

# Nuclear safety

HM Nuclear Installations Inspectorate  
safety assessment principles  
for nuclear power reactors



© Crown copyright 1979  
First published 1979  
Third impression 1986



HMSO publications are available from:

**HMSO Publications Centre**

(Mail and telephone orders only)

PO Box 276, London SW8 5DT

Telephone orders 01-622 3316

General enquiries 01-211 5656

(queuing system in operation for both numbers)

**HMSO Bookshops**

49 High Holborn, London, WC1V 6HB 01-211 5656 (Counter service only)

258 Broad Street, Birmingham, B1 2HE 021-643 3757

Southey House, 33 Wine Street, Bristol, BS1 2BQ (0272) 24306/24307

9-21 Princess Street, Manchester, M60 8AS 061-834 7201

80 Chichester Street, Belfast, BT1 4JY (0232) 238451

13a Castle Street, Edinburgh, EH2 3AR 031-225 6333

**HMSO's Accredited Agents**

(see Yellow Pages)

*and through good booksellers*

£3.80 net

ISBN 0 11 883642 0

## **Nuclear safety**

### Safety assessment principles for nuclear power reactors

---

## Contents

---

Introduction	1
1	Fundamental requirements and policy 3
2	Basic principles 4
2.1	Radiological principles 4
2.2	Radioactive waste 5
2.3	Principles in the evaluation of fault conditions and protective systems 5
3	Engineering principles 8
3.1	General principles 8
3.2	Reactor core and fuel 10
3.3	Primary coolant circuits 11
3.4	Reactor heat transport systems 12
3.5	Protection system 13
3.6	Essential services 16
3.7	Containment systems 16
3.8	Fuel and absorber handling 17
3.9	Radiological protection engineering 18
3.10	Radioactive waste management engineering 20
3.11	Analysis of plant faults, transients and abnormal conditions 21
3.12	Operating conditions 23
3.13	Reliability analysis 23
3.14	Layout 24
3.15	External hazards 25
3.16	Decommissioning 26
3.17	Quality assurance 27
Glossary of terms	29

---

## Introduction

---

Under the Nuclear Installations Act 1965 no site (with certain exceptions) may be used for the purpose of installing or operating any nuclear installation in the United Kingdom unless a licence has been granted by the Health and Safety Executive and is in force. Nuclear installation for this purpose has the meaning assigned in Section 1 of the Act. Inspectors are appointed under Section 19 of the Health and Safety at Work Act to assist in the execution of the relevant statutory provisions of which the Nuclear Installations Act 1965 is one. Inspectors therefore have the task of advising on the issue of licences and the attachment to those licences of appropriate conditions.

Exercise of this responsibility depends on and must be preceded by a review of the licensee's proposals which will be presented in the form of a safety report and other supporting information. It is desirable that the Inspectorate should adopt a consistent and uniform approach to this review process; to this end it is necessary to provide a framework which can be used as a reference for judgements that must be made in the evaluation process. The principles set out in this document are intended to form this framework. They are to be used primarily as a basis for the Inspectorate's own safety assessment work at any time from the generic or conceptual stage through development, manufacture, construction and operation to eventual decommissioning of a given reactor and its ancillary plant. In carrying out an assessment it is intended that the assessor should judge the extent to which the safety submission shows that the design of the plant is in conformity with the principles. In this connection it is not expected that this judgment could be made in full at the pre-licensing stage but it should be clear that there will be sufficient information to make the judgement at a later stage of the licensing procedure.

The principles in this document comprise a set of objectives, most of which are required to be met as far as is reasonably practicable, although in a few cases there is a definite requirement, for example to meet a maximum permissible dose. A number of the principles are expressed in quantitative terms, such as those in Sections two and three, and these are intended to give guidance to the NII assessors on the levels at which they can confine their studies to the validity of the estimates submitted to them and need not embark on detailed working aimed at establishing whether further improvements would be legitimately described as reasonably practicable. It is not the intention that these assessment levels should be imposed on designers or operators since this would remove the flexibility which they must have in exercising their duty to reduce risks so far as is reasonably

practicable. The principles represent the NII's present assessment position and the extent to which they are met in a design would be an important factor in any decision on licensing. It is expected that further development and modification of the principles will be necessary as a result of experience, and appropriate revisions will be issued from time to time after due consideration and approval.

The principles are divided into three broad categories. The first comprises a set of fundamental principles upon which the second and third sets are based. The second category contains basic principles and a variety of overall objectives concerning the limitation of the radiological consequences of the operation of a nuclear reactor installation in normal and fault conditions. The third category is mainly concerned with those engineering features upon which the implementation of the basic principles depends. It embraces a wide range of plant design features as well as environmental and operational considerations and includes a set of principles dealing with quality assurance. The scope of the principles is limited specifically to nuclear power reactors and their ancillary plant and the content of each part of the document has been drafted with only that class of installation in mind. They are not intended for use in assessing other classes of nuclear installation such as fuel processing plant or highly active waste stores; consideration is being given to developing a separate set of principles for such installations.

The principles relate only to the radiological hazards. Other conventional hazards are excluded except where they have a direct effect on nuclear safety. Also excluded is any specific consideration of principles related to the siting of nuclear power reactors and associated plant; this aspect is dealt with in other NII documents. Finally, management procedures are not considered other than in the section dealing with Quality Assurance. The fundamental principles and those dealing specifically with radiological protection should be read in conjunction with the Regulations on radiation protection and any associated Codes of Practice issued by the Health and Safety Commission. The present principles are without prejudice to any requirements arising from such Regulations and Codes of Practice.

It is recognised that the principles, or associated definitions and comments, will not cover all issues adequately. In such circumstances special consideration must be given to the issue concerned to determine the Inspectorate's position on what may be a novel situation. Such cases may indicate a need to produce new or revised principles.

The authors of this document welcome comments from recipients and users of the principles. Such comment should be directed to:

HM Chief Inspector  
Nuclear Installations Inspectorate  
Thames House North  
Millbank  
London SW1P 4QL

---

# 1 Fundamental requirements and policy

---

## Introduction

The policy upon which the assessment principles are based takes the form of a requirement that in normal operation it shall be shown in the design safety submission that the recommendations of the International Commission on Radiological Protection (ref 1) and the requirements of the Euratom Directive on radiation protection standards (ref 2) are followed with regard to radiation exposures to persons on site and to members of the general public.

A similar approach is applied to the limitation of the likelihood and consequences of accidents. It shall be shown that all reasonable steps have been taken to prevent plant failure or plant damage and thus to reduce the chance of accidents occurring and to reduce the consequences of any foreseeable accident should it occur. The more serious the potential consequences, the more onerous will be the task of demonstrating that further precautions are not reasonably practicable. Thus there is a relationship between the seriousness of the potential consequences and the degree to which it will be regarded as reasonable to prevent faults or damage occurring and to require protective measures to be extended. Design, construction and operation are the key features in the safety of a plant. A sound design concept, a well-engineered and proven design, and high quality construction will be required. A high standard of operation based upon carefully prepared operating rules is a further essential line of defence.

## Fundamental principles

In carrying out an assessment, the assessor should judge the extent to which the submission shows conformity with the fundamental principles of radiological protection, the main features of which are

- 1 No person shall receive doses in excess of the appropriate dose equivalent limit as a result of normal operation.
- 2 The exposure of persons shall be kept as low as is reasonably practicable.
- 3 Having regard to principle 2, the collective dose equivalent to operators and to the general public as a result of operation of the nuclear installation shall be kept as low as is reasonably practicable.
- 4 All reasonably practicable steps shall be taken to prevent accidents.
- 5 All reasonably practicable steps shall be taken to minimise the radiological consequences of any accident.

## References

- 1 International Commission on Radiological Protection, Recommendations of the International Commission on Radiological Protection. Oxford, Pergamon Press, ICRP Publication 26, Ann ICRP 1, no 3 (1977).
- 2 EEC Directive of 1 June 1976 laying down the revised safety standards for the health protection of the general public and workers against the dangers of ionising radiation.

---

## 2 Basic principles

---

### Introduction

The principles set out in paragraphs 6 to 24 comprise a set of objectives relating to the radiological consequences of operating a nuclear installation in normal or fault conditions. They are to be used by the assessor in judging the extent to which the fundamental principles have been satisfied in any particular installation.

These principles are based on experience obtained so far on the operation of commercial plant in the United Kingdom and represent a level of protection against the radiological consequences of normal operation and fault conditions that should in most circumstances prove to be reasonably practicable. It is not a requirement that all the basic principles must be rigidly adhered to although it would be expected that any application for a licence would show good cause for any adverse departure from them.

The manner in which the design meets principles 18 to 24 set out in section 2.2, and 193 to 217 section 3.10, are to be assessed without prejudice to any requirements arising from the application of the Radioactive Substances Act 1960.

---

### 2.1 Radiological principles

---

#### Introduction

Some of the assessment principles in this section, and in subsequent sections as may be appropriate, relate to situations which can be expressed in quantitative terms—e.g. exposure of workers—and which are subject to the general requirement that the risks of exposures should be reduced so far as is reasonably practicable. The nature of this request necessitates the making of decisions by designers and operators on a case-by-case basis, and no generally applicable numerical interpretation is appropriate. However, there comes a point at which further consideration of the case would itself be more costly in resources than any likely benefit. Assessors are therefore given guidance on the levels at which they can confine their studies to the validity of the estimates submitted to them and need not embark on detailed working aimed at establishing whether further improvements would be legitimately described as reasonably practicable. This assessment level should not be taken as a target for designers and operators, whose duties remain those of reducing risks so far as is reasonably practicable, and in any case of meeting any defined limits or requirements.

Where the level achieved is above the assessment level the validity of the designer's argument must be

reviewed. If the level of the risk or exposure achieved by designers is firmly based on good engineering practice, and if proper consideration has been given to the possibility and costs of further reductions, then the level achieved may be accepted by the assessors. If the assessor considers that the case has not been properly made or that the level of risk or exposure is still too high then some improvement will need to be made. On the other hand, even if the level of risk or exposure is already below the assessment level, there is no justification for not including further methods of reducing risks or exposure in certain cases where such methods are readily available and not unduly costly in resources even if the level of risk or exposure is already below the assessment level.

#### Normal operation

6 The dose equivalent or dose equivalent commitment from routine or planned operations received by any occupationally exposed person on site should be no more than one third of any of the appropriate annual dose equivalent limits.

7 The average dose equivalent or dose equivalent commitment from routine or planned operations received by all the occupationally exposed workers on site shall be no more than 1/10 of any of the appropriate annual dose equivalent limits when taken over a calendar year.

8 The dose equivalent received by any person outside the site boundary from all sources originating on the site, including direct radiation and any discharged waste, should in any year be no more than 1/30 of the appropriate dose equivalent limits for the general public.

9 It should be shown that adequate provisions have been made to prevent unnecessary leakage of radioactive material from the plant. The design should be such that in areas where personal protection is not provided the exposure of persons to airborne contamination averaged over 40 hours at work will be no more than 1/10 of the appropriate derived maximum permissible concentration in air.

In addition for normal operation:—

10 Use by the designer of exceptional staff rotation, or introduction of additional staff over and above the normal complement for the station to overcome high dose equivalent rates, should call for special justification.

11 Exposure of persons to dose equivalent rates in excess of those which would be acceptable for continuous working should be kept as infrequent as is reasonably practicable.

12 Surface contamination at any place and on any surface where persons on site normally have access should be controlled to the appropriate derived working limits.

### **Fault conditions**

In judging the extent to which the safety submission shows that the design conforms with principles 13 to 17 it should be noted that where protection is provided these requirements apply only to the situation after operation of the protection, including any failure of the protection. The principles are intended to apply to discrete fault sequences although, as is set out in detail in section 2.3, it is permissible to group faults in appropriate sets in which case the members of the set will be judged against these principles for that release and frequency estimated for the bounding case.

For fault conditions the assessment reference levels are:—

13 The dose equivalents received by the public from direct radiation or release of radioactive material due to accidents arising from a discrete fault sequence which is judged to have a frequency of occurrence greater than once in a reactor lifetime (of about 30 years) should be no more than 1/30 of the appropriate annual dose equivalent limit.

14 The dose equivalents received by the public from direct radiation or release of radioactive material due to accidents arising from a discrete fault sequence which is judged to have a frequency of occurrence less than once in a reactor lifetime but greater than once in a reactor programme (of about 100 reactors) should be no more than the appropriate annual dose equivalent limit.

15 The dose equivalents received by the public from direct radiation or release of radioactive material due to an accident (arising from a discrete fault sequence) which is judged to have a frequency of occurrence less than once in a reactor programme should be no more than the appropriate Emergency Reference Level (ERL).

16 The frequency of any accident arising from a discrete fault sequence which might give rise to a radiation level or a release of radioactive material which could result in a member of the public receiving exposures in excess of the appropriate Emergency Reference Level should be made as remote as is reasonably practicable.

In addition for fault conditions:—

17 As far as is reasonably practicable the exposure of persons on site as a result of an accident should be restricted and exposures above the annual dose equivalent limit for occupationally exposed persons should be avoided.

---

## **2.2 Radioactive waste**

---

18 Exposure of personnel on site and the general public of ionising radiation from any radioactive waste should be kept as low as is reasonably practicable.

19 Having regard to principle 18, the collective dose resulting from radioactive discharges from the site should be kept as low as is reasonably practicable.

20 Solid radioactive waste should not normally be disposed of or otherwise removed from a nuclear site except to an installation or place nominated for the purpose of receiving such wastes.

21 Accumulation or storage of any radioactive waste on site should be in such a manner that in all cases the waste can be readily recovered.

22 All reasonably practicable steps should be taken to minimise the period of time for which wastes containing alpha emitters are accumulated on the reactor site.

23 All reasonably practicable steps should be taken to minimise the period of time for which long lived fission products are accumulated on the reactor site.

24 Accumulations of material containing alpha emitters or long lived fission products on a reactor site should be segregated where practicable from other wastes for separate treatment and accumulation.

---

## **2.3 Principles in the evaluation of fault conditions and protective systems**

---

### **Introduction**

This section of the principles is concerned with the basic assessment procedure to be applied to plant faults or accidents and with the basic principles for evaluating faults and the protective systems provided to control them.

The review process which is the basis of the principles is concerned with discrete fault sequences. In principle all potential fault sequences should be subject to this review process. However, an acceptable alternative is one where sets of sequences having similar characteristics are identified and the bounding case selected to represent the set.

For each discrete fault or bounding case considered, the review process carried out by the assessor should lead clearly to a decision as to the general acceptability of the design measures provided to minimise the contribution to the overall risk from each fault. The basis of the process is that many fault sequences examined in this way can readily be accepted on the grounds of the magnitude of the expected radiological release, standard of protection or quality of the design. A number of more difficult cases would remain which would require special consideration

before safety clearance of the reactor concept could be given.

This special consideration or special case procedure would be expected to lead to a narrowing down of unresolved or difficult aspects of reactor safety philosophy. As cases are examined and a position determined subsequent comparable cases would be resolved more readily by reference to the precedent. Thus in time the main aspect of the special case procedure would be to determine the relevance of the precedents to the case under consideration. With sufficient accumulated experience and precedents the principles will be modified accordingly.

It is recognised that for many components there will be a spectrum of possible defective modes or maloperations associated with a corresponding range of fault consequences and frequencies. However, in considering the credit which can be given to protective systems a simplified approach may be adopted by the assessor in which only two states, success or failure, are recognised. In such cases care must be taken to ensure that intermediate cases do not in fact give greater cause for concern. Should account need to be taken of partial success (or failure) in meeting the principles, the assessor should look for justification of this in the safety submission.

For the purpose of judging the engineering measures adopted in a plant which have a bearing on component or system reliability the Inspectorate's position is that well established engineering technology in the nuclear field forms the basic frame of reference. In many instances it is possible to compare like functions between one reactor and another, though this may not always be possible where different physical processes may be involved. Nevertheless it is not unreasonable to expect that the engineered means of achieving a given end in various circumstances could be compared from the reliability point of view. Thus, that which has already been achieved, coupled with the appropriate principles, constitutes a norm which can be regarded as a practical standard which the Inspectorate takes as a starting point in considering any new proposal.

In carrying out an assessment of fault conditions and protective systems the assessor should judge the extent to which the submission shows conformity with the principles set out in this section.

### Principles

**25** Any fault sequence which, even in the absence of any effective barrier, can be shown to satisfy principles 13 to 17 can be accepted subject to confirmatory assessment. Fault sequences which do not satisfy the conditions of principles 13 to 17 may subsequently be shown to meet those requirements by the provision or existence of additional features not thus far considered in the fault analysis.

**26** Those discrete fault sequences which when considered without the aid of any effective barrier would

be expected to give rise to consequences in excess of the values set out in principles 13 to 17 should be assessed as follows:

- (a) Any discrete fault sequence for which the estimated release is less than that which would lead to the ERL should be shown to be controlled by the presence in the plant of at least one effective barrier which must be capable of reducing the potential release due to the uncontrolled sequence to a value within the limits specified in the principles.
- (b) Any discrete fault sequence for which the estimated release is greater than that which would lead to the ERL and for which the expected frequency of occurrence is less than about once in  $10^3$ - $10^4$  years should be shown to be controlled by the presence in the plant of at least one effective barrier capable of reducing the potential release due to the uncontrolled sequence to a value within the limits specified in the principles.
- (c) Any discrete fault sequence for which the estimated release is greater than that which would lead to the ERL and for which the expected frequency of occurrence is greater than about once in  $10^3$ - $10^4$  years, should be shown to be controlled by the presence in the plant of at least two independent effective barriers, each capable of reducing the potential release due to the uncontrolled sequence to a value within the limits specified in the principles.

The assessor should carry out a review of fault sequences including the operation of effective barriers at each stage in the assessment for the purpose of confirming the adequacy of the provisions made.

### Special case procedure

**27** Where it is not practicable to meet principles 25 and 26 the plant cannot be accepted without special consideration of the relevant issues. In such circumstances a special examination of the relevant scientific and technical factors must be carried out by the Inspectorate. The objective of such an examination would be to judge whether and under what conditions the risk associated with the particular uncertainties could be accepted. Any special consideration of safety issues conducted under the provisions of this principle should take full account of the precedents already accepted under a comparable procedure in the past.

### Rules for the conduct of the basic fault sequence evaluation

**28(i)** As an alternative to considering each foreseeable discrete fault, faults may be grouped in appropriate sets and bounding cases for each set identified. The basis for this selection of bounding cases should involve two factors which are:—

- (a) The relevant physical processes involved, including the likely consequences of each postulated fault sequence; and

- (b) The frequencies with which the particular fault sequences in the set are expected to proceed to a particular end point.

The selection of each bounding case would be made with the expectation that judgments made in respect of the chosen representative case would be applicable with at least the same level of pessimism to all members of the set which it represents. There must be a reasonable demonstration that each selected case is in fact a bounding case of the set that it is related to in terms of both consequences and the frequency ascribed to it. See the principles in Section 3.11

(ii) The assessor should satisfy himself that the range of specified faults used in the safety case is sufficient, having regard to the possible range of all faults.

(iii) The results of the evaluation of each discrete fault sequence or bounding case, comprising physical consequences and frequency of those consequences for each case, should be used by the assessor to develop a diagram showing consequences against frequency taking account of all foreseeable faults. In preparing such a diagram, unless alternative valid data are available, all sequences in sets represented by a bounding case should each be assigned the characteristic of the bounding case. With the aid of this information it should be shown that all reasonable steps have been taken in the design of the plant to avoid a distribution of faults having frequencies or consequences such that their cumulative effect on the overall risk would be significant.

(iv) The following general principles should be applied in making judgments concerning those components of the plant relevant to safety and in particular in relation to those engineered features claimed to be effective barriers. These principles are summarised as follows:—

- (a) Well established and accepted standards applied in the design, construction, operation and maintenance of the safety features of nuclear plant already licensed and in operation form part of the basis for judging the standards required for the reliability of comparable features in any new design. Such comparisons should allow for the relative importance of the features being compared in the plant under consideration. Fault and event tree analysis can be expected to provide a powerful means of conducting this assessment.
- (b) Practical experience with nuclear or other plant should be taken into account in considering the adequacy of design, manufacturing and construction standards set in the interest of achieving reliable and safe performance.

- (c) Advances in science and technology should be taken into account in the evaluation of a new system where the application of such advances is relevant to safety. The assessor should require good cause to be shown in those cases where such advances are not taken advantage of in the design or safety case.
- (d) It should be demonstrated that the standard of design, manufacture or construction of any feature of the plant relevant to safety is to the best reasonably practicable standard.
- (e) It is unlikely that the reliability of those systems comprising any effective barrier could be claimed to be much higher than 1 failure in  $10^4$  demands. The reliability of well proven barriers is expected to be of this order. The requirements of principles 26 and 27 are based upon this assumption.
- (f) No set of engineered safety features can be considered as components of an effective barrier if unfavourable interaction effects between systems during any fault sequence can be foreseen, or if any such safety features can be unfavourably affected by the fault sequence it is intended to protect against.
- (g) Interconnection of barrier elements or sharing of diverse elements is acceptable provided it can be shown that the independent action of each barrier is not thereby prejudiced and that the overall reliability objective can be achieved by such an arrangement.
- (h) Where practical difficulties in achieving a particular objective arise a case for concessions should be made in the safety submission.
- (j) Established standards can, as indicated in (a) above, be accepted as a valid basis for judging effective barriers. However, should the potential radioactive release or increased radiation level be significantly greater than that anticipated for the reactor system to which the established standards relate, that basis may no longer be considered valid. Compensating measures may then be required, the principles for which would need to be considered under the special case procedure outlined in principle 27.
- (v) Where data regarding physical processes or frequency of events are inadequate, best estimate analysis of overall plant behaviour in fault conditions is not possible. In these circumstances credit can only be given in assessment for analysis using such conservative data as can be justified in accordance with the principles in sections 3.11 and 3.13.

---

## 3 Engineering principles

---

### Introduction

Sections 3.1 to 3.16 are concerned with various safety-related aspects of plant engineering. The principles contained in these sections are those engineering principles that would be expected, if met by the design, to lead to a plant which would be consistent with the principles in parts 1 and 2. They are intended to apply to all the safety-related systems and components on a commercial nuclear power station site.

These principles will require interpretation in specific circumstances. Guides are being produced based on experience which will be extended as further experience accumulates in the future. These guides will provide the assessor with detailed interpretation and examples of application of the principles along with such background explanatory material as may be judged necessary.

The adequacy of any measure in design, manufacture, construction or operation or the sufficiency of any analysis of plant condition or performance at any time should be judged by the assessor in the light of the fundamental and basic principles and the extent to which their requirements would be expected to be met. Hence the engineering principles of sections 3.1 to 3.16 represent a set of ideals which should be met as far as is reasonably practicable, that is, the assessor should bear in mind the cost and social implications in relation to the safety benefit of meeting the requirements. In this connection the term 'minimise' is used in these principles to mean 'to reduce to as low a level as is reasonably practicable'.

---

### 3.1 General principles

---

#### Introduction

The principles in this section should be used by the assessor as a basis for considering all aspects of plant engineering from the generic or conceptual stage through development, manufacture, construction and operation to eventual decommissioning.

#### Nuclear plant characteristics

**29** It should be shown that the design is such that its sensitivity to faults is minimised. The expected plant response to any initial fault event can be characterised by one of the alternatives set out in (a) to (d) below. The plant should be designed and operated so that the consequence of any such fault is a sequence as near to the top of this list as can reasonably be achieved.

(a) A failure, malfunction or maloperation should produce no significant operational response in the plant. (It is nevertheless desirable that any failure, malfunction or maloperation should be detected.)

- (b) A failure, malfunction or maloperation should produce a change in the plant state towards a safer operation.
- (c) Following a failure, malfunction or maloperation the plant should be rendered safe by the action of engineered safeguards which are continuously available in the state required to control the fault.
- (d) Following a failure, malfunction or maloperation the plant should be rendered safe by the action of engineered safeguards which need to be brought into service in response to the fault.

**30** It should be shown that the designer has taken into account the need for safety-related structures, systems and components to be designed to be inherently safe or to fail in a safe manner.

#### Nuclear plant design

**31** The plant should be designed and operated in such a manner that no single failure should lead to a radioactive release or the occurrence of any direct radiation in excess of the requirements of principles 13 to 17. Where necessary, appropriate and adequate protection should be shown to be provided for the purpose of achieving this objective.

\*

**33** The best practicable standards of design, manufacture, construction, maintenance and operation should be employed commensurate with the reliability of the plant and its components as required in the interest of safety.

**34** In the design of all safety-related structures, systems and components due allowance should be made for uncertainties in operating and fault conditions, physical data and design methods. The possibility of cumulative damage to the safety-related items during plant life, changes in environmental and operating conditions throughout plant life and changes in or uncertainties regarding the required performance of safety-related items which might arise during plant life, should also be considered. There should be a demonstration that the conservatism in design are consistent with the above factors and the confidence with which they may be quantified.

**35** The reliability claimed for any safety-related structure, system or component should be specified and should be shown to take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data, design methods, etc.

**36** It should be shown that all safety-related items can perform their function to the specified degree of reliability at all times throughout their expected life taking account of the environmental conditions to

\*Principle 32 Blank

which each item is subjected and the loads and other physical conditions imposed upon each item at all times.

37 The best use should be made of diversity, redundancy and segregation in the design of the plant and individual safety-related components, systems or structures.

38 Unauthorised access to and interference with safety-related structures, systems and components should be prevented by suitable measures.

39 Common mode failure rates should be reduced to as low a level as practicable commensurate with reliability requirements by design, diversity and segregation as appropriate.

40 Appropriate provision should be made for the protection of plant personnel so that the necessary personnel are available to maintain safety.

41 In determining the protective requirements in relation to any postulated fault sequence or in considering the likely progress of any postulated fault sequence, credit may be taken for any assured inherent feature of the concept or design which can be expected to act to limit the consequences of that fault sequence.

#### **Protection**

42 The basic objectives in providing protection to ensure nuclear safety in the event of plant faults or possible plant maloperation are:

- (a) to prevent the inadvertent movement of radioactive materials away from their normal point of residence both in normal operation and in abnormal conditions; and
- (b) to preserve intact at all times the necessary number of lines of defence between these radioactive materials and persons in or around the site; and it should be shown that these are met in the design.

43 The design aim should be to prevent any operating mode or fault sequence causing any safety-related item to exceed safe limits. To this end:

- (a) All fault sequences and combinations of fault sequences which might cause a radiation hazard should be identified, representative or bounding faults analysed, and appropriate monitoring and protective systems provided where necessary.
- (b) There should be defined for each safety-related structure, system and component a set of physical conditions for which limits can be laid down, such that when within these limits no unsafe condition would reasonably be expected to occur. Any such set of limits should take account of and relate to all anticipated operating conditions, the accumulated effect of operation and any specified faults.

44 Hazardous events and environmental conditions external to the plant, such as are discussed in section

3.15, should be considered and where appropriate they should be treated both as initiating events of fault sequences or in combination with faults originating in the systems.

#### **Testing, inspection and maintenance**

45 All safety-related structures, systems and components should, where practicable, be capable of being type-tested under conditions at least equal to the most severe expected in service.

46 Safety-related structures, systems and components should be capable of being monitored and inspected in service or at intervals throughout plant life commensurate with the expected reliability of each item. In especially difficult circumstances where this cannot be done, it may be acceptable for additional design measures to be taken to compensate for deficiency.

47 It should be shown that the plant and all safety-related structures, systems and components are designed so as to facilitate inspection, testing and maintenance in the interest of preserving the plant in a safe state at all times.

48 Where practicable provision should be made for inservice functional testing of all safety-related systems. Where complete system testing is not practicable the best sub-system tests and closest representation of required service conditions should be employed. It should be possible to carry out these tests without loss of plant protection action.

49 Provision should be made for periodic sampling of material properties where changes in such properties could affect plant safety at any time.

50 It should be shown that attention has been paid in the design to the possible need for repair or replacement of safety-related components during plant life.

51 The expected initial state of the plant should be capable of confirmation by appropriate tests and inspection before the plant service. These results should be used as a basis for evaluating the results of subsequent tests and inspections during plant life.

52 Any test and inspection should be shown to be relevant to those aspects of the physical state or performance of the system, structure or component that have a bearing on the safe state of the plant.

#### **Data used in the design safety case**

53 Where it is reasonable to do so theoretical models should be employed in support or confirmation of the design or alternatively, as a means of describing safety-related conditions in the plant at any time. Such analytical models should be based on sound physical principles. In general the models used should enable a best estimate to be made of processes of interest, any necessary assumptions or approximations being demonstrably such as to bias results in a safe

direction. Analytical models should be tested as a whole or, where this is not practicable, on a modular basis against experiments which are a reasonable analogue of the actual expected plant condition. Where uncertainty exists in the model regarding any physical process or the available input data, conservative assumptions should be employed. Alternative forms of analysis can in some circumstances be accepted in lieu of testing as a means of verifying a proposed analytical model.

54 The data used in design and fault analysis of safety-related aspects of plant performance at all times should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. Where uncertainty in the data exists, a margin in a safe direction should be provided to take account of these uncertainties. Extrapolation from available data should not be accepted without good physical justification.

55 The data base used for plant design etc., as outlined in 54 above, should be reviewed periodically and checked against plant evidence and such new information from other sources as may be relevant.

---

## 3.2 Reactor core and fuel

---

### Introduction

These principles should be read by the assessor as applying to the reactor core as an assembly and to its main elements the fuel and neutron absorbers individually, when the fuel and absorbers are in their normal operational location in the core. For fast reactors breeder assemblies should also be considered.

In order that the assessor may judge that the design is such as to keep the reactor core in a safe state it should be shown that nuclear reactivity and heat generation can be adequately controlled, if necessary by shutting down the reactor, and that heat generated in the core can be removed at a rate which enables the fuel to be kept within prescribed safe limits.

Satisfaction of these requirements depends upon controlling possible changes in core geometry and various physical conditions affecting the nuclear fission process and the maintenance of an adequate supply of coolant. Principles 56 to 72 set out the features requiring consideration in assessment of reactor core integrity.

In carrying out an assessment of the reactor core and fuel the assessor should judge the extent to which the submission shows conformity with the principles set out in this section.

### Design

56 It should be shown that the core design takes account of all operating modes including normal operation, testing, shutdown and fault conditions.

57 The nuclear and thermal design characteristics should be shown to be such as to produce a reactor core which is stable in normal operation and which does not undergo sudden changes of condition outside that range. The stress and strain limits for the core structure and the fuel should be such as to ensure that their arrangement will be adequately maintained at all specified times.

57 The arrangement of the core should be maintained within limits that ensure no unacceptable variations in nuclear reactivity.

59 The arrangement of the core should be maintained within limits which at all specified times enable passage of sufficient coolant to remove heat from the fuel in all parts of the core.

60 It should be shown that means are provided to reduce to a minimum the chance of the occurrence of any obstruction of the coolant flow which could lead to damage to the core as a result of overheating.

61 It should be shown that in the design of the core account has been taken of all identifiable environmental effects such as irradiation, chemical and physical processes, static and dynamic mechanical loads. Thermal distortion and thermally-induced stress, possible variations in manufacture and any other factor which is identified as a safety-related factor, should also be considered.

62 All components of the core should be such that they are mutually compatible and compatible with the remainder of the plant.

63 The incorrect location in the core of any safety-related components such as fuel elements, breeder elements and absorbers should be physically inhibited.

64 The design should be supported by analyses using theoretical models which are designed to account for all safety-related processes affecting the behaviour of the reactor core.

65 Where adequate data and experience are not available, the design of the core should be confirmed by a specified programme of tests for both normal and fault conditions.

66 The core should be designed such that all safety-related conditions can be monitored to an adequate degree of accuracy.

67 The loss from, or addition to, the core of any component or any movement of any component within it should be prevented by design, where such a change could lead to an increase in nuclear reactivity or a reduction in coolant flow such as to cause a fault condition. All changes in core configuration which could increase reactivity or reduce coolant flow should be carried out only in a controlled and demonstrably safe manner.

68 Where changes of condition or state of components within the core, such as temperature changes or

coolant voiding, can adversely affect core reactivity, precautions should be taken in design and operation to avoid or minimise the effect of such changes by the use of adequate design margins and limitation of operating conditions.

69 With an appropriate margin for uncertainty, no movable fissile assembly or absorber when added to or removed from the core should increase the nuclear reactivity by an amount greater than the shutdown margin that has been assumed to be available taking account of all these principles.

70 The core should be securely supported and positively located with respect to other components in the reactor having a functional relationship with it. Gross movements of the structure of the core or adverse internal movements which might, in the absence of adequate restraint, occur at any specified time should be prevented by design.

#### Operation

71 The design should be such that all fuel, including that which does not conform to the standards laid down for its safe condition under normal and fault conditions, can be removed from the reactor.

#### Monitoring

72 Programmes should be established to monitor fuel behaviour and performance both in and external to the reactor. The purpose of such monitoring should be to:

- (a) Confirm the design safety assumptions.
- (b) Detect malfunctions, failures, etc., of fuel which could present a potential hazard.

---

### 3.3 Primary coolant circuits

---

#### Introduction

The primary coolant circuit is that part of the reactor plant in which the reactor coolant is contained and circulates. The coolant may be any fluid and may or may not be maintained at a pressure significantly above atmospheric pressure. The primary coolant circuit includes all vessels, ducts and other components such as closures, stand pipes for fuel insertion, penetrations for plant components etc. Where ancillary circuits or systems are provided the primary circuit may be assumed to terminate at an isolating valve or similar device. Where steam is generated in the primary circuit and supplied to turbines as the main power output of the plant the primary circuit may similarly be assumed to terminate at suitably effective isolation valves.

The main function of the primary circuit is to retain the reactor primary coolant and to provide defined coolant flow routes to and from the reactor core. It

may also provide structural support and a means of location for other reactor components and it may be required to provide a means of restricting releases of radioactive material in normal and reactor fault conditions. Attachments to the primary pressure circuit need not be considered in the assessment except insofar as they affect at any time the integrity of the primary pressure circuit or any other safety-related feature.

In carrying out an assessment of the primary coolant circuit the assessor should judge the extent to which the submission shows conformity with the principles set out in this section.

#### General safety

73 The primary circuit should be designed, manufactured, constructed and operated so that at all specified times adequate margins are available such that any failure, maloperation or malfunction of the reactor plant which could affect the primary circuit will not prejudice its required integrity or its leak tightness.

74 The design should be conservative and should satisfy the requirements of appropriate and accepted codes or standards. Where departures from forms of construction covered in such codes are proposed, it should be demonstrated by sound analytical methods, experimental evidence or relevant past experience, that the proposed departures do not reduce the design standards.

75 The codes, standards and conventions used as the basis of design should be stated. Any exceptions or qualifications in the application of such codes, standards or conventions should be stated and justified.

76 The design, manufacture and construction should employ proven techniques and it should be possible to conduct such analyses of the design as may be necessary for the purpose of demonstrating adequate integrity at any specified time throughout plant life.

77 The design should be confirmed with the aid of the best appropriate analytical procedures. This analysis should take account of all factors which influence primary circuit integrity at all specified times. Derivation of static and variable stress and strain and the prediction of safe component life, taking account of time dependent material properties, should form an essential feature of such analysis.

78 Every effort should be made in the design, manufacture, construction and operation to avoid the occurrence of defects in the structure. Analyses should be provided to demonstrate that at any specified time in the life of the plant:

- (a) an adequate margin exists between the capability of defect detecting equipment and dangerous defects; and
- (b) where defects are detected they can be accepted or an adequate repair made.

79 The design should be such that the importance of defects as a cause of potential failure is minimised.

80 All materials employed in the manufacture and construction of the primary circuit should be shown to be suitable in all respects for the purpose of enabling an adequate design to be constructed, operated, inspected and maintained at all specified times throughout the life of the plant.

81 Having regard to all the factors, referred to in this part, it should be shown that the primary circuit can be operated at all specified times within those limits defined by the safe operating envelope.

82 Means should be available at all specified times to detect, locate and monitor leakage from the primary pressure circuit which could:

- (a) be indicative of a potentially unsafe condition in the primary circuit, or
- (b) give rise to a significant radiological effect.

83 Consideration should have been given in the design to the need for maintenance and repair of the primary circuit and of equipment and components in or associated with it. The need for access and the need to minimise the radiation exposure of persons involved in such maintenance and repair should also have been taken into account.

84 It should be shown that closures and penetrations have been designed to a standard which is appropriate to the consequences of failure and where the consequences are serious diversity should have been employed. Provision should have been made for inspecting, testing and maintaining closure and penetration features during service along with means to ensure that each closure is securely closed and sealed following removal and resealing. The design should be such that it is possible to verify that any closure is secured correctly.

85 Provision should be made in the design to ensure that mechanical closures cannot be unlocked and removed or replaced and relocked when it is unsafe to do so. Provision should be made to ensure that the correct sequence is followed at all specified times.

86 Piping systems which penetrate or form part of the primary pressure circuit should be provided with valves as close to the main primary circuit as practicable, so that any breach in the piping system can be isolated and the pressure circuit integrity maintained.

87 Adequate redundancy and diversity of isolating valves should be provided. They should be capable of being leak-tested and maintained to the required standard. Closures, valves and other such devices essential to the integrity of the primary pressure circuit should be protected against unauthorised operation at all specified times.

---

### 3.4 Reactor heat transport systems

---

#### Introduction

These principles relate to the systems required for removal to a heat sink of heat generated within the reactor at all specified times. The overall objective in the assessment of heat transport systems is to ensure that adequate provision has been made such that at all specified times the possibility of damage to the fuel, which might allow radioactive material to be released from it, is minimised.

In carrying out an assessment of the reactor heat transport systems the assessor should judge the extent to which the submission shows conformity with the principles in this section.

#### System design

88 The various sources of heat to be removed from the reactor under normal or fault conditions should be identified and the uncertainties associated with the magnitude and rate of production of heat estimated in each case. Heat transport systems should be designed so that heat may be removed at an adequate rate from the plant so as to ensure the required integrity or coolable geometry of the fuel at all specified times.

89 Design information regarding such features as the capacity of heat sources, the rate of heat generation, heat transfer and transport processes should be based on valid and relevant sources, having regard to the particular operating conditions and geometry.

90 Provision should be made for removal of the decay heat from the reactor to an adequate heat sink at any specified time throughout the life of the plant irrespective of the availability or otherwise of external resources.

91 Provision should be made to minimise the effect of faults within the plant which may propagate through the heat removal systems and adversely affect the reactor.

\*

93 Possible effects of changes in coolant condition on the nuclear reactivity of the reactor core should be identified in the safety submission. Adequate provision should be made to limit the consequences of any adverse change of this kind either by the provision of appropriate protective systems or by the selection of appropriate reactor core design parameters.

94 Significant loss of primary coolant or any adverse change in heat transport or coolant condition which might lead to an unsafe state should be safeguarded against.

95 Where overheated fuel could cause failure of the primary coolant circuit or where the fuel geometry

\*Principle 92 Blank

could be so changed as to adversely affect the heat transport process it should be shown that adequate provisions have been made in the design to inhibit such a situation or that additional safeguards would be available to maintain the plant in a safe condition and to prevent any release in excess of the requirements of principles 13 to 17.

96 In the case of reactors with liquid primary coolant it should be shown that under all expected operational procedures there is an adequate margin against breakdown of the claimed operating heat transfer regime. The minimum value of this margin should be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.

### Coolant

97 Possible inherent cooling processes such as natural circulation can be given credit in evaluation of the safety submission so long as sound evidence is produced to demonstrate their effectiveness at any specified time in the plant life as regards the adequacy and stability of the inherent heat transfer processes in the fault conditions for which this form of cooling is claimed.

98 A design basis for the coolant should be specified giving basic constituents, limits of impurities and activity levels outside which the plant is not intended to be operated.

99 The composition of the coolant should be such that interaction between it and any non-replaceable safety-related component will not be a limiting factor within the design life of the reactor. Suitable monitoring facilities to meet this requirement should be provided.

100 Provision should be made for a sufficient and reliable supply of reserve coolant, separate from the normal supply, to be available in an adequate time in the event of any significant leakage of primary coolant.

101 It should be shown that adequate provisions have been made in the design to minimise leakage of the reactor coolant and in any case to keep it within specified limits.

102 Safety-related structures and plant should be protected as appropriate from the radiation, thermal and dynamic effects of any specified fault involving the coolant.

103 All coolant leakage should be passed through appropriate filters or treatment plant before being discharged to the environment, and means for providing evidence of the efficiency of this plant should be available as required during the life of the plant. As a general rule such leakage should be regarded as radioactive wastes, for the purpose of control.

104 Where mutually incompatible coolants are used within the plant it should be shown that provision has been made to prevent them mixing and where appropriate to prevent harm to personnel and safety-related structures in the event of their mixing.

105 Facilities for removing and storing the reactor coolant to allow inspection and repair work should be provided where appropriate and reasonably practicable.

106 The design, construction and operation of the plant should be such that the amount of radioactive material in the coolant is kept to a minimum. Facilities should be provided where appropriate to remove radioactive materials from the coolant and coolant circuit.

---

## 3.5 Protection system

---

### Introduction

The principles in this section are concerned with the equipment and systems which are provided to ensure nuclear safety in the event of plant faults or possible plant maloperation and with instrumentation whose failure or maloperation has a nuclear safety significance. Such equipment may be divided into two categories:

- (a) *Protection system.* All equipment or systems which act directly in the event of faults to prevent damage that may lead to the escape of radioactivity, e.g. that equipment provided to:--
  - interlock against unsafe modes of operation;
  - prevent, limit or delay the escape of fission products following a fault;
  - trip the reactor when pre-set limits are exceeded, or when a trip is manually initiated;
  - remove heat from the reactor to a heat sink after reactor shut-down;
  - activate any other safety-related system or equipment;
  - provide power to the protection system.
- (b) *Safety-related instrumentation.* Instrumentation having a significant but indirect effect on nuclear safety e.g. :—
  - control systems whose failure can cause a demand on the protection system;
  - instrumentation used to warn of the onset of hazardous conditions or of conditions requiring manual safety action;
  - instrumentation for monitoring the protection system, reactor and plant variables and parameters;
  - communications equipment for accident conditions;
  - equipment for monitoring abnormal radioactive releases from the site.

In carrying out an assessment of the protection system the assessor should judge the extent to which the

submission shows conformity with the principles in this section. Protective features of emergency cooling systems, essential supplies and containment are also dealt with in principles 88–106, 148–151 and 152–161 respectively and these should be read in conjunction with the principles of this section.

### Principles for the protection system

**107** Adequate protective systems should be provided and, whenever fuel is in the reactor, they should be maintained at a level of readiness adequate to ensure nuclear safety.

**108** The reactor and associated plant should be designed, constructed and operated so that the reactor can always be shutdown and held shutdown in a safe sub-critical state thereafter.

**109** The reactor and associated plant should be designed, constructed and operated so that it can always be adequately cooled.

**110** All those systems which are required to function and provide action in response to any specified fault should be identified in the submission. The aggregate of all such systems comprises a barrier or barriers for that fault.

**111** For each specified fault it should be shown that adequate protection is provided and that such protection is capable of maintaining the plant in a safe state for as long as may be necessary following that fault.

**112** No single failure within the protection system should prevent any protective action achieving its required performance in the presence of any specified fault or external hazard initiating a demand on the protection system.

**113** For the purpose of initiating protection each fault sequence should be detected at the most appropriate point in the sequence and as directly as practicable.

**114** The variables chosen as indicators of each postulated fault condition should be such as to enable the fault to be reliably and unambiguously detected.

**115** The required performance of components, sub-systems and systems should be stated and shown to be adequate for the purpose of providing protection. Limits should be defined outside which components etc., should not be operated and provision should be made to ensure that these limits are not infringed. It should be shown that the overall reliability of the protective system is adequate.

**116** All variables to be used to initiate protective action should be identified and shown to be sufficient for the purpose of protecting the reactor. Appropriate and safe limits for these variables should be specified which are relevant to the state of the plant at any specified time. It should be shown that the protective systems are designed to respond to the appropriate

variables within the above limits and that the resulting performance of the protective system is adequate.

**117** Where a directly related variable cannot be used for the purpose of initiating protective action against a fault, a less directly related variable may be employed. In such cases it should be shown that the variable chosen to initiate protection has a known relationship with the main variable of concern and with the fault being detected. The physical coupling between the measured variable and the fault condition should be as close as practicable.

**118** The final actions of the protection system should be achieved by means such that there is a known and direct relationship with the desired final objective.

**119** Means should be provided to enable the necessary calibration and checks on the functioning of any measuring device used in a protection system to be carried out at appropriate times throughout the life of the plant commensurate with the reliability requirement.

**120** When equipment has more than one function, one of which is to ensure nuclear safety, this equipment should be classed as protection equipment. The protective function should not be jeopardised by the other functions.

**121** It must be recognised that unforeseen plant or protection system faults or maloperations may occur. Protection system design should reflect this aspect by, for example, the provision of reasonably practicable diversity and redundancy, both within each system and in the nature of each input and output.

**122** Diversity of fault detection and protection should be employed where reasonably practicable but where protection system reliability is required to be very high or when there is doubt about the reliability or effectiveness of a non-diverse system diversity should be introduced.

**123** The protection system equipment should be so designed, laid out and sited that, notwithstanding the effect of plant faults, adequate protective action will be available.

**124** The protection system should be automatically initiated. No operator action should be necessary in a timescale of approximately 30 minutes. The design should however be such that an operator can initiate protection system functions and can perform necessary actions to deal with circumstances which might prejudice the maintenance of the plant in a safe state but cannot negate correct protection system action at any time.

**125** Only components having a proven reliability and performance should be selected for use in any protection system.

126 Spurious operation of the protection system should not produce an unacceptable condition in the plant.

127 The minimum amount of operational protection equipment for which reactor operation will be permitted should be specified. Equipment being tested or maintained cannot be claimed as operational where the test or maintenance conditions put the plant into a less safe state.

128 Where a mechanism (including external hazards) can be foreseen which could invalidate more than one redundant or diverse protective function, action or channel, then its probability of occurrence should have an insignificant effect upon the combined reliability claimed for those functions, actions or channels. Additionally this should be applied to those mechanisms which could cause an initiating plant fault and failure of the associated protective functions.

129 Alarms should be provided to give warning that any safety-related system, component or parameter is at a pre-set limit of its acceptable operational state. Where reasonably practicable alarms should be initiated in the event of any unsafe failure of any element of a protective system.

130 Where required on nuclear safety grounds all protection system equipment including pipework and cabling should be segregated from all other equipment and its function clearly indicated. Where interaction or proximity to non-protection equipment or cabling is required each case should be justified. The segregation of equipment and cabling within the protection system should be such as to satisfy principle 128.

131 The design should be such that the means of access to all protection equipment can be physically controlled to limit access to an extent which ensures availability of the minimum amount of operational equipment referred to in principle 127.

### **Instrumentation**

132 Provision should be made in the form of indicating and recording instruments to inform the plant operators at all specified times of the state of those items which have a significant influence on safety and on safety-related aspects of the overall plant state. Such provisions should include devices to give advance warning of unacceptable changes and rates of change and also alarms when set limits are reached. Sufficient information should be made available to the operator at all times to enable an accurate appreciation to be made of the plant state so that all actions necessary in the interest of safety can be taken promptly and effectively. Such instrumentation should as appropriate and where practicable be capable of monitoring, controlling and recording each parameter at all specified times. Provisions made to monitor, record and control the plant should be shown to be

effective at all specified times so far as is necessary for safe operation of the plant.

133 The provision of control, monitoring and recording equipment should include equipment relevant to postulated fault conditions and should be suitable to enable the operator to assess plant state and take necessary control action during such faults.

134 There should be provided a suitable communications system to enable information and instructions to be transmitted between locations and to provide external communications with auxiliary services and such other organisations as may be required.

135 A reliable fire warning system should be provided for all parts of the protection system except where the design precludes a fire hazard.

136 The instrumentation provided to meet the requirements of this part should enable an operator to take all necessary actions from a central control room. Adequate protection against radiation, contamination, toxic hazards and against plant faults should be provided to permit occupancy of the control room under plant fault or accident conditions without personnel being harmed or receiving radiation exposures in excess of the requirement of the radiological principles.

137 Instrumentation and control equipment should be provided at locations other than the main control room to enable the reactor to be manually shut down, maintained in a safe state and effective accident control undertaken should the central control room become inoperable or uninhabitable.

138 The minimum safety-related instrumentation for which reactor operation may be permitted should be specified.

139 All instrumentation should be of the highest quality appropriate to the duty. Evidence should be provided of its satisfactory performance under the worst environmental conditions anticipated.

140 The accuracy, stability, response time and range of all instrumentation should be adequate and appropriate for its required service at all times throughout plant life.

141 All safety-related instrumentation should be supplied from power supplies whose reliability is compatible with the function being performed. In the case of monitoring, warning and communication functions this supply should be non-break.

142 Adequate means should be provided for the testing and calibration of all safety-related instrumentation at any specified time without loss of any essential functions.

### **Special principles for shut down systems**

The above general principles of protection should be

applied by the assessor as appropriate to shutdown systems as should the following principles in addition:

**143** Taking account of appropriate requirements of these principles, the shut down system should be capable of shutting down the reactor and holding it sub-critical with a margin of negative reactivity which should be available at all specified times and which should allow for uncertainties in nuclear characteristics, perturbations in plant state etc.

**144** The design of the reactor should be such that shutdown is not prevented by the other components of the nuclear power plant or by mechanical failure, distortion, corrosion, erosion etc., of plant components or by the physical behaviour of the reactor coolant, during normal operation or any postulated fault condition.

**145** The design of each shutdown system should be such that loss of absorbing material due to physical or chemical changes such as melting, boiling, leaking or mechanical damage is either prevented or is kept within specified limits so as not to lead to an unacceptable loss of shutdown margin.

**146** Retrievable shutdown devices should be capable of being tested and inspected in accordance with the requirements set out in the general principles. Non-retrievable shutdown devices should be capable of being subject to such tests as are practicable in the reactor supplemented by proof and reliability tests in an appropriate facility out of the reactor.

**147** There should be supplied in the submission a design specification for the shutdown devices which should take into account:

- (a) allowances for changes in geometrical configuration due to temperature, irradiation etc.;
- (b) the allowance for variations of neutron absorber concentration due to burnup, diffusion, deposition, corrosion etc.;
- (c) the production of capture or fission products within the absorber assemblies;
- (d) the physical behaviour of the absorber assembly at all times throughout plant life;
- (e) allowance for reactivity changes in the shutdown provision due to physical and chemical changes throughout plant life. At least one long-term shutdown system should not require an external energy source to maintain the reactor in a shutdown state.

---

### **3.6 Essential services**

---

#### **Introduction**

Essential services are all those resources necessary to the maintenance of a safe state in the plant whether in normal or fault conditions. These services may include electricity, gas, water, compressed air, fuel, lubricants

etc. The relative importance of these various services will depend on the class and design of plant considered.

Those essential services which form part of or supply any protective system should be regarded as part of the protection system for assessment purposes. The general principles of protection set out in this section and in section 3.5 apply as appropriate to all such essential services and in carrying out an assessment the assessor should judge the extent to which the submission shows conformity with these principles.

**148** Where a service is obtained from a source external to the nuclear site that service should where practicable also be obtainable from an alternative source on the reactor site. Each such alternative source should have capacity, availability and reliability adequate for the purpose of supplying the essential demands at all specified times for that period which would reasonably be required for full restoration of the normal supply.

**149** Essential services should be designed, manufactured, constructed and capable of operation so that their reliability is not prejudiced by adverse conditions in the normal services to which they are alternatives.

**150** Protection devices provided for essential service components or systems should be limited to those which are necessary and which are consistent with plant requirements. Their possible action should be taken into account in the reliability assessment.

**151** Where sources external to the nuclear site are employed for essential service the same standard of reliability, availability and specification should be shown to apply as is necessary for an on-site source for the purpose of providing adequate protection.

---

### **3.7 Containment systems**

---

#### **Introduction**

These principles apply to all structures, other than the reactor coolant circuit, which are, or may be, sealed for the purpose of containing radioactivity released from a plant under both normal and fault conditions.

Where equipment forming part of a containment system also serves as part of the protection system the assessor should also apply to it the appropriate principles of section 3.5.

In carrying out an assessment of containment systems the assessor should judge the extent to which the submission shows conformity with the principles in this section.

**152** A containment should be provided around the reactor and its primary coolant circuit, unless it can be shown that adequate protection has been achieved by some other means. The containment should ade-

quately contain such radioactive matter as may be released into it as a result of any fault in the reactor plant. Systems should be available to remove heat from the containment such that the adequacy of the containment function is not prejudiced. The general principles for design of protective systems set out elsewhere in these guidelines should be applied, as appropriate, to the containment and its associated systems.

153 Provision should be made, with adequate safeguards being incorporated against a further fault, for making the plant safe following any incident where radioactive matter is released to the containment, by either removing or otherwise dealing with that radioactive material, so that decontamination and post incident re-entry is facilitated.

154 The containment and its associated systems and internal structures should be shown to be capable of withstanding the effect of specified faults, account being taken of pressure, temperature, atmospheric conditions within the containment, impulse loading, missiles, explosions etc., arising from any such fault.

155 The containment should be capable of withstanding the effect of external hazards (as described in section 3.15) so that the safe state of the reactor plant is maintained.

156 The design of the containment and the plant within it should be such as to provide protection in normal operation and during and following specified faults for personnel on site and for the general public.

157 The need for access by personnel to the interior of the containment should be reduced to the minimum that is practicable. Such access facilities as may be provided should be of such a design as to ensure that at all times the containment will perform its safety function adequately if called upon to do so.

158 Where access by personnel to the interior of a containment or other hazardous area is allowed there should be an alternative route for emergency exit. Access to each exit from the containment should be via a sanctuary. In certain circumstances it may be desirable to have isolated sanctuaries where personnel may be protected for the acute period of an accident.

159 The penetration of the containment by pipes carrying radioactive fluids should have been avoided in the design and as far as practicable such extensions of the primary circuit should themselves be contained. Where this is impracticable there should be adequate means of providing protection against radioactive release to the environment through any such pipe.

160 The use of once-through ventilation or cooling systems, or any plant involving the use of open ducts between the containment atmosphere and the environment which must be sealed by isolating valves under accident conditions should be avoided. Where such features cannot be avoided it should be shown that

facilities provided for the isolation of such penetrations are consistent with the required containment duties in all respects and will not prejudice adequate containment performance.

161 Where a useful safety advantage can be shown, the containment may be provided with a pressure relief system. Adequate performance of the containment should be shown to be achieved in the event that any installed relief system operates during or following any postulated fault.

---

### 3.8 Fuel and absorber handling

---

#### Introduction

The principles in this section are concerned with the assessment of any process involving the handling, transport or storage of irradiated or unirradiated fuel or any neutron absorber, whenever those materials are out of their normal location in the reactor core but on the nuclear site.

In carrying out an assessment of fuel and absorber handling the assessor should judge the extent to which the submission shows conformity with the principles in this section.

162 All processes associated with the handling of fuel and absorbers on the reactor site should by appropriate design and operating procedures be such as to provide adequate protection of personnel against radiation.

163 All equipment for moving fuel or absorbers into and out of the reactor, and subsequently to or from storage areas, should be designed, manufactured, constructed and maintained such that:

- (a) the risk of damage to the fuel or absorber assemblies, to containers of such items, or to any part of the reactor is minimised;
- (b) high reliability against equipment failure is ensured;
- (c) the fuel or absorbers can be protected from damage in the event of any fault in the fuel or absorber charge/discharge route or equipment;
- (d) adequate protection is provided against radiation exposures or release of radioactive material in the event of a fault in the fuel or absorber charge/discharge route or equipment.

164 Whenever any machine or plant component is, for the purpose of fuel or absorber charging or discharging, connected to or physically associated with a containment or primary coolant circuit the design, construction and operation should be such that at all specified times the required level of integrity of the containment or primary circuit is maintained.

**165** The quantities and types of fuel and absorber upon which the reactor and handling equipment designs are based should be stated. The location of all fuel material should be recorded and these should be provision for labelling and record-keeping to cover all movements of fuel to and from the site, and during the time it is on the site and in the reactor.

**166** Storage and all processes in the fuel and absorber routes should at all specified times be secure and safe against fire, flooding, criticality, mechanical damage, theft and any environmental effect likely to be prejudicial to the condition of the fuel or absorber.

**167** Provision should be made for inspection and if necessary physical testing of fuel and absorber material prior to insertion into the reactor to verify its integrity and specification.

**168** Provision should be made to ensure that fuel received onto the site and that stored on the site is in a state consistent with the capability of all handling, processing and storage facilities and is maintained in that state. Handling, process and storage facilities should be designed so that abnormal or faulty fuel can at all specified times be safely dealt with as may be required in a suitable facility.

**169** When there is likely to be significant change in reactivity investment as a result of fuel and absorber changes in the core, the replacement sequence should be such as to maintain an adequate reactivity shut down margin.

**170** Where practicable the fuel and absorber handling equipment should be designed to minimise movement of equipment above the reactor and in any case all necessary movements should be such as to minimise the possibility and severity of any impact or other damage to the reactor fuel or absorbers.

**171** All protective devices associated with fuel and absorber handling such as control, instrumentation, interlocks and monitoring equipment should be designed where appropriate in accordance with the protection principles 107 to 142 inclusive.

**172** Containers used for off-site fuel movements should satisfy the appropriate regulations for the safe transport of radioactive materials.

**173** The operational limits of all fuel handling and absorber handling processes or sequences should be specified in the submission.

nuclear plant, to ensure an acceptable level of radiological protection for persons on and off the site at all specified times. As well as a number of general principles against which the assessor should judge the submission this section also includes principles which contain specific numerical requirements. These numerical requirements should not be taken as limits to what is acceptable, rather they are intended as guidance to the assessors as to the levels as which they can confine their studies to the validity of the estimates submitted to them and need not embark on detailed analysis aimed at establishing whether further improvements would be legitimately described as reasonably practicable. They are not to be taken as a target for designers or operators, whose duties remain those of reducing doses so far as it reasonably practicable.

In carrying out an assessment of radiological protection engineering the assessor should judge the extent to which the submission shows conformity with the principles in this section.

### General

**174** Protection of persons against radiation exposure should be achieved by the best reasonably practicable use of distance between sources and people, shielding and limitation of time and exposure.

**175** The safety submission should define radiation and contamination areas within and around the plant. Provisions should be made in the design or operation of the plant for the purposes of control of access, monitoring, limitation of the spread of radioactive contamination and control of direct radiation levels within and outside each area. Where appropriate radiation and contamination areas should be graded according to the anticipated levels of radiation or contamination in each area.

**176** The safety submission should include an evaluation of the expected total annual dose equivalents which might be received by operators, maintenance workers and other workers as a result of operation of the plant. Results should be itemised for each activity making a significant contribution to the total.

For radiological protection in normal operation the assessment levels are:—

**177** Dose rates in areas to which staff who are not classified persons have unrestricted access should be less than  $2.5 \mu\text{Sv/h}$  ( $0.25 \text{ mrem/h}$ ).

**178** Dose rates in areas to which staff who are classified persons have unrestricted access should be less than  $7.5 \mu\text{Sv/h}$  ( $0.75 \text{ mrem/h}$ ).

**179** Access to areas where dose rates exceed  $0.5 \text{ mSv/h}$  ( $50 \text{ mrem/h}$ ) should be prevented by locked doors or similar restrictions with entry subject to permit-to-work or limitation of access procedures.

---

## 3.9 Radiological protection engineering

---

### Introduction

The fundamental and basic principles for radiological protection are set out in Parts 1 and 2. The following principles are concerned with those engineering measures which can be expected, if adopted in any

## Direct radiation

**180** To ensure that all doses are kept as low as reasonably practicable the safety submission should specify a scheme for the limitation of dose equivalent rates to persons working on site and site visitors from normal operation, routine maintenance and inspection. This scheme should include consideration of all parts of the plant to which access may be made. For assessment purposes, the following assessment levels apply to the whole body dose equivalent rates, or the corresponding dose equivalent rates to other organs, from external sources to which persons may be exposed:—

- (a) 25  $\mu\text{Sv/h}$  (2.5 mrem/h) during routine maintenance and inspection;
- (b) 0.5 mSv/h (50 mrem/h) during rectification of likely faults;
- (c) 0.5 mSv/h (50 mrem/h) during access to internal parts of the reactor system for extended periods of maintenance or inspection, which may be necessary once every one or two years;
- (d) 2 mSv/h (200 mrem/h) during access to internal parts of the reactor system for brief periods of maintenance or inspection (lasting a few hours), which may be necessary once every one or two years;
- (e) 2 mSv/h (200 mrem/h) as a result of foreseeable but unlikely faults.

**181** Estimates of dose rates which could arise because of induced activity and build-up of contamination in the plant should normally be based on the maximum conditions expected to occur at any time during the life of the plant. If some lesser condition is used as a basis for the estimates this should be justified.

**182** Special precautions should be taken in the design of shielding and equipment to avoid:—

- (a) the incidence of localised high levels of radiation due to streaming,
- (b) unplanned or uncontrolled movement of shielding,
- (c) installation behind shielding of components requiring regular handling or to which regular access is required, except when such components are sources of radiation of a kind requiring shielding,
- (d) high doses to the extremities of workers during access to and manipulation of radioactive sources; appropriate design features should be incorporated to minimise such extremity doses,
- (e) unplanned or uncontrolled removal from behind shielding of any source which could cause a significant radiological effect when unshielded,
- (f) where liquid is used as a shielding material the loss of such liquid should be prevented by design. Suitable means should be provided for detecting

changes in liquid level and providing an alarm in the event of any unsafe change.

**183** Access to regions behind shielding should be controlled by specific measures such as interlocks, lockable doors and alarms designed to prevent access to any area where a high radiation level exists. Prompt escape by any person from such a high radiation zone should not be inhibited by any feature of the design.

## Contamination by radioactive materials

**184** The design should provide for the control of loose radioactive materials by means of:—

- (a) adequate local containment,
- (b) suitably designed ventilation and atmospheric clean up systems.

**185** The levels of surface and airborne contamination used as the bases for the design of plant containment and ventilation systems so as to minimise the exposure of both classified persons and other persons on site should be specified in the safety submission. As a basis for assessment levels:—

- (a) routine operations which could give rise to airborne contamination above 1/10 of the derived occupational (MPC)<sub>a</sub>40 averaged over 40 hours should be carried out within a suitably sealed or ventilated enclosure; and
- (b) airborne contamination in areas to which persons on site have unrestricted access should be kept below 1/30 of the derived occupational (MPC)<sub>a</sub>40 averaged over 40 hours.

**186** Ventilation of areas and arrangements for personnel access and plant layout should be such as to minimise exposures to airborne contamination.

**187** Manipulation of highly-contaminated articles should be carried out with the appropriate degree of remoteness or where appropriate in sealed enclosures designed to provide protection against the spread of contamination.

**188** Special precautions in the design of the plant should be taken to ensure that appropriate provisions are made for:

- (a) decontamination of areas to which access may be necessary,
- (b) decontamination of articles which may have to be removed from contamination areas,
- (c) ventilation of contamination areas so as to avoid uncontrolled spread of contamination,
- (d) protection of persons entering and working in contamination areas and the prevention of the spread of contamination when persons leave a contamination area,
- (e) monitoring of airborne contamination and a means of alarm when the levels exceed specified limits.

**189** Ventilation systems provided to control and collect radioactive airborne contamination should be designed so that:—

- (a) segregation of clean and contaminated ventilation systems is ensured,
- (b) discharges to the atmosphere are cleaned to an adequately low level by suitable filtration equipment,
- (c) the flow of ventilation air is from spaces where the level of contamination is expected to be low to those where it is expected to be higher.

### **Instrumentation**

**190** The design should include facilities for portable radiation and contamination monitoring which can be made available for use at all times throughout plant life.

**191** Instrumentation should be provided where appropriate to give prompt, reliable and accurate indication of radiation and radioactive contamination levels in operating areas and should be fitted with alarms to indicate significant changes in levels. All such equipment should be capable of providing reliable indications and alarms taking account of the prevailing conditions, such as changes in temperature or humidity, at any specified time.

**192** All installed instrumentation systems, alarms and interlocks for radiological protection should as appropriate be designed to provide adequate protection based on the principles set out in paragraphs 107 to 142.

---

## **3.10 Radioactive waste management engineering**

---

### **Introduction**

Basic principles concerning radioactive waste are set out in paragraphs 18 to 24 inclusive. It is expected that the adoption of such measures would ensure an acceptably low level of exposure to ionising radiation to persons on and off the nuclear site at all specified times. Waste in the form of fission products contained in the fuel is not for the purpose of these principles included in that arising on a reactor site since it is despatched from the site, incorporated in the irradiated fuel. Handling and transport of irradiated fuel on the nuclear site is dealt with in section 3.8

In carrying out an assessment of radioactive waste management engineering the assessor should judge the extent to which the submission shows conformity with the principles in this section.

### **General**

**193** The design should be such that waste can be handled and kept in such a manner as to ensure

adequate protection of persons on site and members of the general public.

**194** The plant itself should be such that waste arising on the site in any form is kept to a minimum.

**195** All sources of waste arising on the site at any specified time should be identified and conservative estimates made of the quantities in terms of volume and radioactive content for each source. The expected form and physical and chemical properties of each type of waste should be stated.

### **Waste storage**

**196** For the purpose of determining appropriate storage, processing and discharge conditions relevant characteristics such as physical properties, specific activity and type of radiation emitted of all wastes expected to arise on the site should be identified and the wastes classified accordingly.

**197** Where waste is to be kept on the nuclear site the design of the plant should be such that:—

- (a) appropriate spaces or areas can be designated and reserved for the purpose;
- (b) unauthorised access to such areas or spaces is prevented;
- (c) waste kept anywhere on the nuclear site is protected from any adverse environmental effects;
- (d) each facility provided for the keeping of waste is suitable having regard to the physical and chemical properties of the waste materials and the radioactive hazard that might be associated with the waste that it is proposed to keep in each location.

**198** All locations and containers where waste is likely to be kept or handled should be clearly identified and marked.

**199** The design of the plant at locations where waste is kept or handled should be such as to permit effective control of any radiation hazard at all specified times.

**200** Means should be provided for:—

- (a) inspecting stored radioactive wastes;
- (b) recording the quantity and type of radioactive wastes placed in stores;
- (c) assessing the volume and activity of waste in each store;
- (d) assessing the storage space remaining available in each store.

**201** It should be demonstrated that the capacity of any location where waste is to be kept is sufficient, with a margin for uncertainty, to permit all waste expected to arise during the life of the plant to be:

- (a) kept on the site indefinitely,
- (b) despatched from the site,

(c) kept for a period and then despatched, as may be appropriate in each instance.

### Handling and transport

202 Waste temporarily kept on a nuclear site should be in such a form and so located that it is readily recoverable.

203 The need to transport and handle waste on the site should be minimised.

204 All operations such as transport, handling and processing of wastes on the site should be arranged so as to take full account of the properties of the waste materials and to provide adequate shielding. Containment to prevent the spread of contamination should also be provided as appropriate.

### Gaseous waste

205 The waste storage capacity and other means of control of discharges of gaseous waste should be such that discharges will be:—

- (a) kept within authorised limits; and
- (b) made in such a manner as to minimise exposure to persons and to the population.

206 Discharges to the atmosphere should take place via controlled routes, which should preferably be terminated by a suitable stack.

207 The design should provide for monitoring or sampling at discharge points as appropriate. Where the expected release could exceed 1/10 of the daily derived working level of release continuous indication should be provided.

### Liquid waste

209 The waste storage capacity and other means of control of discharges of liquid waste should be such that discharges will be:—

- (a) kept within authorised limits, and
- (b) made in such a manner as to minimise exposure to persons and to the population.

209 Liquid waste should only be collected, handled, processed or kept in impervious containment. Secondary containment of sufficient capacity to hold any possible loss of liquid due to failure of the primary container should normally be provided. Provision should be made for collecting and measuring leakages. An alarm should be activated when any loss of liquid from the primary container occurs which is significantly greater than that due to normal operation.

210 Redundant storage should be provided for liquid waste. The design of such facilities should be such that liquid waste likely to be held in store can be safely transferred to an adequate alternative container should the normal container become defective and unsafe.

211 Wet materials such as sludges and solids having a high liquid content should normally be treated as if they were liquid waste.

212 Means should be provided for estimating quantities stored and where appropriate entering and leaving liquid waste storage facilities so that any leakage or other loss may be determined.

213 Specified precautions should be taken in the design to ensure that:

- (a) inadvertent discharge of liquid waste does not occur,
- (b) different waste streams or stored quantities of waste cannot become inadvertently mixed.
- (c) discharge to the environment will only be via routes allocated for the purpose.

### Solid waste

214 Precautions should be taken to ensure that fissile material other than in the form of contamination is segregated from solid waste and handled at all specified times as irradiated or unirradiated fuel as appropriate.

215 Solid waste which might contain, generate or release gases or liquids should be kept in containers with suitable ventilation or sump facilities.

216 Where solid wastes are stored under water, conditions appropriate to the storage of liquid waste should be observed.

217 Low-activity solid waste which can be safely handled manually should be contained in suitable double wrapping or containers for the purpose of controlling dispersal of contamination during transport and storage.

---

## 3.11 The analysis of plant faults, transients and abnormal conditions

---

### Introduction

Section 2.3 sets out general principles to guide the assessor in determining the adequacy of various protective measures aimed at preventing significant radiological effects occurring as a result of any specified fault or abnormal condition.

This section is concerned with the analytical processes involved in discovering, characterising and evaluating postulated fault sequences for any nuclear reactor plant. For the purpose of these principles this process is referred to as fault analysis.

The aim of fault analysis is to estimate in quantitative terms the behaviour of the reactor and associated plant in specified fault conditions, the outcome of such faults and the likelihood of their occurrence.

In carrying out an assessment of faults, transients and abnormal conditions, the assessor should judge the

extent to which the submission shows conformity with the principles in this section.

**218** All sources of radioactive materials within the nuclear plant should be identified and quantified.

**219** A search should have been carried out for routes and mechanisms whereby these sources could yield a radiological hazard. The fault analysis in any safety submission should be based on systematic and detailed studies which span the range of specified discrete faults, including common mode faults, combinations of faults and situations beyond the design basis of the plant. All relevant plant items should be considered together with a range of conditions covering the operation of the plant over its lifetime. The assessor should satisfy himself that the range of specified faults selected by the designer to make the safety case is sufficient having regard to the range of all faults.

**220** Techniques using fault tree or event tree analysis should be regarded as aids in logical evaluation of the fault potential of any plant. Evidence of such analysis should be presented in any safety case and should also be basic tools to be employed where appropriate by an assessor in examining such a case.

**221** The basis of fault analysis, in the form of necessary technical information regarding all relevant features of the nuclear plant and its proposed mode of operation, should be stated.

**222** Fault analysis should include an examination of the plant characteristics from which both the likelihood of the various discrete fault sequences and their consequences should be determined. Detailed quantitative studies should include, where appropriate, studies of transient behaviour of all or part of the plant, including the response of protection systems to the fault. The analysis should take into account the possibility that safety-related items have become inoperative before the fault sequence or become so as a result of it.

**223** The description and analysis of discrete fault sequences and claims regarding their course and termination should be based on relevant valid and demonstrable physical evidence in respect of all events in each discrete fault sequence considered.

**224** Where statistical data are employed as a component in an argument to substantiate a reliability claim, those data should be obtained from a relevant and sufficiently large population. Adequacy of the sample should be judged with regard to the nature of the physical processes involved and the required accuracy of the reliability estimate. The principles in section 3.13 should apply.

**225** Arbitrary statements or claims regarding any fault, fault sequence or set of fault sequences should not be applied or accepted.

**226** Analysis of the behaviour and integrity of the plant and its protection systems provided to intercept

and limit the consequences of faults should contain allowances for margins on performance and reliability of the various safety features commensurate with:—

- (a) the quality of the information available regarding any fault process,
- (b) the importance and uniqueness of the relevant feature to the overall safe course of the fault sequence,
- (c) the consequences of the sequence.

**227** Where practicable the analysis should have been independently checked using different methods and analytical models. Data used in any analysis should be verified.

**228** As far as practicable there should be practical confirmation of plant behaviour in faults, fault sequences, or parts of fault sequences to support and confirm the theoretical studies. When this is not practicable, methods of analysis and theoretical models and computer codes should be validated by appropriate experiment or tests.

**229** Where a safety case is based on the examination of discrete fault sequences which are claimed to be bounding cases evidence should be produced to show that:—

- (a) a comprehensive survey and identification of all foreseeable discrete fault sequences has been considered,
- (b) the groupings of each set and the bounding case for each set of sequences is relevant to the particular condition under examination, and
- (c) interaction between different sets of fault sequences is not significant.

**230** The fault analysis should from time to time be reviewed and where necessary revised so that methods used for the analysis and the theoretical models take account of:—

- (a) changes to the nuclear plant during construction,
- (b) changes to the nuclear plant or its mode of operation during plant life,
- (c) changes due to relevant technical and scientific knowledge concerning plant behaviour and fault potential, and
- (d) changes in data.

**231** The fault analysis should yield information on the behaviour of the nuclear plant during the fault sequences, in particular on:—

- (a) the performance required of the protection system e.g. protective actions and functions such as trips, emergency cooling and containment and of other safety-related items, e.g. instrumentation;
- (b) the margins to failure of safety-related components and the sensitivity of the outcome of an accident as a function of uncertainties in analytical methods, plant data and initial conditions;

- (c) the margins between expected conditions during any plant fault and those conditions which might give rise to a radiological release;
- (d) the likelihood and outcome of each specified fault sequence and the associated uncertainties, to be judged against the principles of part 2 and section 2.3;
- (e) the risk associated with each fault sequence or bounding case, following the requirements of rule (iii) of section 2.3, to be judged against principles 13 to 17.

---

### 3.12 Operating conditions

---

#### Introduction

The state of the nuclear power plant at all specified times must be considered in assessment for the following reasons:—

- (a) to evaluate the consequences of plant operation in terms of the radiation levels to which persons could be exposed and the extent and nature of radioactive waste arising;
- (b) to search for deleterious effects of plant operation on safety-related components which might lead to short term or cumulative damage of such magnitude that the plant safety may be reduced unacceptably;
- (c) to ensure that the conditions in the plant at any specified time are compatible with the assumptions used in the fault analysis.

In carrying out an assessment of the proposed operational conditions associated with a design the assessor should judge the extent to which the submission shows conformity with the principles in this section.

**232** Plant parameters which are relevant to safe operation should be identified. The proposed values of all such parameters at all specified times should be stated along with expected limits on variability as appropriate. The safety case should demonstrate the completeness and relevance of the listed safety-related parameters and of the data relating to each such parameter.

**233** Damage-threshold envelopes should be specified for the reactor and for each safety-related component, structure or system. Each envelope should comprise a set of limits on the values of those safety-related plant parameters which might affect the integrity of the plant or component outside which deterioration or failure might be expected. Such limits should be defined for the plant and components for conditions at any specified time.

**234** Safe-operating envelopes should be specified for the reactor and each safety-related component, structure or system related to the condition of the plant at any specified time. Each envelope should comprise a

set of limits to the values of safety-related plant operating parameters such that the reactor and each component etc., would not be expected, even in the event of a specified fault occurring at any specified time, to be put in a condition outside the relevant damage-threshold envelope.

**235** Where a safety-related item is required to work only in the event of a fault, its safe-operation envelope should be taken to be that combination of plant conditions appropriate to the fault. The safe-operation envelope should be within the damage-threshold of that item at all specified times.

**236** Proposed values of plant parameters should at all specified times be such as to keep them within the safe-operating envelopes with due allowance being made for uncertainties in determining the physical state of the plant.

**237** The limits referred to in 232 and 233 should be set having regard to the expected extremes of plant condition at any specified time. Account should be taken of all relevant combinations of parameter values which are expected. The possibility of both short and longer term or cumulative damage processes should be considered in setting and defining threshold and operating envelopes.

**238** Provisions should be made to ensure that the operator can perform any necessary actions in the event of departure of safety-related items from the agreed operating conditions.

**239** The parameter values defined by the damage threshold and safe-operating envelopes along with the margins allowed for uncertainty etc., should be reviewed and where necessary revised during plant life in the light of:—

- (a) changes to the plant during construction;
- (b) changes to the plant during operation, including design changes, and any deterioration due to the effect of operation;
- (c) changes in the relevant technical and scientific knowledge;
- (d) changes in data;
- (e) revisions to fault analyses.

---

### 3.13 Reliability analysis

---

#### Introduction

Guidance is given in this section on the conduct, presentation and assessment of system or component reliability analysis. Such analysis may be provided in a safety case along with and in support of other evidence relating to the safety of any nuclear plant.

In reviewing reliability analyses, the assessor should judge the extent to which the submission shows conformity with the principles in this section.

**240** Data used in reliability analysis should be shown to be appropriate to the components subject to analysis and the relevant conditions to which those components are subject. The source, sample size, sample elements and their working conditions should be stated. Differences between the sample and the components subject to analysis should be shown either to be unimportant or acceptable with appropriate allowance being made in any extrapolation of the data.

**241** Where insufficient relevant data are available the basis for any quoted component failure rate, distribution or other necessary factor should be stated.

**242** The measures proposed, including quality assurance, whereby the quoted reliability of systems and components will be achieved in practice should be stated. Evidence should be provided to demonstrate the adequacy of any such measures.

**243** All assumptions made in the course of the reliability analysis should be justified and listed with the conclusions.

**244** The following information should be provided for the system or component analysed:—

- (a) drawings and specifications defining the system or component,
- (b) a statement of the intended function of the system or component,
- (c) a statement of the minimum performance of the systems or component required for successful discharge of its function,
- (d) a logical representation of the failure modes of the system or component,
- (e) the relevant system conditions,
- (f) other information needed for an understanding of the system operation.

**245** The testing and maintenance procedures proposed and their time intervals should be stated.

**246** The reliability claimed for any human actions involved—e.g. maintenance—should be based on the complexity of the task, the stress involved and other relevant factors. Repetitive actions should be suitably weighted.

**247** Allowance made in the analysis for the time taken for testing and maintenance of system components should reasonably reflect the tasks involved.

**248** Reliability analyses should, *inter alia*, take account of:—

- (a) the confidence associated with available data;
- (b) possible variation in time of expected failure rates of systems or components;
- (c) testing and maintenance frequency.

**249** Where independent behaviour of components and/or of human operators is assumed, the basis for the assumption should be stated.

**250** A limitation should be placed on the claimed reliability of any system employing redundancy through the use of identical components, measurements or actions. For protection equipment this limitation should be in the range corresponding to one failure per  $10^3$  to  $10^5$  demands, depending on the complexity and novelty of the system.

**251** The reliability of a system should be expressed at a suitable confidence level.

**252** For complex systems the results of the reliability assessment should also be given for subdivisions within the system of such a size as to permit independent verification.

**253** The system reliability should be estimated for the minimum operational system components for which plant operation will be permitted.

**254** For critical components within the system and those for which an assumption of failure rate has had to be made, bounding calculations should be performed, assuming in turn that all such identical components have zero or a specified limiting reliability.

---

### 3.14 Layout

---

#### Introduction

In carrying out an assessment the assessor needs to be satisfied that adequate consideration has been given to the disposition of items of plant and equipment so as to minimise unwanted interaction and the effects of internal and external hazards. The safety submission should also show that the plant will be secure against outside interference.

In carrying out an assessment of plant and site layout the assessor should judge the extent to which the submission shows conformity with the principles in this section.

**255** The licensed site or such part of it as may be agreed shall be enclosed by a suitable fence or barrier and security arrangements shall be provided to prevent unauthorised entry. The grid switching station and emergency water supplies, if located outside this enclosed area, shall be similarly protected.

**256** Entry to the site shall be controlled and shall usually be at one location only but alternative means of access should normally be provided. Such alternative access routes should be suitable for all types of vehicle which may be required on site in the event of an accident occurring on or adjacent to the site.

**257** Safety-related plant and buildings should be located relative to security fencing or barriers and to areas accessible to unescorted visitors such that the risk of unauthorised access or interference is minimised.

258 The layout of the reactor and other safety-related plant should be such as to minimise the effects of external hazards and of any interactions between a failed structure, system or component and other safety-related structures, systems or components.

259 The disposition of the protection system equipment, e.g. engineered safeguard systems, reactor heat removal systems, grid connection and site electrical supplies including associated pipe and cable routes, should be such that no fault or other incident affecting the site (such as are considered in section 3.15), whether originating onsite or offsite, will prevent the safe shutdown and adequate cooling of the reactor and the maintenance of a safe state thereafter.

260 Hazardous materials such as toxic, explosive and flammable materials or processes involving such materials should be separated from each other and, where practicable, from safety-related plant such that any accident to or release of such materials will not prevent safe shutdown and adequate cooling of the reactor and maintenance of a safe state thereafter.

261 Control facilities and instrumentation essential to safety should be provided at locations other than the main control room such that, in the event of any fault or other incident affecting the site, sufficient facilities will always be available and accessible to ensure safe reactor shutdown, adequate heat removal, and maintenance of a safe state thereafter.

262 Station services important to personnel and plant safety such as site communications, fire fighting hydrant mains and water supplies should be designed and routed such that sufficient capability to perform their emergency function will remain after any fault or other incident affecting the site.

263 The layout of buildings and roadways on the site should be such that in the event of any fault or other incident affecting the site:—

- (a) an alternative means of access will be available to plant or controls essential to safety which may require local manual intervention;
- (b) alternative access will be available to all normally manned areas for personnel rescue equipment;
- (c) safe means of escape will be provided from all buildings or plant areas which may be affected by the incident; and
- (d) where practicable, site personnel will be physically protected from direct or indirect effects of the incident.

---

### 3.15 External hazards

---

#### Introduction

This section is concerned with influences originating outside the reactor plant which could have an adverse effect on plant safety. In carrying out an assessment

of external hazards, the assessor should judge the extent to which the safety submission shows conformity with the principles in this section.

#### Abnormal wind loading

264 Evaluation of the effect of abnormal wind loading should include consideration of such loads, not only directly on all safety-related components, but also on other components or parts of the plant which might interact with safety-related components. Evaluation of the effect of wind loading should be based on the best meteorological data on wind velocity and frequency for the location which is available.

265 Abnormal wind loadings should, so far as is reasonable in the light of meteorological evidence, be assumed to occur simultaneously with other adverse meteorological effects such as:—

- (a) accumulated ice deposits on surfaces;
- (b) high rainfall;
- (c) heavy snowfall.

266 Due account should be taken of the effect of plant layout, building size and shape in localising wind loads suffered by various parts of the plant.

267 Any temporary structure or building should either be shown to be suitably designed to resist external effects or be located sufficiently far from the nuclear plant so as not to represent a hazard to the plant should it sustain damage due to wind loading.

#### Seismic effects

268 Two levels of free field ground motions, designated the Safe Shut Down Earthquake (SSE) and the Operating Basis Earthquake (OBE) should be determined for each site.

269 The safe shutdown earthquake should be related to the most severe that might be expected to occur based on the best available seismological data for the location concerned. The operating basis earthquake should be based on the scale of event that would be expected to occur at least once in the lifetime of the plant.

270 The nuclear plant design should be such as to ensure that in the event of the SSE the reactors can be shut down safely and all safety-related structures and plant can be maintained in a safe condition.

271 The design should be such as to ensure that the safety of the reactors, fuel storage and radioactive waste storage facilities will not be impaired in the event of repeated occurrence of ground motions at the site up to the equivalent of the OBE level.

272 Overall evaluation of the effect on the nuclear plant of any particular seismic event should take account of the potential effect of any local, natural, existing or projected man-made geological feature which could add to or modify the effect of an earthquake on the plant. Consideration should also be

given to the possibility of a seismic event including an additional external event such as a flood due, for example, to the failure of a local dam or sea defence, other hydraulic installation or to excessive wave height on local waters which might reasonably be associated with an earthquake or other severe disturbance.

**273** The SSE and the OBE should each be assumed to occur simultaneously with the most adverse normal plant operating conditions at any specified time. Attention should be paid to possible common mode effects.

**274** Consideration of the effect of a seismic event on any plant should include the assumption of a simultaneous effect of that event on any other plant, system or service which may have a bearing on safety.

### **Flood**

**275** A maximum flood level should be defined related to the most severe that might be expected to occur based on the best available data for the location concerned. In estimating the maximum water level account should be taken, as appropriate, of:—

- (a) for coastal sites astronomical tide, storm surge and significant wave height;
- (b) for river and lakeside sites, the maximum expected flood flow based on recorded data or synthesised from appropriate and conservative meteorological data. Where appropriate, account should be taken of wind-generated water disturbances;
- (c) for estuary or tidal river sites the combined effect of tide and flow as outlined in a and b above.

**276** Where the site is below the estimated maximum flood level or where safety-related components are below that level, design features should be provided to prevent any adverse effect on plant safety due to flooding.

**277** Suitable drainage systems should be provided for the collection of water reaching the site from any source including:—

- (a) rainfall;
- (b) flood defence overtopping by waves;
- (c) flood defence leakage;
- (d) spray.

Reasonable simultaneous ingress of water from these sources should be considered.

### **Fire, explosion, missiles etc.**

**278** It should be shown that the nuclear plant is adequately protected from unsafe effects due to any incident in an installation, means of transport or pipeline outside the nuclear site. Projected and planned future developments should, where appropriate, also be considered.

**279** All sources which could give rise to an explosion, fire, toxic or other hazard and which are on the nuclear site should be identified, specified quantitatively and their potential as a source of harm to the nuclear plant estimated.

**280** Where hazardous substances are kept or generated on the nuclear site it should be shown that the nuclear plant is adequately protected against any leakage, failure, explosion, missile or fire which could occur as a result of a postulated incident involving such hazardous substances.

**281** The principles to be applied in ensuring nuclear safety in the presence of hazardous materials should be based on the general and specific principles set out in these guidelines. In particular attention should be paid to:—

- (a) protection of the nuclear plant and personnel;
- (b) segregation and isolation of hazardous substances one from another and from the nuclear plant;
- (c) the necessity for storage in bulk;
- (d) reasonable limitation of the size of bulk storage;
- (e) the provision of monitoring and alarm equipment;
- (f) the provision of appropriate countermeasures for use in emergencies;
- (g) inspection, testing and maintenance of each part of the plant containing a hazardous substance.

### **Aircraft impact**

**282** Protection of the plant against the effect of aircraft impact on the nuclear site should be considered at the design stage. The possibility of aircraft fuel ignition should also be taken into account.

**283** Determination of the need for physical protection should be based on the best available data relating to the frequency and pattern of aircraft crash for a reasonable range of aircraft types. Should physical protection be required a design basis impact should be specified.

**284** Overflying of the site by aircraft at an altitude of less than 2000 feet should be prohibited.

---

## **3.16 Decommissioning**

---

### **Introduction**

The eventual need to keep the reactor and associated plant in a safe state at the end of its operating life, and if possible to restore the site to unrestricted use, has to be borne in mind at the design stage and during operation.

In carrying out an assessment of the provisions for decommissioning the assessor should judge the extent to which the submission shows conformity with the principles in this section.

**285** The design of reactors and associated plant, including radioactive waste facilities and stores, should be such that they can be maintained in a safe condition for as long a period as is necessary following the end of their useful lives.

**286** At the end of their useful lives, complete decommissioning and dismantling of the reactors and associated plant should be shown to be feasible at stipulated points in time and the design should be such as to facilitate this. The aim should be to keep to a minimum the surveillance required of the decommissioned site and the period before it can be returned to unrestricted use. Other less stringent means for decommissioning, such as removing only the fuel and waste material in the form of liquids or sludges, may be acceptable provided the site is capable thereafter of being maintained in a safe condition.

**287** To meet the requirement for eventual decommissioning, dismantling and removal of the plant consideration should be given in the design to the following:—

- (a) means, such as arrangement and location of the various items of plant and access thereto, to aid in and ease decommissioning and dismantling.
- (b) means, such as choice of materials of construction, to minimise the production of radioactive waste, particularly that due to long-lived nuclides.
- (c) minimising the radiation doses which might be received.

**288** Records should be kept of methods and details of the construction of the plant, with particular regard to the proposed methods of dismantling it.

**289** Outline plans for the restoration of the site to a radiologically safe condition should be formulated at the initial reactor design stage and should be kept up-to-date as necessary during subsequent operation, maintenance and modification.

**290** The plant should be capable of being decommissioned after it has been involved in an accident. In particular, consideration should be given to the need to retrieve irradiated fuel, including fuel which has melted out.

**291** Means should be provided for measuring the recording during the lifetime of the station parameters such as neutron fluence rate and radiation dose rate, and for estimating the radioactive inventory and contamination levels, which will be necessary for the prediction of anticipated radiation doses to workers and members of the public during and after decommissioning.

**292** Consideration should be given to the means and the route of transportation to the eventual storage or disposal sites of wastes resulting from decommissioning processes.

**293** An assessment should be made of the rate and mode of deterioration of any plant left on the site, and of the influence of such deterioration on the radiological hazard from the site. It should be demonstrated that any such deterioration can be safely contained and/or dealt with.

**294** Leakage of activity from the reactor and ancillary plant when in the shutdown or decommissioned state should be capable of control such that no member of the public would receive an exposure in excess of any of the requirements of principles 8, 9 and 12. To monitor this, suitable means should be provided for measuring and recording the amounts of radioactive material leaking from the reactor and ancillary plant.

---

### **3.17 Quality assurance**

---

#### **Introduction**

Quality assurance is a management system used to ensure adequate control of the design, manufacture, construction and operation of any nuclear plant. Its function is to ensure so far as practicable that all specifications for the achievement of safe conditions at all specified times are met.

In carrying out an assessment of quality assurance the assessor should judge the extent to which the submission shows conformity with the principles in this section.

**295** An effective quality assurance regime should be in force in respect of all safety-related aspects of a nuclear plant during all phases of design, manufacture and construction and at all specified times throughout plant life.

**296** The proposed quality assurance organisation and programme should be described in the safety case presented in respect of any nuclear plant. As a minimum such presentation should include documented statements of the principles of the organisation involved in the programme.

**297** The plant should be designed and operated in such a manner as to allow the quality assurance requirements to be effectively implemented, and quality control to be applied.

**298** The licensee of the plant is responsible for establishing a quality assurance organisation and overall programme to meet the requirements of paragraphs 295 and 297. The programme should provide for control of the constituent activities associated with the nuclear plant such as design, construction and operation and should specify the quality assurance to be applied to each item.

**299** The overall requirements and principles set out in the programme referred to in 298 should form the basis for subordinate programmes proposed by main

and sub-contractors in any project to design and construct a nuclear plant.

**300** A main contractor should be responsible for implementing quality assurance in his own organisation and for ensuring that agreed quality assurance is implemented by each sub-contractor.

**301** Any quality assurance organisation and all personnel having responsibilities for quality assurance should so far as practicable be remote from the commercial pressures of production and progress.

**302** Quality assurance requirements should be carried out in accordance with appropriate procedures and the results documented so that they can be verified independently.

**303** To verify compliance with all aspects of a quality assurance programme, provision should be made for planned and random documented audits to be carried out internally by contractors and externally by the owner or purchaser.

**304** Internal audits should be conducted by persons who have no responsibility for the design, procurement, manufacture or construction processes.

**305** Quality assurance programmes should include arrangements for recording and feeding back information for the purpose of further improving designs, standards and specifications and quality assurance practice.

**306** Any modifications, additions or changes, including acceptance of non-conforming items should be subjected to the same level of quality assurance as was applied to the original design.

**307** Quality assurance personnel should have the responsibility within their own organisation to recommend a stoppage of work through appropriate management in the event of unauthorised departures from agreed procedures.

---

## Glossary of terms

---

**Absorber** is any material intended for insertion into a reactor core in the form of solid pins, elements, stringers, sub-assemblies or as liquids, particles or gases, which contain elements capable of absorbing neutrons so that the neutron chain reaction may be controlled or shut down.

**Accident** is any event arising from a fault which gives rise to exposures in excess of those anticipated for normal operation.

**Accumulation**, with reference to radioactive waste, means approved storage of radioactive waste on a reactor site for a period which may or may not be defined but with a view to subsequent disposal on or from the site.

**Adequate** means the necessary and sufficient extent of any measure such that the plant can be judged to comply with these principles.

**At all specified times** or **At any specified time** means during any normal operational mode, fault condition, testing, maintenance, refuelling or shut down and where appropriate during and following fault conditions throughout the life of the plant.

**Best Estimate** when used in connection with the analysis of any fault process, means that the conduct of that analysis should be made only with the aid of the data which are specific to the circumstances of the fault under consideration. The result of such an analysis would be expected to provide the most accurate description of the fault or its consequences as allowed within the limitations of the analytical model employed.

**Bounding Case** is a member of a set of cases, such as a set of fault sequences, which represents the extreme case of that set in respect of the conditions of interest in any particular study.

**A channel** is a non-redundant chain of instrumentation or equipment to the point of combination with other identical channels or single output function.

**Components** are elements within the plant which represent the smallest subunits considered in assessment.

**Conservative Estimate** is used where reasonable doubt regarding the accuracy of data prevents a best estimate from being made. Appropriate assumptions or data estimates are used in place of accurate data such that, when employed in the analysis of a fault or its consequences, they would be expected to lead to a result bounding the best estimate on the safe side.

**A Containment** is any structural membrane, other than the reactor coolant circuit, surrounding a part of the nuclear plant which is either provided for the purpose of or is capable of restraining the accidental or routine release of radioactive material from that

part of the plant to the environment. This includes any systems or components necessary to the required performance of the containment and any extensions of the main structure such as pipe work or ancillary structures which communicate directly with the containment atmosphere or the source of radioactivity.

**Design basis** a formal statement of intended physical performance, limitations and working conditions for a component or system.

**Discrete fault sequence** is any specific chain of successive events which can be foreseen from consideration of the characteristics of a nuclear plant, starting from an initial fault through to that point at which the chain can be seen to have terminated and the consequences fully developed.

**Diversity** the provision of dissimilar means of achieving the same objective.

**Equipment** any plant items or components, including instrumentation but excluding structures.

**Effective barrier** is a passive or active engineering provision, system or group of provisions or systems provided to prevent or terminate any discrete fault sequence which might otherwise lead to the release to the environment of radioactive material.

**External hazards** hazards arising from outside the site but including loss of grid connection or services, fires within the site, missiles generated within the site and any similar hazards.

**Fault** is any foreseen unplanned departure from the specified operating mode of a system or component because of a malfunction, maloperation or defect in a system or component.

**Fertile material** any material containing any element which when irradiated by neutrons is converted into fissile material.

**Fissile material** any material containing any element capable of participating in a nuclear chain reaction.

**Frequency** is the expected mean rate of occurrence of an event. Where a plant contains more than one component which may be the seat of an initiating event or an event sequence and where similar sequences with similar consequences are expected to arise irrespective of which component fails, then, for the purpose of assessment, the frequency of the initiating event should be taken as the product of the expected frequency of that event in one component multiplied by the number of such components in the plant.

**Fuel** means any pin, element, stringer, sub assembly or other component which contains fissile or fertile material and which is intended to form part of a

reactor core or be irradiated by the neutron flux generated in a reactor core.

**Heat Transport System** means all those structures, systems and components necessary to maintain a given item within safe temperature limits. It therefore includes the heat sink.

**Heat Sink** is that feature associated with any nuclear installation which guarantees, for practical purposes, an unlimited capacity for heat absorption with negligible rise in mean temperature, though local temperatures may rise significantly, and negligible change of state.

**Instrumentation** all equipment provided to measure, indicate, record, control or communicate.

**Minimise** means to reduce to as low a level as is reasonably practicable. Minimum is used in the same sense.

**Operation** means all states that the plant may be in as a result of any approved and planned normal operation including shut down, maintenance, testing and inspection.

**Plant** the plant includes all those facilities on the nuclear site upon which safe operation of the reactor and associated sources of radiation depends. In some circumstances where safe operation of the reactor is directly dependent upon equipment or facilities outside the nuclear site then such features should be considered as part of the plant.

**A Postulated Fault** is any discrete fault sequence considered in accident analysis, irrespective of its probability or consequences, and which may be used to provide a basis for the design of the plant, in particular the design of any protective feature, or which may be used as a basis for evaluating the response of the reactor plant to such fault conditions.

**Protective Action** the single specified action performed by a channel or group of identical channels, e.g. primary reactor trip, to close a particular containment penetration.

**Protective Function** the combined objective of one or more protective actions e.g. trip reactor, close containment.

**Protection System** is all that equipment provided to act in response to a fault so as to prevent, limit or otherwise control the development of any unsafe state in the plant. Each part of the protection system is assigned a specific function and more than one function may have to be performed by more than one system to control certain faults.

**Quality Assurance** all those planned and systematic actions necessary to provide adequate confidence that an item or a facility will perform satisfactorily in service.

**Quality Control** involves those quality assurance actions which provide a means to control and measure the characteristics of an item, process, or facility to established requirements.

**The Reactor Core** is the assembly of fuel and neutron absorbers mounted within a suitable structure designed to locate the fuel, provide access for the absorbers and control flow of coolant past the fuel. Any other elements within the core assembly such as detecting equipment which could have an influence on safe operation of the reactor core should be considered as being a part of the core for the purpose of these principles.

**Redundancy** is the provision of more than the minimum amount of similar equipment that is necessary for performance of a given action.

**Reliability** is a measure of the certainty that a component, sub-system or system will continue to perform its required function or perform that function when called upon to do so.

**Safety Parameters** a safety parameter is a physical quantity which has a direct relationship to those conditions in the plant which if changed adversely could lead to an accident.

**Safety-Related Feature** a safety-related feature is any aspect of plant design, construction or operation that could be associated with the initiation, detection or limitation of any fault sequence that might give rise to an accident.

**Safe State or Safe** a plant or a subordinate system of the plant is, for the purpose of these principles, considered to be safe or in a safe state when it is in all respects within those limits which have been identified and specified for the purpose of limiting the risk due to that plant, at any time.

The term **safe** is also used to qualify actions or measures that may be taken in design, construction or operation. In these cases it is intended to indicate a bias being introduced by the application of that measure etc., towards a lower level of expected risk due to the plant.

**Shutdown Provision** the total provision for shutting down the reactor.

**Shutdown System** a system provided to shut down the reactor from the input to the activating mechanism, through to, and including, the neutron absorbing medium.

**Site** the area of land, defined by the site licence, on which the nuclear installation is sited; the boundary of this area is the site boundary.

**Specified Fault** is any foreseen fault which is assumed to occur and which is analysed with a view to demonstrating plant safety.

**Unsafe or Unsafe State** the plant or a subordinate system of the plant is, for the purpose of these principles, considered to be unsafe or in an unsafe state when any limit which has been identified and specified for the purpose of limiting risk is at any time exceeded.



HMSO publications are available from:

**HMSO Publications Centre**

(Mail and telephone orders only)

PO Box 276, London SW8 5DT

Telephone orders 01-622 3316

General enquiries 01-211 5656

(queuing system in operation for both numbers)

**HMSO Bookshops**

49 High Holborn, London, WC1V 6HB 01-211 5656 (Counter service only)

258 Broad Street, Birmingham, B1 2HE 021-643 3757

Southey House, 33 Wine Street, Bristol, BS1 2BQ (0272) 24306/24307

9-21-Princess Street, Manchester, M60 8AS 061-834 7201

80 Chichester Street, Belfast, BT1 4JY (0232) 238451

13a Castle Street, Edinburgh, EH2 3AR 031-225 6333

**HMSO's Accredited Agents**

(see Yellow Pages)

*and through good booksellers*

£3.80 net

ISBN 0 11 883642 0