAL EQUIPMENT
  - 4.1 Safety Modes of Electrical Equipment Operations
  - 4.2 System Requirements
  - 4.3 Equipment Item Requirements
5. FAILURE MODES OF ESSENTIAL ELECTRICAL EQUIPMENT
6. INSTALLATION AND COMMISSIONING
  - 6.1 Installation
  - 6.2 Commissioning Tests
7. OPERATIONAL RELIABILITY SAFEGUARDS
  - 7.1 Design Features to Facilitate Inspection, Test and Maintenance
  - 7.2 Alarm Arrangements
8. SPECIAL DESIGN FEATURES
  - 8.1 Design Provisions Against Fire
  - 8.2 Ventilation Systems
9. PROVISIONS TO FREEZE THE DESIGN

## 1. INTRODUCTION

The safety related electrical equipment consists firstly of all electrical equipment possessing failure modes with nuclear safety implications and secondly all electrical equipment which may be claimed as protective equipment in a nuclear safety argument, excepting where such equipment is specified in the Specification for Reactor Safety Systems.

This Annex is intended to identify the main safety requirements. They are in addition to the requirements of the main electrical specification which may also have safety implications.

## 2. DESIGN PRINCIPLES

### 2.1 Principles Drawn from Annex IX

Following a normal or accident-associated reactor trip or shut down, the overall requirements of the appropriate equipment claimed for safety shall be as given in Annex IX. This equipment will in general be partly electrical and partly mechanical, and therefore the unreliability of the electrical equipment itself should lie far enough within the limit to provide an adequate allowance for the unreliability of the mechanical equipment. The method of defining the maximum unreliability of the electrical equipment is given in Section 4.

### 2.2 Additional Principles Specific to Essential Electrical Systems

In addition to the principles drawn from Annex IX, certain further principles are to be applied specifically to any area of electrical equipment which can readily be identified as an essential system required to operate following any particular fault sequence. These are as follows:

- (1) It is a requirement not only that safety related equipment shall fulfil its nuclear safety duty with adequate integrity, but also that a satisfactory case can be constructed that it does so. In order to promote both of these requirements, it is an objective that the nuclear safety argument should be as simple as practicable. In pursuit of simplicity, the following are subsidiary objectives:-



- (i) Interactions between groups of essential electrical equipment which are intended to be independent of one another should be minimised.

Thus interactions between reactor/turbine units should be minimised. Furthermore, if safety related equipment on a particular reactor/turbine unit is grouped into trains/chains, interactions between these trains/chains should be minimised. Electrical interactions can be created by, for example, supply interconnection, plant sequencing and plant interlocking.

- (ii) In the attainment of safe states at the system level, the dependence on plant sequencing and interlocks within any group of safety related equipment should be minimised.
- (iii) The attainment of safe states at the system level should not, as far as practicable, be dependent on the correctness of operator indications and alarms. Notwithstanding this, failures of alarms and indications associated with the state of a plant item should preferentially be in a direction which suggests that the plant item is in the state least favourable to nuclear safety.
- (iv) The design of safety related electrical equipment should be based on logic which operates on parameters as close as practicable to the plant state of direct safety significance and avoids utilising inferred dependencies.
- (v) Items of equipment should be designed as far as practicable to prevent both the initiation and propagation of faults.
- (vi) As far as practicable, failure modes in the dangerous direction (in the nuclear safety context) on safety related systems should be avoided. Where a fail-safe mode is claimed, a justification shall be given that this particular failure mode is in fact safe. Where equipment is not fail safe, facilities should be provided for continuously monitoring the state of the equipment and initiating appropriate alarms.
- (vii) Where small current circuitry switches a major plant item, the unreliability of the circuitry should not dominate the overall unreliability of the major item. Additionally, however, in order to facilitate the reliability analysis and also the process of testing, the switching circuitry should be simple.

(viii) Where segregation is claimed between groups of safety related plant, the segregation rules should not, as far as practicable, be different for different essential operations.

- (2) Under all conditions in which particular equipment is claimed for safety, that equipment shall be operating within its specified electrical and environmental limits. It should be recognised that, under fault conditions, the electrical and environmental conditions may be disturbed.

### 2.3 Calculation of Reliabilities and Permitted Failures (Drawn from Annex IX)

Calculations shall be performed to show that, for the various initiating faults, the overall system failure probabilities are less than those specified in Annex IX when all possible component failures of the essential electrical system are considered.

If any post trip cooling system is required to operate with the reactor at power, combinations of faults could lead to system failure to an extent which requires the reactor to be tripped or shut down. In such cases the fault combination becomes a reactor trip initiating fault.

All data and methods of calculating system failure probabilities shall be agreed with the Engineer. The rules detailed in Section 5 of Annex IX shall be followed.

### 2.4 Operator Actions

Rules for operator action are detailed in Annexes IX, XI and XX.

### 2.5 Segregation

In the nuclear safety context, the object of segregation is to ensure that, following any incident involving damage to safety related equipment, sufficient equipment remains to carry out the safety duty and meet the integrity requirements of Annex IX. A requirement for segregation applies potentially both to mechanical and electrical equipment, and it should be satisfied for all incidents covered by Table IX-1 of Annex IX. The degree of protection provided by the claimed segregation shall in each case be consistent with the potential extent of damage. A further general objective regarding segregation is identified in Section 2.2(1) (viii) above.

Where segregation is claimed for limiting fire damage, the segregation barriers shall function effectively as fire barriers. There should also be a means of fire detection and extinguishing within each segregated area. The means of fire detection and extinguishing shall be consistent in terms of integrity with the integrity required by Annex IX. The segregation requirements in relation to fire are amplified in Section 8.1 below.

Certain special segregation requirements for operator alarms are identified in Section 7.2, and for ventilation systems in Section 8.2.

Segregation requirements are set out in the GDCD Technical Instruction on the Segregation of Cables and Electrical Plant in PWR Power Stations (E/TI/004).

### 3. IDENTIFICATION OF SAFETY-RELATED ELECTRICAL (AND MECHANICAL) EQUIPMENT

This section is concerned with identifying:

- (1) all electrical equipment possessing failure modes with nuclear safety implications.
- (2) all electrical equipment (except safety system equipment - covered separately) which may be claimed as protective equipment in a nuclear safety case:
  - (a) in normal reactor operating/trip conditions
  - (b) in fault conditions.

By identifying the limiting fault sequences involving every recognisable area of safety-related equipment, both electrical and mechanical, the total extent of this equipment can be determined. Fault sequences can be regarded as limiting if:

- (i) the most extreme permissible conditions of system operation and plant unavailability are taken into account.
- (ii) reliance in terms of reliability on each particular area of safety-related equipment is higher than for other conditions. If particular equipment is required to operate in different modes in different fault conditions, a separate limiting fault sequence is appropriate for each mode.

### 4. RELIABILITY REQUIREMENTS OF ESSENTIAL ELECTRICAL EQUIPMENT

#### 4.1 Safety Modes of Electrical Equipment Operations

From the identification procedure outlined in Section 3 above, it is possible to list all electrical equipment which may be claimed as protective equipment in the nuclear safety argument and all the safety modes of operation of this equipment.

#### 4.2 System Requirements

The maximum unreliability for each mode of operation in each equipment area should be consistent with Table IX-1 of Annex IX and also with the Principles of Section 2 above (taking into account failure modes itemised in Section 5 below). It is not sufficient for the electrical equipment alone to achieve an adequately low unreliability. There shall be a sufficient unreliability provision for the mechanical plant also.

#### 4.3 Equipment Item Requirements

All safety related electrical equipment shall be individually to the Board's approval and, where possible, be of an established reliable design. Items should either have been proven in similar service or should be subject to thorough type testing. Where EES 1980 is relevant, type testing shall be in accordance with this document (class applicable to the siting of the relevant equipment), and for control and instrumentation equipment shall cover radio frequency interference, ambient temperature and relative humidity to the same standard as Annex VII (subject also to the principle specified in Section 2.2(2) above), with the power levels to the approval of the Engineer. Where EES 1980 is not relevant by reason of the equipment type and/or the environmental conditions, type testing shall be to the approval of the Engineer.

The failure rate of each item of equipment shall be established either by:

- (i) observation to a suitable confidence level of identical equipment under similar operating conditions, or
- (ii) calculated from a component count, the data of which has been established to a suitable confidence level under similar conditions, or
- (iii) derived in a manner to be agreed with the Engineer from generic data (obtained from similar, but not necessarily identical, equipment) where neither (i) nor (ii) above is reasonably practicable.

#### 5. FAILURE MODES OF ESSENTIAL ELECTRICAL EQUIPMENT

From the identification procedure outlined in Section 3 above, it is possible to list all electrical equipment possessing failure modes with nuclear safety implications and all the relevant failure modes of this equipment.

Failure modes to be considered include:

Simple failure of any switching operation,

e.g. relay contact failure  
 relay coil failure  
 timer failure  
 circuit breaker operation failure

Fuse failure  
 Control system failure  
 Alarm failure  
 Failure of an individual power supply source  
 Diode failure  
 Single open circuit  
 Single short circuit  
 Busbar/cable earth fault  
 Total open circuit of all cables within a single fire protection zone (resulting from a fire)  
 Combinations of open and short circuits within a single fire protection zone  
 All consequential electrical failures which can result from any incident in classifications C to H inclusive from the Table in Annex IX  
 Any other identified electrical fault which is considered to impose a safety hazard

N.B. Specific instances of short circuiting may be argued as incredible by reason of separation or protection. This, however, does not apply to busbar or cable earth faults.

The faults listed above are to be categorised according to Table IX-1 of Annex IX. The protective equipment must be shown to be adequate as in Section 4 above.

## 6 INSTALLATION AND COMMISSIONING

### 6.1 Installation

All control equipment of the safety related electrical equipment should be housed in segregated cubicles which should be locked by unique key systems.

The key locking systems shall permit the maximum access for maintenance and testing at any time subject to the limitation that it shall not be possible to invalidate the Design Requirements in this and other Annexes.

Emergency lighting shall be provided at all the locations where safety related electrical equipment is operated.



A direct telephone facility shall be provided between all the locations where safety related electrical equipment is installed. This facility may be self powered handsets with suitable outlets at each equipment location.

#### 6.2 Commissioning Tests

All safety-related electrical equipment shall be subjected to commissioning tests when the equipment has been installed in its correct position and is working.

The testing shall demonstrate that the equipment performs in accordance with the design intent in terms both of function and integrity within the environment of the reactor systems. The tests shall demonstrate the capability to:

- (a) correctly initiate the operation of essential equipment in response to all demands for which a response is invoked in the safety case;
- (b) correctly sustain the operation of essential equipment for the periods required for reactor safety.

### 7. OPERATIONAL RELIABILITY SAFEGUARDS

#### 7.1 Design Features to Facilitate Inspection, Test and Maintenance

Items of equipment and cabling shall be inspectable.

Testing facilities shall be provided so that the correct safety functioning of all safety related electrical equipment can be proved. As far as practicable, equipment shall be testable without prejudicing the overall safety function and without causing a restriction in station operation. Arrangements for essential maintenance should fulfil the same requirements. After testing or maintenance it shall be possible to demonstrate that all items of equipment have been reinstated to their correct safety operational conditions.

The frequency of testing and maintenance of safety related electrical equipment shall be sufficient to satisfy the reliability and failure probabilities required for safety and also to ensure that the operational experience of the equipment is consistent with the commissioning tests. Equally, however, proposed frequencies of testing and maintenance shall take into account the following:

- (i) the burden on operating staff;
- (ii) the consideration that maintenance errors may themselves set limits to claimable reliability;
- (iii) the risk of causing premature equipment wear out.



Requirements for testing and maintenance of electrical equipment are in the Appendix to Annex IX. Testing/maintenance periods should be minimised taking into account the consequences of such outages.

In all cases the testing and maintenance periods shall be defined.

## 7.2 Alarm Arrangements

Safety related electrical equipment shall include alarms for annunciating failed modes of the equipment. Alarms with safety significance shall be defined as safety alarms and shall satisfy the requirements of this and other Annexes. In particular, Annex XX gives safety principles and design considerations to be applied to these alarms. Alarms and other outputs from plant protection equipment shall be adequately buffered so as to ensure that spurious operation of the protection equipment does not occur as a result of a fault in an output circuit. Safety alarms shall be provided in the Main Control Room and in the Emergency Control Room. In each safety-related equipment area, sufficient local alarms shall be provided to enable all equipment faults to be located quickly.

## 8. SPECIAL DESIGN FEATURES

### 8.1 Design Provisions Against Fire

Items of equipment and cabling shall be designed and located as far as practicable to prevent both the initiation and propagation of faults and in particular the start and spread of fire. Electrical protection devices, e.g. overcurrent protection, shall be provided to minimise the risk of fire resulting from electrical overload.

In order to determine the extent of the fire hazard to nuclear safety, it is necessary to identify all locations where a fire could break out and, either directly or by spreading, give rise to a risk of damage to safety related equipment or cabling.

Areas where fires could potentially start shall be divided into fire zones. Note that unless special provisions are identified, the possibility of operators (inadvertently) transporting combustible material or starting a fire cannot be ruled out. The use and storage of combustibles in areas adjacent to or containing items important to safety shall

therefore be kept to a practicable minimum, and heat and spark producing operations such as welding, cutting, brazing, etc., should be controlled by issue of work permits. A minimum fire resistance of 1 hour shall be provided for any boundary of a fire zone. Fire shall be prevented from spreading from one zone to another by either of the following two means:-

- (a) Provision of zone boundaries of sufficiently high fire resistance such that the fire would burn out before the boundary is breached. This requires administrative procedures during both design and operation to ensure that allowable inventories of combustibles are not exceeded.
- (b) Provision of means of fire protection which, in conjunction with the fire resistance of the boundary, is such that the fire would be extinguished before the boundary is breached. This requires fire protection within the zone of sufficient capability to extinguish in due time any credible fire, taking into account any exacerbating fire related events (e.g. explosion, structural collapse, pressure component failure, fire extinguishing water supply system pipework failure). Such aggravating events may only be discounted if it can be shown that there could be no cause/effect relationship with the fire.

The positioning of fire zone boundaries in relation to the segregation of safety related plant may be according to either one or the other of the following two approaches:-

- (i) Fire zone boundaries may coincide with segregation boundaries, such that failure of all safety related equipment within the fire zone shall be acceptable when judged against the Design Requirements of this and other Annexes. This is the preferred approach and should be implemented wherever practicable, taking into account other important design requirements.
- (ii) It may alternatively be argued that, by virtue of the application of local fire protection of sufficient capability within a zone, the extent of failure of safety related equipment within the zone will be limited such as to be acceptable when judged against the Design Requirements of this and other Annexes. This approach should only be adopted where other important design requirements demand it, and requires prior agreement of the Engineer.

It shall be assumed that all safety related equipment which could be affected by a fire fails in the most adverse relevant manner.

Every fire compartment bounded by a fire barrier where the barrier is claimed in the nuclear safety argument should possess fixed means of fire detection of adequate functional capability and integrity, whether or not that compartment itself contains safety related equipment or cabling. Fire extinguishing equipment shall be provided where appropriate which is capable, with adequate integrity, of extinguishing any fire which can arise in any such compartment, within the fire rating of the compartment boundaries. Fire detection and extinguishing systems should be immune from possible failure resulting either directly or indirectly from any fire they are intended to detect and extinguish.

Fire detection and extinguishing systems with safety significance shall be defined as safety fire detection and extinguishing systems and shall satisfy the Design Requirements of this and other Annexes. They shall be capable of operation under all envisageable emergency conditions in which they remain of safety significance. Safety fire detection systems shall fulfil the same general requirements as safety alarms (see Section 7.2 above) and shall annunciate in the Main Control Room and in the Emergency Control Room. They shall be capable of being energised by emergency power supplies.

Fire detection systems shall have an acceptably low spurious initiation rate. The function and integrity of safety related equipment shall not be unacceptably impaired by spurious operation or a breach associated with any fixed means of fire extinguishing. Note that spurious operation or a breach may potentially arise as a consequence of an incident such as a fire or an explosion in another location or as a consequence of hot fluid release (e.g. steam). Access to operate manual means of fire extinguishing (where manual fire extinguishing is claimed in the formal safety argument) shall be practicable under all conditions which might arise in association with the relevant fire. Automatic means of fire extinguishing shall be capable of manual initiation and shut off, where feasible.

Means of fire extinguishing shall be provided with adequate support systems, particularly ventilation (see Section 8.2 below) and drainage (in areas where a wet means of extinguishing may be employed).

Provision shall be made for adequate in-service inspection, test and maintenance of fire detection and extinguishing equipment, with regard to both electrical and mechanical aspects.

## 8.2 Ventilation Systems

See Annex IX for requirements.

9. PROVISIONS TO FREEZE THE DESIGN

At the appropriate time the Contractor shall provide Specifications, Drawings and Test Results required in connection with obtaining a site licence from the Nuclear Installations Inspectorate and shall adhere rigidly to the procedures detailed below.

- (a) Each individual item of equipment in safety related electrical equipment shall be specified individually and completely. Separate drawings shall be produced for the safety related electrical equipment.
- (b) After design approval has been given by the Board for such equipment no modifications shall be carried out without the permission of the Engineer.
- (c) An individual manufacturer's test certificate shall be provided for each item of equipment. The test procedure shall be agreed with the Engineer.
- (d) A list of drawings defining the safety related electrical equipment shall be agreed between the Board's Engineer and the Contractor. This list shall include a Schedule of all major items in the Systems.

Emergency Control



CONTENTS

1. NEED FOR EMERGENCY CONTROL
2. PROVISIONS FOR EMERGENCY CONTROL

## APPENDIX



## 1. NEED FOR EMERGENCY CONTROL

Basically the need for emergency control arises from some event which could destroy the effectiveness of the normal essential systems post trip, or destroy the means for controlling such systems. The following is a list, not necessarily exhaustive, of events (not all necessarily considered credible) which could necessitate emergency control to varying degrees:

1. Aircraft crash causing major damage to the main control room
2. Aircraft crash causing damage to the normal essential systems exterior to control room.
3. Fire or sabotage causing major damage to the control room.
4. Sabotage outside main control room.
5. Possibility of a common mode or systematic fault invalidating normal essential systems e.g.  
     Complete CW blockage  
     Common mode fault in all diesels following a grid disconnection incident
6. Fire destroying a control equipment location
7. Turbine disintegration
8. Insurgents
9. Effect of hypothetical major accident on nearby reactor

A discussion of the consequences of the above events is given in the Appendix. Such consideration of the consequences led to the formulation of the guidelines detailed in the next section.

## 2. PROVISIONS FOR EMERGENCY CONTROL

The following aspects should be considered in the development of an acceptable scheme. It may not be necessary, however, to accommodate every one of the provisions listed.

1. Any single main control room (MCR) could suffer major damage by fire, sabotage or an aircraft crash. Other incidents also could render the MCR uninhabitable. Although it would be possible to provide some degree of protection against these hazards, and indeed this is desirable, the principle to be adopted is that it must be possible to safely shut down, and to successfully remove the post trip heat, in the assumed event of extensive damage to the MCR.
2. In complying with principle 1, it shall be assumed that spurious signals could also be transmitted to any plant item for which control can be exercised in the MCR.

3. Adequate indication shall be provided to monitor the state of the reactor from at least one emergency control centre should the MCR be rendered uninhabitable or suffer major damage.
4. Conversely, it shall be possible to safely shut down, and to successfully remove the post trip heat in the assumed event of major damage to any emergency control centre, or to an emergency control room if one is provided. Providing the emergency control room or control centre is adequately separated from the main control room, the main control room may be assumed to remain undamaged. Due account shall be taken of any spurious signals that could be transmitted from any emergency control room or centre.
5. In the event of major damage to the MCR the manual actions which subsequently may be claimed depend upon whether or not a permanently manned emergency control room is provided and whether a completely separate alternative cooling system (for pressurised faults) is also provided.

If a permanently manned emergency control room is provided, then, subject to the design proposals being acceptable to the CEGB, manual action could be claimed after 30 mins. - providing principle 2 is satisfied.

If a permanently manned emergency control room is not provided no manual actions may be claimed for at least 60 minutes. Actions which may be claimed thereafter depend upon whether or not a completely separate alternative cooling system is provided:

- (a) If a completely separate alternative cooling system is not provided reliance may instead be placed upon the separation and segregation of the normal systems together with the provision, if necessary, of local emergency control locations. However, there shall be one designated emergency control point from which the state of the reactor can be adequately monitored (see 3 above) and which has adequate communications with any local emergency control location. Because of the uncertainty as regards total damage to the system any control action claimed, other than local control, should be kept to a minimum.
- (b) If a completely separate alternative cooling system, together with an emergency control room, are provided both physically remote from the MCR, then various actions may be claimed after 60 minutes, although any claimed action shall be consistent with the complexity and indication provided.

Due account shall be taken of the availability of trained operators. There shall be adequate access to any emergency control points from outside the station buildings, and remote from the MCR.

Note that major control room damage is one of the external hazards identified in classification H of Annex V and IX and should be analysed according to the requirements of those annexes. Any emergency control centre(s) provided to deal with MCR destruction may also be claimed when demonstrating any other reliability requirements.

6. The probability of failing to safely shut down and to remove post trip heat, in the event of damage to the MCR, should each be less than  $10^{-3}$ . See Annex IX.
7. The MCR shall be so sited that no single credible fault could cause both a depressurised fault situation and MCR destruction.
8. In the case of a multiple reactor site, it shall be possible to safely shut down and cool each reactor in the event of a major radioactive release from any other reactor.
9. Adequate diversity, segregation and separation of the essential systems shall be provided, as required by Annex III, to take into account aircraft crashes, fires, turbine disintegration, common mode faults, pipework failure and its consequences etc.

No specific provision for sabotage or protection against insurgents has influenced the above 9 principles. See Annex III for sabotage requirements.

The trip system should also be fail safe so that any damage to it results in a reactor trip. If an incident destroying the control room does not trip the reactor this is acceptable and reliance can be placed on automatic trip should the need arise. Each emergency control centre should be provided with a means to trip the reactor.

APPENDIXDISCUSSION OF POSSIBLE CONSEQUENCES OF FAULTS LISTED IN SECTION 1

Fault (1) requires at least one emergency control point, remote from the main control room (MCR), from which the state of the reactor may be observed. It may require some manual control facilities of the normal essential systems to be provided outside the MCR, noting that if control normally is from the MCR spurious signals could be dispatched from the MCR; or requires provision for operating a completely separate emergency cooling system located well away from the MCR.

Fault (2) could be accommodated by splitting the normal essential system into a number ( 2 ) of completely segregated chains and providing adequate physical separation between chains.

Fault (3) places the same requirements as fault (1).

The approach to fault (4) is described in Annex III.

Fault (5) could require provision of a completely separate back-up cooling system, although there is no requirement here for control to be outside MCR.

Fault (6) can be covered by adequate separation and segregation of the chains in the essential cooling systems. Note that a single location for installing all control equipment is not permissible.

Fault (7) would only require adequate separation of normal essential systems from the T/A.

Fault (8) will be guarded against by CEGB site security measures.

Fault (9) could be accommodated by requiring, in the hypothetical event of a major release of fission products from a nearby reactor, that all staff essential to the safe shut-down of the reactor could be collected in time within the MCR which would have adequate protection, and contain adequate provisions. Self air units also would have to be available should plant external to the MCR require attention.

Containment

CONTENTS

1. DEFINITIONS
2. THE ROLE OF CONTAINMENT
3. PRINCIPAL DESIGN REQUIREMENTS
4. REQUIRED HAZARD ASSESSMENTS



## 1. DEFINITIONS

The primary containment is a pressure retaining structure enclosing the reactor system. The complete contents of the primary cooling circuit should be contained in the event of a rupture in the primary circuit. The secondary containment is a structure enclosing the primary containment and reactor auxiliary circuits. It is designed to prevent an unfiltered release to atmosphere of leakage from the primary containment. The interspace is that volume between the primary and secondary containments. Major releases of radioactivity to the environment due to failure of plant and equipment outside the containment which could result in a possible path for release of activity to the environment shall be prevented by automatic isolating valves of the requisite integrity.

## 2. THE ROLE OF CONTAINMENT

The containment system shall be designed to ensure that in the event of any credible fault the release of radioactivity to the environment is within the limits given in Annexes V and XIX.

Under credible LOCA conditions the design of essential systems should be such as to ensure that, in general, fuel pin geometry is preserved to the extent that the fuel remains coolable and unacceptable damage to the fuel is precluded. However the containment system shall be capable of meeting the release criteria assuming that a considerable proportion of the gas gap inventory is released from the fuel as a result of the accident.

In addition to its primary role in limiting the release of activity from site the containment may be required to fulfil the following functions:

1. Provide a means of collection of coolant for re-use following LOCA.
2. Protect the reactor, primary circuit and other vital plant against hazards such as aircraft crash, gas cloud explosions, missiles e.g. generated by turbo-generator disintegration (see Annexes III and IV). It is not however, considered necessary for the containment to maintain the design leakage rate following such a fault.

Some form of cooling system shall be provided to enable the pressure in the primary containment to be reduced as rapidly as possible.

3. PRINCIPAL DESIGN REQUIREMENTS

Arising from the foregoing the following requirements shall be met:

1. The secondary containment structure surrounding the primary containment and the ventilation plant associated with this shall be capable of preventing an unacceptable leakage of activity to the environment under both normal operating and worst credible accident conditions.
2. The discharge of ventilation air from the space between the primary containment and the building shall be through a clean-up plant and stack so arranged that the release limits given in Annex V and Annex XIX are met.
3. Small releases of activity from within the turbine house should be controlled to acceptable levels by discharging through appropriate filtration plant if necessary.
4. The containment and associated cooling and clean-up systems shall, in general, be designed in accordance with requirements suitably adapted from the following:
  - (i) NRC Rules and Regulations Title 10 Part 50 Appendix A.
  - (ii) ANS 7.60 "Standards for Containment Leakage Rate Testing".
5. The design leak rate from the primary containment at full design pressure shall be such that the radioactive release criteria are not exceeded, but in any case a maximum rate of 0.1% of the containment volume per day should be taken as a design target.
6. The primary containment structure including access locks and penetration closures should be designed to withstand with a margin the maximum pressure and temperature conditions arising from any credible LOCA without exceeding design leakage rate. The proposed safety margin between design and calculated conditions shall be discussed with the Engineer. The margin should take due account of the uncertainty which exists in the prediction of containment conditions and the response of the containment and other structures following LOCA. In assessing the adequacy of the margin it should be assumed that the emergency cooling is the minimum consistent with the basic reliability requirements and the resulting metal/water reaction heat shall be taken into account.
7. The design should include measures to ensure that control of any hydrogen release as a result of fault conditions, including the effect of degraded emergency cooling, will be adequate to prevent the possibility of an unacceptable explosion.

8. Primary containment isolation under fault conditions shall be ensured by provision of automatic isolating valves; the detailed arrangements proposed shall be agreed with the Engineer.
9. The containment structure shall be designed so that in conjunction with missile barriers provided within the containment no missile, pipe whip, shock wave, or any other effect arising from any credible fault will cause the design leakage rate to be exceeded.
10. All essential systems and components within the primary containment shall be so designed or protected that neither their operation nor that of the containment shall be jeopardised by the pressure, temperature, humidity and radiation conditions nor by missiles, pipe whip or any other effect caused by any credible accident.
11. The containment structure shall be so designed that it meets the requirements for protection of plant within the containment set down in Annexes III and IV.
12. The reliability of the containment and containment cooling, filtration and ventilation systems should be consistent with the requirements of Annex V and IX. In practice it is anticipated that if the standards of design, construction and testing are in accordance with the foregoing the containment structure reliability will be such that it can be assumed to fulfil its role. However, particular attention shall be paid to the reliability of penetration closures including air locks, pipes and valves, cables and removable closures.
13. Adequate instruments shall be provided for remote monitoring of environmental conditions including pressure, temperature and toxic materials in the atmosphere within the primary containment, both in normal operation and following any credible accident. Facilities shall be provided to monitor the condition of all essential plant and consideration should be given to the feasibility of providing television equipment for remote visual inspection of plant following any credible accident.

#### 4. REQUIRED HAZARD ASSESSMENTS

The following hazard assessments will be required taking into account the expected containment, ventilation and filtration plant performance and making appropriate assumptions with regard to leakage rate, plate-out factors, filter efficiency, plume behaviour etc.

1. Estimates of doses to station staff and members of the public resulting from the worst credible accident of each type.

2. Estimates of doses to members of the public following a (Design Basis) guillotine fracture of a main loop pipe.
3. The effect of a partial blockage in the fuel array under normal and fault conditions.
4. Assessment of the possibility and if applicable consequences of a molten fuel/coolant interaction accident.
5. Assessment of the consequences of faults deemed to be incredible as required by Annex V.

Dose estimates should be based on "best estimate" calculation methods, data and assumptions wherever possible. Additional estimates should be provided to show the consequences of changes in sensitive aspects and aspects where there are significant uncertainties.

Access to Containment

CONTENTS

1. INTRODUCTION
2. PRIMARY CONTAINMENT
  - 2.1 Requirements Relating to Access under Normal Conditions
  - 2.2 Requirements Relating to Fuel Handling
  - 2.3 Requirements Relating to Access at Shutdown
3. SECONDARY CONTAINMENT
4. ACCESS FOLLOWING ACCIDENTS



## 1. INTRODUCTION

The philosophy to be applied to man access to reactor containments of the form envisaged for PWR is given in this annex. The requirements are given, together with explanatory notes on the reasons for them, for access to both primary and secondary containments under both normal operation and shutdown conditions.

As defined in Annex XII, the primary containment is the pressure bearing containment structure surrounding the reactor and primary circuits; the secondary containment is that part of the reactor building complex surrounding the primary containment, one of whose functions is to collect and route to atmosphere via appropriate plant any leakage from the primary containment.

## 2. PRIMARY CONTAINMENT

### 2.1 Requirements Relating to Access under Normal Conditions

- 2.1.1 The design shall not require the continued presence of personnel in the containment during normal operation. Access for limited periods, by limited numbers of persons, is acceptable for inspection and test purposes and for essential maintenance. The frequency and duration of such access shall be kept to a minimum and is to be agreed with the CEEGB. Access should be possible without the use of respiratory protection and/or airfed suits.

It is considered that the design should not require routine on-load access but that it would not be acceptable to have a design in which access within the containment vessel with the reactor on-load was impossible, irrespective of the circumstances. For example, it would be unreasonable to be compelled to shut the reactor down in order to rectify a minor equipment fault.

Furthermore it is considered that even if only infrequent access is envisaged the environment in the containment should not necessitate respiratory protection or air fed suits which would prolong access times and impede escape in the event of an accident occurring.

- 2.1.2 Access during operation shall only be via appropriate airlocks the design of which shall permit their use for escape under credible accident conditions; appropriate interlock arrangements shall ensure that they cannot be misused. A minimum of three airlocks should be provided (of which a goods access may be one) arranged so that the inner doors of two can always be open during man access. Alternative arrangements may be accepted subject to the agreement of the Engineer. All air locks shall be designed in such a form that unauthorised access to the containment can be readily prevented.

The design of the airlocks shall allow the possibility of escape even under accident conditions, i.e. they shall be operable at the containment pressures which might arise under these conditions. Egress shall be made as easy as practicable with well defined, well lighted and unobstructed routes to the airlocks.

The need to control access to the primary containment on security, as well as radiological safety, grounds is recognised. Some form of locking system preventing unauthorised access, but not interfering with the escape function shall be provided.

It is envisaged that airlocks in at least two different areas will be necessary in order to provide reasonable escape routes and it is also considered that during man access the inner doors of two locks, both of which can be reached reasonably easily by the personnel involved, should always be open.

## 2.2 Requirements Relating to Fuel Handling

- 2.2.1 Irradiated fuel shall be stored external to the containment unless there are overriding technical reasons which prevent compliance with this requirement.

From the foregoing, it will be appreciated that irradiated fuel handling procedures involving access to the containment with the reactor on load are not regarded as acceptable. This precludes any system of storing irradiated fuel within the containment and despatching it for reprocessing between refuelling periods. Storing within the containment but restricting further handling to subsequent off-load periods is also deprecated, since this would increase the work load during down time and also deny day-to-day access to the storage area, both of which lead to increased outage times. Temporary storage as part of the fuelling sequence is acceptable.

- 2.2.2 Equipment used during refuelling periods shall be readily removable from the containment unless it is of such simple design that any maintenance or test work can easily be carried out during normal outage time.

With any off-load refuelling scheme the associated down time should be kept to a minimum. For this reason, if significant maintenance and testing of refuelling equipment may be necessary it is obviously preferable for this to be carried out between refuelling periods rather than during outage time.

However it is accepted that some types of refuelling equipment might be of such simple design that maintenance and testing would be unlikely to add significantly to the unavoidable outage time.

### 2.3 Requirements Relating to Access at Shutdown

Other than for short periods associated with transfer of large items of plant or machinery, the primary containment boundary should be maintained intact when the reactor is shutdown.

It is considered that, since the possibility of major reactor incidents cannot be wholly excluded when the reactor is shutdown, (e.g. inadvertent reactor start-up) and there is also a possibility of fuel handling accidents, it is not acceptable to have a permanently open equipment access during shutdown.

Whilst the CEGB do not wish to unduly complicate the equipment access arrangements, the opening of the equipment access for short periods is only acceptable if it can be demonstrated that the probability of any incident requiring benefit of the containment is sufficiently low, within the times concerned.

It will thus be necessary for the contractor to provide justification of any opening requirements proposed.

### 3. SECONDARY CONTAINMENT

Other than as limited by radiological requirements (Annexes XV and XVI), there shall be free access to the secondary containment at all times. However any accesses provided shall be of a form which do not affect the function of the containment.

It is considered that, for maximum operational flexibility, no restriction must be placed, by its containment function, on access to the secondary containment areas. Access to large areas are, of course, likely to be limited by dose rate or contamination level criteria.

On the assumption that the operation of the secondary containment is principally one of leakage collection, using the technique of discharge from a sub-atmospheric pressure building (the depression being maintained by the discharge plant), the main need is to ensure that access does not so affect the in-leakage rates as to prejudice overall performance. It is considered that, where access is direct to large open areas of the buildings, consideration should be given to the need for interlocked doors on a vestibule area, so as to ensure no possibility of a large direct opening from the containment. On the other hand, where the access is to a limited area, which is itself normally separated from other areas, such arrangements may not be necessary.

In all cases, however, the designer will need to justify the arrangements proposed, on the basis of the ability of the ventilation system provided being able to maintain the appropriate depression and extract under all circumstances which may be reasonably envisaged.

#### 4. ACCESS FOLLOWING ACCIDENTS

Following any accident, there shall be no requirement for access to the primary containment in order to ensure the safety of the reactor in both short and long term. However, following any credible accident there should be no undue limitation on access to any plant, or area, necessary for recovery of reactor operation.

Access to plant, or areas, following an accident may be considered either on safety or economic (reactor recovery) grounds.

Bearing in mind the range of possible accidents and the possible extent of the hazards in the primary containment in the extreme case, it does not seem reasonable to rely on gaining access to the primary containment in order to ensure long term reactor safety. Thus there shall be no requirements for such access, although access may be available after some time.

The economic incentive to re-instate the reactor, on the other hand, dictates the need for fairly free access to all areas, albeit with some relaxation on the normal radiological criteria (e.g. higher allowable dose rates within the overall constraints of Annex XV and increased use of respiratory protection). Thus the design should aim to provide such access after any credible accident.

In the case of the secondary containment, it seems reasonable to assume that access should be available on a fairly short timescale (possibly with relaxed radiological limitations as above) and it may, therefore, be claimed that access will be available, after some time, to essential safety plant. It will be necessary for the contractor to justify such access in terms of need, practicality and provisions to be included.

Design Targets for Doses and Dose Rates

CONTENTS

1. INTRODUCTION
2. DOSES IN NORMAL OPERATION
3. DOSES FOLLOWING ACCIDENTS
4. OCCUPATIONAL DOSE RATES IN NORMAL OPERATION



## 1. INTRODUCTION

The station shall be designed so that it can be operated to ensure that all radiation doses resulting from normal operation and following accidents will be as low as reasonably achievable. Consideration shall be given to the following aspects in the manner subsequently described:-

- (i) Occupational doses and dose rates.
- (ii) Doses to members of the public in normal operation.
- and (iii) Doses to members of the public following accidents.

These design guidelines shall be used to ensure that the layout, access control, shielding, ventilation systems etc., are adequate.

The best practicable methods of calculation shall be used with adequate allowance made for uncertainties in data and calculational methods to ensure that the design targets are not exceeded.

## 2. DOSES IN NORMAL OPERATION

### 2.1 Occupational Doses

The station shall be designed within the following annual target dose limits which are such as would ensure compliance with the dose limits recommended in ICRP26:-

- (i) The maximum individual effective dose equivalent to any member of occupationally exposed staff shall not exceed 1.0 rem (10mSv) per annum.
- (ii) The station collective effective dose equivalent shall not exceed 0.2 man-rem per annum per MW(e) installed. Reasonable year to year averaging can be assumed.
- (iii) The maximum dose equivalent to the lens of the eye of any individual occupationally exposed person shall not exceed 15 rem (0.15 Sv) per annum and to the extremities and skin shall not exceed 50 rem (0.5 Sv) per annum. These limits are set by non-stochastic effects, i.e. there is no detriment from exposures below the limit, but nevertheless active components shall normally be handled and maintained in shielded facilities to minimise whole body exposures and consequently both eye and hand exposures should be low.

The station shall be designed so that it can be operated and maintained within the exposure limits without artificial dose sharing i.e. ex-site staff cannot be used for maintenance solely to reduce exposures to the site staff. Non-artificial dose sharing between site staff of similar occupations is acceptable.

## 2.2 Doses to Members of the Public.

Radiation doses to members of the public 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 to take into account the location and local conditions around the station. The relevant plant shall comply 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) shall not exceed 5 mrem/year, taking into account local occupancy factors and any other station on the site.

Estimated doses to members of the public shall be derived from the above considerations and any other 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, given in para. 8 of "Safety Assessment Principles for Nuclear Power Reactors" published by HM Nuclear Installations Inspectorate.

## 3. DOSES FOLLOWING ACCIDENTS

All reasonably practicable protection features shall be incorporated in the design with the aim of limiting over-exposure following credible reactor accidents or because of plant malfunctions or maloperation.

## 4. OCCUPATIONAL DOSE RATES IN NORMAL OPERATION

The dose equivalent rates, in each part of the controlled area, from external sources should not exceed the values in Table 1.

Table 1 - Design Dose Equivalent Rates in the Controlled Area from External Sources

Access requirement	Design dose equivalent rate (mrem/hr)	
	Mean	Maximum
Continuous ( $>10$ man-hr per week)	0.1	0.5
1-10 man-hr per week	1.0	5.0
$\leq 1$ man-hr per week	10	50
1-10 man-hr per year	100	1000
$\leq 1$ man-hr per year	1000	*

\* Dose rates in excess of 1000 mrem/hr are acceptable providing the exposure time is correspondingly short.

In all cases, however, the requirements of 2.1 are overriding.

Whenever practicable, dose rates to the lens of the eye and to the extremities should not exceed the above values. Higher values shall be justified in terms of the appropriate dose limits and access times.

The above values are for guidance of the designer and following agreement with the Board may, in exceptional circumstances, be exceeded. Outside the controlled area the dose equivalent rate should not exceed 0.1 m rem/hr. The overriding limits for design are the annual limits although every effort should be made to ensure that the dose equivalent rate limits in Table 1 are not exceeded.

When estimating dose equivalent rates all sources shall be considered including core radiation, fission products and activation products.

Exposures from high transients shall be minimised as far as practicable and shall not contribute a significant fraction of normal operational exposure in any case. The plant design shall be such that personnel are not normally exposed to transiently high dose equivalent rates. Transients in areas where frequent or regular access is required shall not be significantly higher than the normal values in those areas.

DSG2

Annex XVI

Control of Contamination in Accessible Areas

CONTENTS

1. INTRODUCTION
2. STATEMENT OF REQUIREMENTS
  - 2.1 General Philosophy
  - 2.2 Ventilation and Control of Airborne Contamination
  - 2.3 Access Routes and Change Rooms
  - 2.4 Decontamination Facilities

## 1. INTRODUCTION

There is no intention, for PWR, to apply significantly different standards of contamination control to those developed for gas-cooled reactors and it should be possible to apply the CEGB Safety Rules (Radiological).

It has been thought worthwhile, however, to clarify the requirements and emphasise certain areas of concern, so as to minimise the possibility of the designers overlooking the necessary principles and requirements.

It must be borne in mind that, although it is possible to define general principles, it is difficult, if not impossible, to define specific contamination zone classifications throughout the station at this early stage. The final classifications will depend on levels of contamination arising in circuits, maintenance detail, plant layouts and practical ventilation schemes. Detailed knowledge of such factors will only become available as the design progresses (and in some cases only after operation) and the provision of suitable design features likely to limit contamination levels to values judged appropriate for any particular area or operation will need to be agreed with the designers over an extended period.

## 2. STATEMENT OF REQUIREMENTS

### 2.1 General Philosophy

The design, layout and proposed method of operation of the reactors and ancillary equipment shall be such as to minimise the possibility of hazards due to radioactive contamination.

All plant or systems containing potentially radioactive fluids shall be designed to limit leakage in normal operation and during maintenance. In particular plant or systems containing high levels of activity, such as primary circuits, shall be designed for minimum practicable leakage using, for example, bellows sealed valves and all welded pipework. In addition full consideration shall be given to the provision of appropriate flushing arrangements so as to minimise contamination problems on maintenance.

The design shall be such as to minimise the size and numbers of areas that may become contaminated and the degree of contamination. Nevertheless, in areas where such contamination may arise the plant design and building layout shall allow adequate control of personnel and minimise the possibility of spread of contamination to other areas by personnel, goods, vehicular traffic or the ventilation and drainage systems.



In areas where airborne and loose surface particulate contamination may occur, including the containment, fuel handling facilities, active plant maintenance facilities, decontamination centre, etc., the arrangement of equipment such as pipes and cables, external plant surfaces, access platform galleries and stairways should be such as to preclude pockets of contamination occurring in normal operation, or following an accident. The design of any lagging or cladding in contamination areas shall take full account of the implications of contamination and, where practicable, shall have non-porous surfaces and be readily decontaminable and non dusting. The general standard of finishes in potential contamination areas shall be such as to facilitate decontamination using normal washing, wiping and vacuuming techniques.

Appropriate installed decontamination facilities, e.g. vacuum cleaners, should be provided, designed on an integrated (station) basis so as to provide the maximum degree of operational standardisation and equipment interchangeability.

The containment buildings, fuel handling buildings, and any other areas containing radioactive plant or material shall be arranged as a (Radiation and Contamination) Controlled Area. Normal personnel access to this area will be controlled by use of turnstiles operated by dose meter holders and control of egress will be by turnstiles operated by installed personnel monitoring systems. It is envisaged that a minimum of 3 access and 6 egress turnstiles will be required.

In general, toilet and eating facilities should not be provided within the controlled area. Where the size of the building and the distance from the main change complex dictate to the contrary toilet facilities may be considered on the clean side of sub-change rooms; in such cases, they should be capable of being locked off.

Contamination zone classifications are defined in the Central Electricity Safety Rules (Radiological) and the station design shall be such as to allow zoning in accordance with these rules without undue restriction on operation.

Unless there is good reason to the contrary, all potential contamination zones should be ventilated by an appropriate active (contaminated) ventilation system.

## 2.2 Ventilation and Control of Airborne Contamination

In areas where airborne contamination may arise and where routine access is required in normal operation, or for maintenance, the plant arrangements and ventilation provisions should be such as to preclude, wherever practical, the need for the use of breathing protection. (The safety rules call for use of breathing protection in contamination zones CIII or CIV, i.e. generally when airborne contamination levels exceed 1/10 of the recommended ICRP occupational derived airborne

concentrations). In order to achieve this maximum use should be made of local containment and where this is not practicable the air flows should be designed to be from the operator to the contamination and thence to the contaminated ventilation system. Full use should be made of provision of local ventilation flow control using part containment or hoods enclosing potential sources of activity.

Special consideration should be given to the ventilation provision in areas of the primary containment where access is envisaged with the reactor on load. It is desirable that access be possible, without breathing protection, at short notice. Continuous ventilation of access areas would, therefore, seem appropriate and an arrangement requiring purging of some or all of the containment atmosphere prior to access should only be considered if there are significant other advantages.

Careful consideration should also be given to the special problem of ventilation above fuel handling and storage ponds and in particular the limitation of the likely enhanced spread of activity when partial or total pond drainage is carried out.

Regardless of any special provision that may be made, general ventilation flows shall be arranged to be into contamination areas from areas of lower contamination level. Appropriate arrangements shall be made to prevent reverse flows of air from high contamination zones both in normal operation and under fault conditions.

As far as station design and layout will permit the active ventilation system should be segregated completely from any non-active ventilation system. Ducts conveying contaminated air should not be routed through uncontaminated areas and all equipment associated with contaminated extract air should be grouped together to ease radiological segregation, shielding, access control during maintenance and filter removal.

Unless otherwise agreed with the CEGB "bag-change" filter systems shall be used - e.g. Vokes Unipak - and filters should be mounted in filter rooms segregated from all other plant. Wherever practicable filters should be combustible.

### 2.3 Access Routes and Change Rooms

A main change room and monitor hall shall be provided at the access to the controlled area for use by all persons working in the controlled area. Local sub change rooms shall then be provided to control the spread of contamination from actual contamination zones within the controlled area.

Permanent sub-change rooms should be provided for all those areas which must be designated for design purposes CI, CII, CIII, or CIV in normal operation and to which frequent access is required, and for those areas which are normally designated contamination zones and which may be designated CIII and CIV under periodic maintenance conditions.

Areas normally designated contamination zones to which infrequent access under CI and CII classification is anticipated and areas which will only become contamination zones during infrequent maintenance conditions may not require permanent sub-change rooms, but services and space shall in this case be provided for setting up temporary sub-change facilities.

Good personnel access to the main change room is required from all designated permanent and temporary sub-change rooms and while this access need not be segregated from other access routes, it should not, in general, be through other working areas, or contamination zones. Other than in exceptional circumstances to be agreed with the CEEB, lifts should not be located in, or open directly onto, contamination zones.

Suitable access routes shall be provided for transfer of equipment from plant areas to the decontamination facility and/or active workshops, and for the transfer of protective clothing between change rooms and the active laundry. Wherever practicable these routes should be within the controlled area and should take account of the need to minimise the spread of contamination outside existing contamination zones.

If ancillary reactor plant is located outside the main complex direct access shall be provided to it from the complex.

Where vehicle loading or unloading facilities are required within or adjacent to the Controlled Area the arrangement shall be such that adequate personnel control can be exercised during load/unload operations; unless designated an emergency exit, at all other times entry or exit shall be physically barred (e.g. by locked doors). Personnel movement between contamination zones and vehicle load/unload facilities should be physically prevented at all times. Consideration should also be given to the need for "airlock" arrangements at loading bays so as to maintain the contamination control and ventilation arrangements.

It is anticipated that permanent sub-change rooms will be required for at least the following areas:

- Containment (one or more, depending on detailed layout)
- Fuel storage pond and flask decontamination

Decontamination centre and contaminated equipment workshop  
Reactor coolant, pond water and effluent treatment plant  
Radio-chemistry facilities  
New fuel preparation and assembly (clean conditions but may have contamination control requirements)

The need for other permanent and any temporary sub-change rooms shall be considered bearing in mind the need for access in normal operation, fault situations and during maintenance. Within the containment temporary facilities may be provided where the provision of a permanent room would create unacceptable compartment pressurisation following a LOCA.

Permanent sub-change rooms shall be sized and equipped (by agreement) on the basis of the necessary duty and personnel through put and in accordance with the Safety Rules.

Where temporary change facilities are to be set up there should be provided a supply of town's main water, a drain connecting to the active drains system and power points for monitoring instruments.

The number of permanent sub-change rooms should be reduced to a minimum by grouping contamination zones together as far as practicable. Also, access to areas which become contaminated during maintenance should, where possible, be capable of being re-routed through an adjacent permanent change facility. Where sequential access is required to a number of areas as part of maintenance procedure, such areas should, if practicable, be served by a common sub-change facility.

Access to Class CIV zones shall be through an airlock. If frequent access is required permanent airlock facilities shall be provided; if access is required only infrequently, space and facilities shall be provided for a temporary airlock.

Breathing air supplies will be required for man access to all Class CIV zones and areas in which there is a toxic hazard and shall be distributed to the required areas by permanent pipes, terminating within, or adjacent to the appropriate sub-change room (not in the CIV zone). Similar arrangements will normally be required for CIII zones. Sufficient spare capacity shall be provided in the system to allow ready extension to other areas.

For all areas in which breathing apparatus may be required, suitable connections shall be provided to permit its use within the appropriate sub-change facility as well as in the actual operations area. Appropriate arrangements are required to allow for passage of air hoses, in use, through doorways between areas, with the doors closed.

#### 2.4 Decontamination Facilities

Decontamination and active maintenance facilities shall be provided within the Controlled Area for the necessary decontamination and/or maintenance of items of plant. The detailed requirements for these facilities should be decided bearing in mind the size, likely contamination level and frequency of maintenance of the various plant items involved. Nevertheless it is clear that various abrasive washing and soaking facilities will be involved with necessary active drains and connections to the active effluent treatment plant.



DSG2

Annex XVII

Radioactive Waste Management



CONTENTS

1. INTRODUCTION
2. PRINCIPAL DESIGN OBJECTIVES
3. DISCHARGE LIMITS
4. GENERAL DESIGN PRINCIPLES
  - 4.1 Gaseous Wastes
  - 4.2 Liquid Wastes
  - 4.3 Solid Wastes

## 1. INTRODUCTION

A co-ordinated, consistent design approach to radioactive liquid, gaseous and solid waste management is required for the power station as a whole. The general design objectives, criteria and principles are outlined below.

## 2. PRINCIPAL DESIGN OBJECTIVES

The following principal design objectives shall be adopted:

- 2.1 To provide safe means for collecting, segregating, storing, processing, sampling and discharging liquid wastes generated during plant operation, maintenance and fault conditions which potentially contain radioactive nuclides.
- 2.2 To provide sufficient processing and control of liquid wastes such that the discharges to the environment in normal and fault conditions do not cause the limits specified in Section 3 below to be exceeded.
- 2.3 To provide safe means for collecting, transferring, sorting, treating, storing and retrieving or despatching from site as appropriate all solid radioactive wastes generated during plant operation and maintenance.
- 2.4 To provide safe means for collecting, processing, sampling and discharging gaseous wastes which potentially contain radioactive material in gaseous, particulate or vapour form.
- 2.5 To provide sufficient containment and processing of gaseous wastes such that the discharges to atmosphere in normal and fault conditions do not cause the limits specified in Section 3 below to be exceeded.

## 3. DISCHARGE LIMITS

The design of the station shall be such as to minimise as far as is reasonably practicable radiation doses received by operating staff and members of the public as a result of radioactive waste management practices at the station.

The radiological design criteria are given in Annex XV and Annex XIX. The liquid and gaseous discharges are controlled by Authorisations issued by the Department of the Environment and the Ministry of Agriculture Fisheries and Food, who will take into account discharges arising from other plant on the site.

The discharge Authorisations are given on the basis of need and the Board is required to reduce its discharges to as low a level as is reasonably achievable. To this end the Board intends to apply the principles of ICRP 26 with regard to cost-benefit in the operation of the station. Until the methodology of applying these principles to the design of waste treatment systems is agreed the station should be designed on the following basis:

- 3.1 Estimated doses to the public derived from the anticipated discharges, together with the contribution of direct radiation from plant and buildings, and other existing sources on the site, should be assessed against the level of 1/30th of the ICRP recommendations for the general public in any year, given in para.8 of Ref.1.
- 3.2 Normal operational transient increases in daily discharges are permitted. However these discharges should be such that, even if they were allowed to continue throughout the whole year, the annual dose equivalent limits to the public recommended in ICRP 26 would not be exceeded in the critical pathway.
- 3.3 Critical pathways for exposure of the public and occupancy factors (where appropriate) should be agreed with the Board.
- 3.4 The discharge Authorisations will be agreed for intended station operation and the designer should include sufficient safety factors (to be agreed with the Board) to allow for data uncertainties and to give operational flexibility.
- 3.5 With regard to liquid waste discharges, notwithstanding Section 3.1, the plant design should be such that, taking into account uncertainties in arisings, an annual discharge for the station of 20 curies (alpha plus beta), excluding tritium, could be achieved in operation if so desired.
- 3.6 Discussions will be held at an early stage of the project to obtain provisional agreement between the Board and the Authorising Departments on the discharge limits. Final Authorisations will be issued towards the end of the construction period when effluent plant design and performance have been examined, and station needs fully established.

#### 4. GENERAL DESIGN PRINCIPLES

The design of all Systems and plant should be such that, consistent with other requirements the generation of radioactive wastes is minimised. In particular, account should be taken of the need to minimise processing of waste products prior to disposal, discharge or storage on site and to minimise the volume of wastes requiring storage.

Care should be taken in the design of all plant to minimise the generation of waste oil contaminated with radioactive nuclides. Provision shall be made for transferring all radioactive waste oil to the Radioactive Waste Building for storage and treatment.

In the design of pipework and ducts associated with waste discharges and transfers, particular attention should be paid to minimising the possibility of deposition or trapping of radioactive material therein.

#### 4.1 Gaseous Wastes

- 4.1.1 All gaseous discharges and ventilation air discharges shall be treated and released to atmosphere in a manner which will reduce the radiological and toxic hazards on and off site to as low a level as is reasonably achievable. In deciding the treatment, the location of discharge points to atmosphere, and in assessing the consequences of these discharges, due account shall be taken of the possibility of abnormal release of activity from fuel into the reactor coolant and of the possibility of abnormal leakages from any part of the plant containing active material. In assessing the consequences of discharges to atmosphere, account shall be taken of prevailing winds, local topography, the effects of building turbulence and the proximity of grazing land for dairy cattle.
- 4.1.2 Means, which take account of variations in discharge flowrate, shall be provided for the routine assessment of all radioactive discharges to the atmosphere and the methods of discharge should be chosen in order to facilitate this requirement (e.g. the number of discharge points should be minimised). In some cases, quantitative assessment of discharges may not be practicable using stack measurements. In such cases effective assessments shall be possible using the results of other process sampling or monitoring in the plant.
- 4.1.3 All gaseous discharges which may contain radioactivity should be released to atmosphere at a high level. Where possible these discharges should be made above roof height to minimise the effects of turbulence in the vicinity of buildings.
- 4.1.4 Means shall be provided for demonstrating the functional performance of all treatment plant.

#### 4.2 Liquid Wastes

- 4.2.1 All liquid discharges which may contain radioactivity shall be treated and released in a manner which will minimise the radiological hazards. The plant shall be so arranged that wherever practicable the discharge of such liquids can be carried out only through the Liquid Waste System to the main cooling water discharge system.
- 4.2.2 The possibility of escape of radioactive liquid to the ground shall be eliminated as far as practicable. Throughout the station all plant, pipes and valves containing active or potentially active liquid should be so arranged that any leakage therefrom will be contained within a small area and will be capable of ready detection. In general 'double containment' should be provided for all radioactive liquids but in most cases rooms can serve as the secondary containment provided they are served by a radioactive waste drainage and collection system. In the case of tanks and structures which normally contain liquids of significant activity (e.g. the irradiated fuel storage pond) facilities for detecting leakage shall be provided. In other cases facilities for inspecting or sampling for leakage shall be provided.

- 4.2.3 Means shall be provided for the routine assessment of all liquid radioactive discharges and the methods of discharge should be chosen in order to facilitate this requirement (e.g. provision of suitable monitoring tanks with means of representative sampling).
- 4.2.4 All active or potentially active liquid wastes, sludges, ion-exchange resins, etc which require treatment, storage or discharge shall be routed to the Radioactive Waste Building via a radioactive waste drainage and collection system.
- 4.2.5 Means shall be provided for demonstrating the functional performance of all treatment plant.
- 4.2.6 It is important that all systems which contain radioactive fluids shall be tested for leakage prior to service and the design should be such as to facilitate this. All pressure vessels and pressurized pipework shall as a minimum be designed and constructed to BS 5500 and BS 3351 respectively, and shall be to the approval of the Board.
- 4.2.7 The possibility of oil entering the Radioactive Waste Drainage and Collection System shall be minimised and provision should be made for trapping such oil and transferring it to the Radioactive Waste Building oil storage tanks.
- 4.2.8 The recommendations of the Atomic Energy Code of Practice on Drainage of Radioactive Areas (AECF 1058) should be taken into account.
- 4.3 Solid Wastes
  - 4.3.1 All solid radioactive wastes accumulated on site shall be stored in a safe, inspectable and retrievable manner. The number of locations of waste stores shall be minimised. In particular, a Radioactive Waste Building shall be provided for all wastes which can readily be transferred to it.
  - 4.3.2 All solid wastes stored on site should be segregated as far as practicable on the basis of physical and chemical form and relative or specific activity. Such segregations are desirable particularly in the cases of ion-exchange resins and sludges to facilitate conditioning and final disposal.
  - 4.3.3 The location of all solid waste stores shall be determined by considerations of capital economy, operational convenience and the need to minimise radiological hazards.



- 4.3.4 The store arrangements shall be such that the risk of releasing radioactive wastes to the environment in normal operation or under fault conditions is reduced to a minimum. Explosion and fire risk should be minimised either by storage in an inert atmosphere, by appropriate segregation of flammable materials, or by other means. All waste stores for combustible or inflammable material which do not rely on an inert atmosphere for fire prevention shall be provided with fire detection and fixed fire fighting equipment. Where practicable waste stores should be sited away from combustible materials.
- 4.3.5 The location, layout and access to all active solid waste stores should be such that the contents may be viewed when required in normal operation and, where applicable, personnel access may be obtained to the stores in case of emergency. Removal of all accumulated waste from all stores shall be practicable.
- 4.3.6 Notwithstanding the fact that waste may be removed during or at the end of station life, it is the Board's intention that all long term storage facilities shall be designed for a minimum period of usage of 50 years.
- 4.3.7 The design of the solid waste facilities shall be based on the following:
- (a) High active solid waste (e.g. irradiated control rods) will be accumulated on site and safely stored until station decommissioning when it will be retrieved for disposal. Earlier retrieval for disposal shall be possible however.
  - (b) Intermediate activity level dry solid wastes will be accumulated and safely stored in a suitable location in the Radioactive Waste Building until they can be safely disposed of by a suitable route. Since a suitable disposal route may not be readily available, the storage facilities may have to be capable of storing arisings until station decommissioning but the facility shall allow the safe and ready retrieval of this waste throughout station life and in particular allow waste stored first to be retrieved first. Similar provision shall be provided for bulky contaminated items of low-intermediate activity for which routine off-site disposal may not currently be available.



- (c) Low - intermediate activity level sludges, ion exchange resins and concentrates are intended to be disposed of off-site after suitable processing. Storage shall be provided for one year's arisings prior to processing. A process plant shall be provided to solidify/encapsulate these wastes into a form compatible with further storage on site, transport and disposal off-site. Storage shall be provided for one year's arisings of the processed waste prior to removal from site.
- (d) Low activity solid wastes will be disposed of routinely offsite. Sufficient plant shall be provided so that the wastes can be sorted to allow suitable wastes to be incinerated in small 'Pup' incinerators and certain other wastes to be volume reduced by compaction before packaging in steel drums. One year's storage shall be provided for the packaged wastes awaiting disposal offsite.
- (e) The processing and packaging requirements for the wastes to be disposed of will depend on the availability of and acceptance criteria for the disposal routes as well as the transport requirements. These aspects shall be agreed with the Board at an early stage.

Reference 1 : "Safety Assessment Principles for Nuclear Power Reactors". Health and Safety Executive - April 1979.

DSG2

Annex XVIII

Criticality Safety Requirements and Recommendations  
for the Design of the Fuel Route

CONTENTS

1. INTRODUCTION
2. SAFETY REQUIREMENTS
  - 2.1 Overall Design Requirements
  - 2.2 Safety by Design
  - 2.3 Safety Margins
  - 2.4 Methods of Ensuring Sub-Criticality
  - 2.5 Conditions to be Considered
  - 2.6 Safety Assessments
  - 2.7 Fuel Irradiation and Enrichment
  - 2.8 Fire Detection and Fire Fighting
  - 2.9 Independent Calculations
  - 2.10 Security
3. SAFETY RECOMMENDATIONS

## 1. INTRODUCTION

This note considers criticality safety on site, external to the reactor core itself. Statements made below come under two headings, "requirements" which are mandatory and "recommendations" which are optional. However, the optional statements shall not be ignored without good reason nor without the agreement of the Engineer.

The purpose of the statements in this note is threefold. Primarily it is aimed at making the risk of accidental criticality at CEGB stations acceptably small. Secondly, it is aimed at relieving the operators, as far as is practicable, from the need to divert their attention from the job in hand to criticality safety. Thirdly, it is aimed at making conditions such that criticality safety can be readily proven with only minimum reliance on subjective arguments regarding credibility of postulated accident conditions.

## 2. SAFETY REQUIREMENTS

### 2.1 Overall Design Requirements

The design aim shall be to prevent the occurrence of criticality external to the reactor core itself.

A safety case based on a claim that the occurrence of criticality in a given area would not result in danger to the operators is unacceptable.

### 2.2 Safety by Design

Safety shall be achieved "by design", i.e. the design shall be such that the possibility of criticality following the occurrence of the worst credible single accident can be discounted.

This requirement has two main aims. First, to reduce the probability of accidental criticality at CEGB stations as much as is reasonably practicable and second, to relieve the Station Staff from the need to provide and rely upon strict administrative controls to ensure safety. The ideal is unlikely to be achieved to the full extent in practice and judgements will have to be made as to the acceptable degrees of complexity and acceptable cost of approaching the ideal in given circumstances. Nevertheless the general aim must be to make it highly unlikely that the operators will want or will be able to carry out unsafe fuel handling operations. To this end, fuel handling operations should be simple, the equipment reliable and suitable interlocks provided.

It is recognised that all safeguards may ultimately rely to some degree on administrative control. It is not intended that the present requirements shall entirely rule out a safety case which includes administrative control provided such control is reliably backed by interlocks. Where interlocks are provided, their integrity shall be compatible with the hazard.

### 2.3 Safety Margins

Safety margins shall be established using the criteria discussed in Section 3.3.

### 2.4 Methods of Ensuring Sub-Criticality

Criticality safety, with the fuel elements themselves in their prescribed configurations, shall not rely on the presence of neutron absorbers unless the absorber is fixed to either the fuel or the structure, e.g. for fuel stored "wet", the presence of dissolved boron in the water shall only be relied upon for safety under infrequent accident conditions. This requirement may be relaxed for certain operations carried out over a limited period of time provided that it can be demonstrated that satisfactory measures have been taken to monitor and maintain the boron levels throughout the operation. An example of such an operation would be the refuelling of the reactor core.

### 2.5 Conditions to be Considered

The fuel shall be shown to be safely sub-critical under normal and under accident conditions. All credible accident conditions shall be considered and, where applicable, these will include:

- (i) The introduction or redistribution of moderators (water, heavy water, oil, etc).
- (ii) Redistribution/compaction of fuel from any cause including those resulting from internal and external site hazards, for example, explosions or earthquakes.
- (iii) The introduction of neutron reflectors.

### 2.6 Safety Assessments

Criticality safety assessments shall be made for:

- (i) all parts of the fuel route, including (if applicable) any area where fuel might be taken in error.
- (ii) all transport containers brought onto or despatched from the site.
- (iii) any transport container not used on a CEBG site but for which the CEBG is responsible (e.g. PIE fuel transfer between Winfrith and Windscale).

In the case of off-site transport containers these shall comply both with CEGB requirements and with IAEA Regulations. Criticality clearance of a transport container by the Department of Transport shall not absolve the CEGB from satisfying itself about the acceptability of the proposals.

## 2.7 Fuel Irradiation and Enrichment

In the safety assessment it shall be assumed that:

- (i) all irradiated fuel is at the burn-up giving maximum reactivity.
- (ii) all fuel elements are of the most reactive type available in quantity on site (for example, safety must not rely on identification of fuel enrichment).
- (iii) there is no burnable poison in the fuel unless all fuel elements are so poisoned and then only with appropriate assurances.

The intention is that the criticality assessment shall be carried out from the outset for fuel of an enrichment which is no less than the maximum value expected to be used in significant quantities during the life of the Station. It is recognised, however, that a few special experimental fuel elements of greater reactivity may be proposed at a later stage in the design for experimental purposes. As is the case with all fuel, criticality safety shall be fully assessed, but provided the special fuel elements are few in number it will not be necessary to assume that all fuel is of that form.

## 2.8 Fire Detection and Fire Fighting

Fire detection equipment and fire fighting equipment will be provided in those parts of the fuel route where fuel is handled or stored dry. The fire fighting equipment shall not be based on the use of water or other efficient moderator (eg foam).

## 2.9 Independent Calculations

Independent checks of criticality calculations, preferably using an independent computer code and using independently acquired data, shall be carried out. The checks shall be carried out for each significantly different geometrical arrangement of fuel which is assumed in the studies, thereby giving confidence that there are no significant errors in the assessment of fuel route safety.

## 2.10 Security

The fuel route shall be secure against unauthorised access.



### 3. SAFETY RECOMMENDATIONS

- 3.1 Water and other moderators in bulk should be excluded from those parts of the fuel route intended to be dry.

Water pipes, rain-water pipes, etc should not pass through fuel stores or through other potential criticality areas. The fuel route should be provided with drains to prevent the build-up of flood water, care being taken to ensure that these cannot themselves become potential sources of water.

Where potential water sources are located close to the fuel route, floor drains should be provided external to the fuel route to divert flood water and access to the fuel route should be banded.

- 3.2 Areas where specific steps are not taken to exclude water from the fuel route should be sub-critical when the fuel is moderated by pure (light) water to the optimum extent credible. By "optimum moderation" is meant water at optimum density and includes non-uniform distributions of water within each fuel "cell". The fuel arrays should either be taken as (i) infinite in extent, or (ii) finite, with full water reflections on all external faces. If more efficient neutron reflectors than water (concrete for example) could be present, then these should be taken into account.

To this end it is recommended that any new-fuel transport containers to be used as storage boxes on site, should themselves be designed to be sub-critical when optimum moderated and stacked in the most reactive, 3-dimensional array. Ideally this array should be assumed to be infinite but, if this is not reasonably practicable, the number of boxes in the array should be at least twice the maximum number carried on one transport vehicle. Additionally, when safety is only demonstrated for a limited number of boxes in a 3-dimensional array, it should be shown that an infinite 2-dimensional array of these boxes is safe. The vertical height of the array should be at least that permitted for normal box storage and neutron reflection from surfaces above and below the array should be assumed.

The safety arguments can be simplified if it is possible to establish sub-criticality under conditions of optimum moderation and, simultaneously, by taking the fuel array to be infinite in extent. Simplification is achieved since a large range of conditions is automatically encompassed and these will not therefore require individual assessment, for example:

- (i) fire fighting with water.
- (ii) flooding.

- (iii) water distribution in receded flood situations.
- (iv) voidage of water near normally flooded fuel as a result of boiling, gas leaks, steam leaks, etc.
- (v) effect of human beings in the vicinity of fuel.
- (vi) effect of hydrogenous packing materials in transport boxes, including their redistribution by melting in a fire.
- (vii) effect of moderation of neutrons by a water reflector.

3.3 The acceptability or otherwise of a given safety margin, in terms of its degree of sub-criticality for a given situation depends on judgements related to:

- (i) the degree of pessimism inherent in the calculative model.
- (ii) the extent to which the computer code has been checked for the conditions under examination.
- (iii) the sensitivity of the predicted degree of sub criticality to basic data uncertainties.

Additionally, for accident conditions:

- (iv) the likelihood of the accident occurring.
- (v) the extent to which it has been established that the geometry under study is the most reactive configuration for that type of accident.

The following expression should be used to demonstrate that a particular calculated value of  $K_{eff}$  is acceptable:

$$K_{eff} + S + 3\sigma \leq L$$

where  $K_{eff}$  is the best estimate calculated value of reactivity.

S is the total systematic error in the calculation and the modelling.

$\sigma$  is the standard deviation of the total random error. (The various terms are added in quadrature).

L is the limit which applies to normal and accident conditions.

A definitive value of L cannot be given for every situation but values of L in excess of 0.95 will not be accepted without a very detailed justification.

- 3.4 Packing materials used in quantity in transport boxes should either be non-hydrogenous or should include sufficient neutron absorber to negate the reactivity effect of the hydrogen. The influence of the packing material on criticality safety must be considered in the assessment.
- 3.5 The dry portion of the fuel route should be sited above possible flood levels.
- 3.6 Fuel stores should not be used for storage of other components.
- 3.7 The fuel route should be constructed of non-inflammable materials.
- 3.8 In assessments for off-site transport containers, which are subject to IAEA Regulations, no reliance should be placed on dissolved neutron poisons even under accident conditions.

DSG2

Annex XIX

Radiological Limits for Accidental Release of Radioactivity  
to the Atmosphere

CONTENTS

1. INTRODUCTION
2. METHOD OF APPLICATION
3. EXPLANATORY NOTES

## 1. INTRODUCTION

- 1.1 This Annex sets out the radiological limits for members of the public for accidental releases of radioactivity to the atmosphere to be adopted in the design of nuclear power stations for the CEGB. It is emphasised that within the limits given here, every effort shall be made to design the reactor and associated systems so that both the frequency of accidents and the resulting releases of radio-activity to the environment are reduced to as low a level as is reasonably achievable.
- 1.2 The limits have been derived with the following main objectives:
  - 1.2.1 Taking into account the magnitude of the radiological consequences of a release to atmosphere and the expected frequency of occurrence of such a release the risk to members of the public must be acceptable.
  - 1.2.2 In the context of small releases with negligible risk public anxiety must not be aroused (e.g. by frequent contamination of foodstuff by radioactive materials).
- 1.3 In practical situations it is inappropriate to lay down absolute limits for dose to members of the public from accidents since by definition these are unplanned events which cannot necessarily be controlled to meet some fixed dose limit. What is practicable and useful is to define a design target relating the likely consequences of identified accidents to their frequency of occurrence.
- 1.4 In 1975 the UK Medical Research Council made recommendations (reference 1) regarding actions to be taken in the event of an accident. They defined an ERL as follows:

"An Emergency Reference Level of dose is the radiation dose below which counter measures are unlikely to be justified. When the dose seems likely to exceed the ERL, counter measures should be undertaken if a substantial reduction of dose is likely to be achieved and if the counter measures can be carried out without undue risk to the community. The counter measures appropriate to doses only moderately in excess of the ERL should be such that they do not involve appreciable risk to the community. Counter measures involving greater hazards should be called for only if radiation exposures would otherwise be considerable".

The MRC gave values of ERL's which were adopted by the CEGB as a basis for guidance to reactor designers. In 1981 the National Radiological Protection Board issued a document (See Reference 2) which recommends upper and lower ERL's of dose separately for evacuation, sheltering and distribution of iodine tablets. The lower ERL's for evacuation correspond to the 1975 MRC values and these are the ERL values used in these Design Safety Guidelines (See Table 1).



TABLE 1:- ERLs to be used for purposes of assessment

Organ	Dose	
	(rem)	(Sv)
Whole body	10	0.1
Thyroid, lung or other single organs	30	0.3
Skin	100	1.0

- 1.5 The limit of  $10^{-4}$  p.a. given in Annex V for accidents leading to doses of about 1 ERL is considered acceptable on the grounds of overall risk to individual members of the public while at the same time it is likely to limit to an acceptably low number the number of occasions on which counter measures such as evacuation might be expected to be necessary. The Design Safety Criteria for CECB Power Stations also define acceptable higher frequencies for releases giving rise to lower doses. An additional aspect to be taken into account relates to the action(s) to be followed in the event of food-stuffs being contaminated. Here the Board considers that restriction of the consumption of such foodstuffs might occur if the dose that would otherwise be incurred exceeded the ERL/100 value. The Board considers that, as a design aim, the frequency of such events should not exceed  $10^{-2}$  year<sup>-1</sup> per reactor.

Table 2 below, incorporates the Board's requirements consequent upon these considerations.

Table 2: Guidelines for Accidental Releases of Radioactivity

Dose Band	Releases giving rise to doses		Total permissible frequency of release per reactor (year <sup>-1</sup> )
	greater than	up to	
1	$\frac{\text{ERL}}{1000}$	$\frac{\text{ERL}}{100}$	$10^{-2}$
2	$\frac{\text{ERL}}{100}$	$\frac{\text{ERL}}{10}$	$10^{-3}$
3	$\frac{\text{ERL}}{10}$	ERL	$10^{-4}$

## 2. METHOD OF APPLICATION

- 2.1 Identify all accidents (in reactor and ancillary plant) which lead to releases of activity to atmosphere and estimate the frequencies of occurrence of the releases (see Annex V).
- 2.2 Using 'best estimate' methods for activity release and behaviour calculations assess the magnitude of the releases to atmosphere and the maximum doses to critical members of the public. It should be assumed that members of the public have access up to the site security fence although an occupancy factor may be claimed for extended accident releases. Any food route dose greater than ERL/100 need not be taken into account.
- 2.3 Each accident can then be ascribed to a 'dose band' (see Table 2).
- 2.4 Sum the individual frequencies of occurrence of each accident in each dose band. The sums should be less than as shown in Table 2 in order to meet the target.
- 2.5 If the targets of Table 2 are not met it will then be necessary to consider reducing the release from certain accidents to their frequency of occurrence or both.

### 3. EXPLANATORY NOTES

- 3.1 The ERL values to be used are listed in Table 1.
- 3.2 It is considered inappropriate to include undue factors of safety in the assessments of activity release and consequences, i.e. 'best estimate' methods should be used. The probability of exceeding the best estimated dose should be compatible with the amount by which the dose may be exceeded.
- 3.3 The frequency limits apply to the sum of all possible releases from a given reactor.
- 3.4 In cases where doses are due to more than one nuclide the total dose shall be assessed (in terms of ERLs) by summing the individual contributions.
- 3.5 The requirements of Annex V should be met for all accidents associated with the reactor system.
- 3.6 If it is not practicable to apply fully the method described in section 2 a simplified approach, based upon demonstrating appropriate releases from single event sequences, may be agreed with the CEGB.

### REFERENCES

- 1. Criteria for controlling radiation doses to the public after accidental escape of radioactive material, Medical Research Council (1975).
- 2. Emergency Reference Levels: Criteria for Limiting Doses to the Public in the Event of Accidental Exposure to Radiation - National Radiological Protection Board ERL 2.

DSG2

Annex XX

Control Instrumentation and Alarm Systems

CONTENTS

1. INTRODUCTION
2. GENERAL SAFETY PRINCIPLES
3. CONTROL, INSTRUMENTATION AND ALARM SYSTEMS
  - 3.1 Design
    - 3.1.1 Essential Control
      - 3.1.1.1 Safety Principles
      - 3.1.1.2 Design Considerations
    - 3.1.2 Instrumentation and Alarms
      - 3.1.2.1 Safety Principles
      - 3.1.2.2 Design Considerations
      - 3.1.2.3 Choice of Parameters
      - 3.1.2.4 Operator Supporting Information
  - 3.2 Quality Assurance
    - 3.2.1 Schedules
    - 3.2.2 Validation
    - 3.2.3 Qualification
  - 3.3 Testing
  - 3.4 Operational Constraint
  - 3.5 Hazards
  - 3.6 Security
4. RECORDS
5. CONTROL ROOMS AND OPERATOR ACTION
  - 5.1 General
    - 5.1.1 Main and Emergency Control Rooms
    - 5.1.2 Local Control
    - 5.1.3 Operator Action
    - 5.1.4 Control Room Design
  - 5.2 Main Control Room
  - 5.3 Emergency Control Room
6. TECHNICAL SUPPORT CENTRE

## APPENDIX

## 1. INTRODUCTION

This Annex sets out the principles involved in the provision of control, instrumentation and alarm systems in nuclear power stations. It also summarises the safety requirements upon the control rooms and upon operator actions.

These requirements are covered in principle in Annexes I to XIX, however, in view of the importance of the man/machine interface in safety arguments it has been deemed desirable to develop them in a single Annex.

## 2. GENERAL SAFETY PRINCIPLES

Instrumentation and alarm systems are installed to inform the operator of conditions in the reactor and associated plant that, in the main, are controlled automatically in a pre-determined manner. The operator is also given control facilities which enable him to affect the working of the automatic systems and of plant items to a greater or lesser extent. The important principle underlying the design of these facilities and the delineation of the role of the operator is that the equipment, together with the Operating Rules, SOI's and Administrative Controls, should provide every opportunity for the promotion of nuclear safety and should reduce as far as possible the chances of it being degraded.

It is a requirement that the safety case does not depend upon operator action for a certain time post trip, but it is acknowledged that there are situations in which appropriate operator action within this time may be beneficial to safety. In these circumstances the design should be such that the total system is tolerant of and allows identification of individual failures of the operator to act correctly so that they may be remedied in an unhurried manner without prejudicing safety.

It is judged that the equipment provided in accordance with this Annex will enable the operator to carry out the actions necessary to maintain safety.

## 3. CONTROL, INSTRUMENTATION AND ALARM SYSTEMS

### 3.1 Design

#### 3.1.1 Essential Control

##### 3.1.1.1 Safety Principles

Essential Control Systems shall be provided:

- (a) to maintain the reactor and other plant within prescribed limits at all times during operation. These limits will be such that it can be shown that no safety hazard will arise should any credible fault occur from any permissible operating regime.



- (b) to maintain the reactor and other plant in a safe state following any credible hazard or incident (including destruction of the MCR)

These systems may be automatic or manual, or a mixture of the two. Automatic systems should meet the reliability and other requirements of Annexes I to XIX. Manual control system hardware should have sufficient reliability for the overall requirements of Annex V to be met, taking into account the permitted claims on operator actions, which are summarised in section 5 below. In the event of failure of an automatic control system, arrangements shall be made as appropriate to permit the manual control necessary to ensure safety.

Some control systems or parts of control systems which primarily provide control during normal operation could also assist in controlling a fault situation. Credit for such systems or parts of systems may be claimed in the safety arguments, but any claim must be fully justified and special measures applied as appropriate to support the claim. It shall be demonstrated that, following any credible malfunction in these systems, the essential control systems are capable of maintaining safety.

#### 3.1.1.2 Design Considerations

The design shall take the following into account:

- (a) Where reasonably practicable the essential control systems shall be so designed that failure tends to put the reactor in a more safe state, without increasing the spurious trip rate unnecessarily.
- (b) The essential control systems and their interlocks should not unnecessarily inhibit minor rearrangements of the normal operating configuration which may improve plant flexibility or performance.
- (c) The instrumentation and alarms provided for operator feedback.

#### Note

The protection system, shut-down system and post trip sequencing logic are included amongst the essential control systems, but are covered by Annexes VI, VII and VIII respectively.

### 3.1.2 Instrumentation and Alarms

#### 3.1.2.1 Safety Principles

Instrumentation, which may include recorders, mimics and computer displays, and alarms shall be provided to serve the following purposes. (Computer displays may also be provided in a supporting role). Each item of equipment provided need not be confined to serving only one purpose.

##### Normal Operation (and Pre-Trip)

- (a) To enable the operator to determine that the plant is being operated within safety constraints which shall be defined in Operating Rules, Identified Operating Instructions or other documents.
- (b) To enable the operator to monitor the status of any essential system that would be required post-trip or following any credible incident.
- (c) To provide early warning as appropriate of the onset of faults prejudicial to safety, including incipient plant failure.
- (d) To detect and provide warning as appropriate of internal or external hazards. See Annexes III and IV for details of the hazards to be considered.
- (e) To enable the operator to perform any appropriate action identified as being necessary for safety.

##### Post Trip

- (f) To provide the operator with a set of indications which is sufficient to provide confirmation that the required safety functions are being performed, to permit assessment of the state of the reactor and of the potential for a breach of one or more barriers to the release of radioactive material.
- (g) To enable the operator to diagnose the trip and determine the implications.
- (h) To enable the operator to monitor the performance of the essential systems and to take corrective action if appropriate.
- (j) To enable the operator to assess the situation after the completion of post trip automatic initiations and take any appropriate action.

- (k) To provide information for use in determining the magnitude of the release of radioactive materials.
- (l) To provide information for continuously assessing the inventory and the potential for release of radioactive materials.

Information should be provided using appropriate means to warn the operator that the plant is operating outside defined constraints and to warn of defined hazards and loss of function or redundancy in an essential system.

#### 3.1.2.2 Design Considerations

The design shall take the following into account:

- (a) Instrumentation shall be selected with regard to the requirements of its duty so as to be suitable in terms of accuracy, stability, range, speed of response and frequency of update. The reliability shall be commensurate with the purpose for which it is required. The need for redundancy shall be determined from a consideration of the requirements of the total system.
- (b) Where it is necessary to use displays whose ambiguity under certain operating conditions could mislead the operator, he shall be provided with information to enable him to resolve the ambiguity.
- (c) Instrumentation identified under 3.1.2.1 shall not be prone to consequential failure in the situations it is claimed for safety to be monitoring. It shall survive and continue to function as long as the information it provides is necessary to the operator for safety.
- (d) Instrumentation and alarms shall be fed from electrical, etc. supplies of adequate quality, tolerances, freedom from interruptions and security. In particular these supplies shall be free from unacceptable interactions with supplies feeding other plant, or the essential control systems.

- (e) Alarms (which may be via computer devices) shall have adequate reliability. Where necessary redundant hardware may be used, but the resultant display shall not mislead or confuse the operator. Wherever practicable failure modes shall be such as will tend to cause the reactor to be put into a more safe state.
- (f) Alarms shall not be capable of being reset by the operator until the initiating parameter has returned to the non-fault condition or value. Operator suppression of alarms shall not be possible.
- (g) The alarm system shall be so designed that the operator is presented with information that he is able to assimilate in the time available to him before he is required to take action.
- (h) Alarm legends and messages should specifically employ the parameter or condition monitored. Where this is not possible the implied relationships that are used should be shown to be true under all credible operating conditions.
- (j) The instrumentation and alarms should provide the operator feedback necessary for efficient safe manual control of the plant.

### 3.1.2.3 Choice of Parameters

In choosing the parameters to be monitored the following shall be taken into account:

- (a) Monitored parameters shall be as direct a measure as practicable of the information fundamentally sought. Where direct measurements are not possible displays should be scaled in terms of the parameter sought.
- (b) The operator shall be provided with appropriate independent means of verifying key information.
- (c) For the monitoring of critical safety parameters the operator shall be provided as appropriate with information which has not been subjected to auctioneering or other processing, in addition to the results of any such processing.

## 3.1.2.4 Operator Supporting Information

The provision of the following is considered necessary.

- (a) A computer display system to assist the operator in the supervision of compliance with operating restrictions and safety related plant constraints.
- (b) A continuously operating display system informing the operator of the status of an agreed set of safety parameters.

## 3.2 Quality Assurance

## 3.2.1 Schedules

For Q.A. purposes all parameters to be monitored, alarmed or manually controlled shall be entered in a comprehensive schedule, and categorised according to the purpose they serve. The categorisation should include the purposes itemised in 3.1.2.1 and should be accompanied by reasons to justify it. The instrumentation and alarms so proposed shall be identified, together with their functional specification including reliability, diversity, redundancy and range. Substantiation shall be provided of their ability to meet their intended purposes.

## 3.2.2 Validation

The adequacy of the proposed instrumentation and alarm system should be demonstrated by a simulation of alarms and indications that would be received following appropriately selected fault sequences to be agreed with the Engineer. Simulation should also be used to confirm the feasibility of any claimed operator actions. The form and degree of the simulation shall be agreed with the Engineer.

## 3.2.3 Qualification

Instrumentation and alarm equipment and control facilities shall be appropriately qualified and shown to be capable of performing their intended duty throughout their claimed lifetime. Selected parameters serving purposes (f) to (l) of 3.1.2.1 shall be monitored by instruments qualified to environmental requirements appropriate to post accident or faulted conditions. These instruments shall have appropriate ranges, so as not to saturate under fault or accident conditions. Where the use of a single extended range instrument would lead to a lack of readability or accuracy during normal operation, both normal and extended range instruments shall be provided.