Health and
Safety
Executive

HM Nuclear Installations Inspectorate

This version of the SAPs has been superseded by the 2014 version.
Please see www.onr.org.uk/saps

Safety Assessment Principles for Nuclear Chemical Plant

October 1983

SAFETY ASSESSMENT PRINCIPLES FOR NUCLEAR CHEMICAL PLANT

Nuclear Installation Inspectorate
Silkhouse Court
Liverpool

CONTENTS

FOREWORD

In April 1979 the Health and Safety Executive published "Safety Assessment Principles for Nuclear Power Reactors" (ref l), for the use of HM Nuclear Installations Inspectorate. Consideration of other types of nuclear installation was excluded from that document, though its general principles are applicable to all nuclear installations. This document sets down principles specifically for the guidance of HMNII assessors of nuclear installations other than reactors and nuclear assemblies. It incorporates the general principles of the earlier document, although there are differences in detail resulting from the different activities to which it applies The installations addressed have a range of functions such as fuel fabrication, fuel reprocessing, isotope separation, waste storage and waste disposal; for convenience, in this document such installations are referred to as nuclear chemical plants. (See Glossary.)

INTRODUCTION

Under the Nuclear Installations Act 1965 (ref 2) no site, except those of the UKAEA and Government Departments, 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. Certain provisions of the Nuclear ~nstallationsAct are relevant statutory provisions of the Health and Safety at Work etc Act 1974 (ref 3) which enables inspectors to be appointed to assist in the execution of such provisions. Inspectors therefore have the task of advising on the issue of licences, the attachment to those licences of appropriate conditions, and the enforcement of those conditions.

Exercise of this responsibility depends on, and must be preceded by, a review of the prospective licensee's proposals which will be presented in the form of a safety submission, ie a safety report and other supporting information. It is desirable that HMNII should adopt a consistent and uniform approach to this review process within 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 form this framework. They are to be used primarily as a basis for the HMNII's safety assessment work in support of the licensing process or, as appropriate, for any other assessment work which the HMNII may need to do. They apply mainly to those nuclear installations prescribed (ref 4) under the Nuclear Installations Act. They will be used at any time from the generic or conceptual stage of a project, through design, developnt, manufacture, construction and operation, to eventual decommissioning, and they will also be used in the assessment of proposals for modifications to existing plant.

In carrying out an assessment it is intended that the assessor should judge the extent to which the safety submission shows that the proposals are in conformity with the principles. In this connection it is not expected that this judgement could be made in full at the proposal stage for plant on a new site, or prior to the construction stage for new plant on an existing nuclear site. However, it will be necessary for the assessor to be satisfied that information sufficient to complete the judgement prior to the operation of the plant is likely to be made available.

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 are specific requirements, such as maximum permissible doses. Some of the principles in Parts 2 and 3 are expressed in quantitative terms which give guidance to assessors on the levels at and below which they can confine their studies to the validity of the estimates sutanitted to them and need not embark on detailed working aimed at establishing whether further improvements would be deemed to be reasonably practicable. It is not the intention that these quantitative assessment levels should be rigidly imposed on designers or operators, since this would remove the flexibility which they must have in exercising their duty to reduce overall risks as far as is reasonably practicable. In principle the depth of assessment will generally be commensurate with the magnitude of the potential hazard. The principles represent the HMNII's present assessment position; the extent to which they are satisfied in a safety submission would be an important factor in decisions on licensing a new site or consenting to the operation of a new plant on an existing site. However, it is recognised that, given the range of facilities concerned, not all the principles may be appropriate to any one plant or site. Furthermore, it is expected that future 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 set out in the four Parts of the document:

> Part 1 comprises a set of fundamental principles on which the principles in Parts 2 and 3 are based.
>
> Part 2 contains basic principles and states the overall objectives of limiting the radiological consequences of the operation of nuclear installations in normal and fault conditions.
>
> Part 3 is mainly concerned with those engineering features upon which the implementation of the basic principles depends. It covers aspects of plant design and operation, and environmental considerations.
>
> Part 4 is concerned with managerial arrangements for safety, and it includes quality assurance.

Parts 2, 3 and 4 are divided into Sections, each of which gives a set of principles applying to a safety-related topic rather than principles relating to particular industrial processes. The fundamental principles and those dealing specifically with radiological protection should be read in conjunction with, and are without prejudice to, any regulations on radiological protection and my associated Codes of Practice. It is recognised that issues may arise for which the principles, or associated definitions and comments, do not provide adequate guidance. In such circumstances special consideration must be given to the issues concerned to establish the Inspectorate's position. Such cases may indicate a need to produce new or revised principles.

The scope of the document precludes the provision of guidance on conventional hazards, except where they may generate a radiological hazard, and any consideration of siting policy.

Attention is drawn to the Glossary, which provides certain definitions, and interpretations of terms used in the text where, unless otherwise required by the context, meanings other than common usage are intended.

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

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

1 REQUIREMENTS AND POLICY

Introduction

The policy upon which the assessment principles are based is that the design safety submission shall show that in normal operation the recommendations of the International Commission on Radiological Protection (ref 5) and the requirements of the EEC Directive (ref 6) are followed with regard to radiation exposures to persons **both** on and off the site.

In addition, in respect of the limitation of the likelihood and consequences of accidents, it shall be shown that all reasonably practicable steps have been taken to prevent plant failure, plant damage, or maloperation and thus to reduce the chance of accidents occurring. It shall also be shown that steps have been taken to minimise the consequences of any foreseeable accident. The more serious the potential consequences, the greater will be the extent of the proposed safety measures that would be regarded as reasonably practicable.

Design, manufacture, construction and operation are key features in the safety of a plant. A sound design concept, a well-engineered and proven design, and a high quality of manufacture and construction will be required. High standards of operation based upon carefully planned management organisation, training and operating rules are essential requirements.

Fundamental Principles

In carrying out an assessment, the assessor should judge the extent to which the safety submission shows conformity with the following fundamental principles:

1 NO person shall receive radiological doses in excess of the appropriate dose limit as a result of normal operation.

2 Doses to individual persons shall be kept as low as is reasonably practicable.

3 Having regard to principle 2, the collective dose to persons on and off the site resulting from 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 consequences of any accident.

2 **BASIC** PRINCIPLES

Introduction

The principles given in Part 2 have been formulated to guide the assessor in judging the extent to which the fundamental principles, given in Part 1, have been satisfied, with the ultimate objective of limiting the radiological consequences of the operation of nuclear installations.

The following principles are based on UK operational experience to date. They represent a level of protection against the radiological consequences of normal operation and fault conditions which should in most circumstances prove to be reasonably practicable. Whilst it is not a requirement that all the basic principles must be rigidly adhered to, or applied in every case, it should be expected that any safety submission would justify any departure from them.

The assessor should judge the extent to which the safety submission shows conformity with the principles of Part 2.

2.1 RADIOLOGICAL PRINCIPLES

Introduction

Although some assessment principles relate to subjects for which numerical criteria exist *(eg* radiological exposure), there is an overriding requirement that the risks must be reduced as far as is reasonably practicable. Since the scope for such risk reduction will vary from case to case, the application of numerical criteria may need to be accompanied by consideration of the overriding requirement for risk reduction. However, there comes a point at which further consideration of risk reduction would itself be more costly in resources than the value of any likely benefit. Assessors are therefore given guidance in terms of assessment levels at which they need not embark on detailed working aimed at establishing whether further improvements would be deemed to be reasonably practicable. The assessment levels should not be taken as targets for designers and operators, whose duties remain those of reducing risks as far as is reasonably practicable, and of complying with any prescribed limits or requirements. In general, assessment levels are given as fractions of the dose limits in current statutory provisions.

Where a proposed level of risk is above the assessment level the designer's arguments must be examined to determine whether further measures should be taken to reduce the level of risk. If the level of the risk proposed by the designer 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 proposed may be accepted by the assessor. If the assessor considers that the case has not been properly made or that the level of risk is still too high then some improvement will need to be made.

In cases where the level proposed is below the assessment level, the assessors' studies may be confined to the validity of the arguments from which the levels are derived. However, there is no justification for not seeking 'further risk reductions where methods of reducing risk are readily available and not unduly costly in resources, even if the level of risk is already below the assessment level.

For the purpose of applying assessment levels, persons who are exposed to radiation are grouped as follows:

(i) Classified persons, being those exposed workers who might receive during their employment annual doses in excess of three-tenths of the annual dose limits for workers aged 18 years and over.

(ii) Exposed workers, being those persons who might receive during their employment annual doses in excess of one-tenth of the annual dose limits for workers aged 18 years and over.

(iii) Persons other than exposed workers.

Normal Operation

For normal operation the assessment levels are:

1 For the effective dose (including committed dose) received by any exposed worker on the plant being assessed: three-tenths of the appropriate annual dose limit multiplied by the fraction of a working year for which the worker under consideration is occupied on the plant.

2 For the average effective dose (including committed dose) to exposed workers: one-tenth of the appropriate dose limit. This average dose will be calculated by dividing the annual collective dose received by all exposed workers when occupied on the plant under assessment by the numbe~of exposed worker-years for those workers receiving that dose.

3 For the effective dose (including committed dose) which may be received in any year, from sources originating on the site, by any person who is not an exposed worker: one-thirtieth of the appropriate annual dose limit for persons other than exposed workers.

Additionally:

4 The design of the plant should be such that the exceptional rotation of workers, or the use of numbers above the normal complement, to avoid individual high doses, is avoided.

5 Expsure of persons to dose rates which in the case of continuous exposure would lead to doses in excess of the appropriate annual dose limits should be as infrequent as is reasonably practicable.

6 Surface contamination at any place to which persons on site normally have access should be controlled to the appropriate derived working levels.

Fault Conditions

In judging the extent to which the safety submission shows that the design conforms with principles 7 to 11 below, it should be noted that, where protection is provided, the requirements of these principles apply only to the period from fault initiation to re-establishment of normal operation. The principles are intended to apply to discrete fault sequences although, as shown in detail in Section 2.3, where appropriate, groups of faults may be considered, when the release of radioactive material and total frequency of occurrence estimated for the group bounding case may be judged against these principles.

The principles are:

7 Doses sustained by persons on and off the site as a result of faults shall be minimised.

8 Doses above the appropriate annual dose limit shall be avoided.

9 The assessor should be satisfied that the assessed risk to persons on the site arising from fault conditions in the plant being assessed does not constitute an appreciable addition to the risk assessed for the normal operation of the plant.

10 In respect of effective doses from discrete fault sequences to persons off the site, the following assessment levels apply:

(a)	For faults where frequencies are judged to be greater than once in thirty years,	one-thirtieth of the appropriate annual dose limit.
(b)	For faults whose frequencies are judged to lie between once in thirty years and once in 3000 years,	the appropriate annual dose limit.
(c)	For faults whose frequencies are judged to be less than once in 3000 years,	twenty times the appropriate annual dose limit.

11 The frequency of any fault on the site which might result in a decision to take off-site countermeasures in order to limit the exposure of persons off the site should be made as low as is reasonably practicable.

2.2 PRINCIPLES FOR THE EVALUATION OF RADIATION EXPOSURES UNDER NORMAL OPERATING CONDITIONS

Introduction

This section gives guidance on the procedures to be used in the assessment of radiation exposures, and the principles which should be applied by an assessor in judging a safety submission.

The submission should be subjected to a review in which the radiation doses and dose rates which result from normal operation of the plant are assessed against the principles set out in Parts 1 and 2 and Section 3.5.

The submission should include a dose budget, setting out the doses expected to be received from the plant by exposed workers and by persons on the site who are not exposed workers. Where necessary the dose budget should give information on assumed occupancy factors.

The effective doses to be detailed in the dose budget are:

(a) the collective annual dose,

(b) the annual group average dose, and

(c) the highest individual annual dose.

Principles

1 It should be demonstrated that consideration has been given to the specific tasks involved in the operation and servicing of the plant. It will be necessary to evaluate the effective doses, dose rates, duration, frequency and numbers of persons involved, for each of the component tasks.

2 Effective doses and dose rates should be conservatively estimated, with appropriate allowance for the different uncertainties associated with the estimates of internal and external exposure. Experience is an important guide in this connection, and the assessor should take account of relevant operational data.

3 Estimates of the dose rates which could arise from the build-up of contamination and material in process should normally be based on the maximum values expected to occur at any time during the life of the plant. If some less stringent basis is used this should be justified.

2.3 PRINCIPLES FOR THE EVALUATION OF FAULT CONDITIONS AND PROTECTION SYSTEMS

Introduction

This section gives the assessment procedure to be applied to plant faults, and the principles which should be used by an assessor in judging a safety submission.

The submission should be subjected to the review procedures of Section 3.10, by which potential discrete fault sequences should be identified and considered. In practice it may be acceptable to consider the bounding cases of certain groups of fault sequences.

The review carried out by the assessor should lead clearly to a decision on the general acceptability of the design measures provided to minimise the contribution to the overall risk from each fault or bounding case considered. The submission should be such that most fault sequences examined in this way can readily be accepted on the grounds of the magnitude and nature of the expected radiological release, the standard of protection or the quality of design.

A number of more difficult cases may remain, requiring special consideration before the safety submission could be accepted. This special case procedure would be expected to lead to a narrowing down of unresolved or difficult aspects of plant safety philosophy. As cases are examined, and positions determined, subsequent comparable cases could be resolved more readily by reference to the precedents. Thus in time the principal objective of this procedure would be to determine the relevance of the precedents to the case under consideration. With sufficient accumulated experience the principles could be modified if necessary.

It is recognised that for many components there will be a spectrum of possible defective modes or maloperations and a corresponding range of fault consequences and frequencies. However, in considering the reliance placed on protection systems a simplified approach may be adopted by the assessor in which only two states, success or fajlure, 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 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 HMNII's position is that well established engineering technology forms the basic frame of reference. In many instances it is possible to compare like functions between one plant and another, though this may not always be possible where different physical processes are involved. Nevertheless it is not unreasonable to expect that the engineered means of achieving a given objective 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 for HMNII to use as a starting point in considering any new proposal.

Principles

1 Fault sequences which, without consideration of any effective barrier, can be shown to satisfy principles 10 and 11 of Section 2.1 may be accepted subject to confirmatory assessment. Fault sequences which do not satisfy those principles may subsequently be shown to meet the requirements when the fault analysis takes into account the existence or introduction of effective barriers.

2 The number of effective barriers required should be determined by comparing the estimated doses to persons off the site, from discrete fault sequences without effective barriers, with the following dose levels, in conjunction with the requirements of principle 3:

Whole Body	0.1 Sv (10 rem)
Single Organ	0.3 Sv (30 rem)
Skin	1.0 Sv (100 rem)

(These values are derived from ref 13)

3 Those discrete fault sequences which, without consideration of any existing effective barriers, would be expected to give rise to consequences and associated frequencies in excess of those set out in principles 10 and 11 of Section 2.1, should be assessed as follows:

(a) Any discrete fault sequence for which the dose to persons off the site is estimated to be less than the appropriate level in principle 2 should be shown to be controlled by the presence in the plant of at least one effective barrier. This must be capable of reducing the potential dose and frequency to values given in principle 10 of Section 2.1.

(b) Any discrete fault sequence for which the dose to persons off the site is estimated to be greater than the appropriate level in principle 2, 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. This must be capable of reducing the dose and frequency to values given in principle 10 of Section 2.1.

(c) Any discrete fault sequence for which the dose to persons off the site is estimated to be greater than the appropriate level in principle 2, and for which the expected fr uency of occurrence is greater than about once in $1 3 - 10^4$ years, should be controlled by the presence in the plant of at least two independent effective barriers. Each of these must be capable of reducing the potential dose and frequency to values given in principle 10 of Section 2.1.

SPecial Case **Procedure**

4. Where it is not reasonably practicable to meet principles 1 to 3 above, the plant cannot be accepted without special consideration of the relevant issues. In such circumstances a special examination of relevant scientific, technical and other factors must be carried out by the assessor. The object of such an examination would be to judge whether or not, and under what conditions, the risk associated with the particular issues could be accepted. Any special consideration of safety issues conducted under the provisions of this principle should take full account of precedents established in similar circumstances.

Principles for **the** Conduct of the Basic Fault Sequence Evaluation

5 As an alternative to considering each foreseeable discrete fault sequence the faults may be grouped and a bounding case for each group identified. The basis for the selection of bounding cases should involve two factors:

(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 group are expected to proceed to particular end points.

Each bounding case should **be** chosen to give the most pessimistic view of its group of fault sequences. It must be demonstrated that each selected case is in fact a bounding case of the relevant group in terms of both the consequences and the frequency ascribed to it. (See Section 3.10.)

6 The assessor should be satisfied that the choice of postulated faults adequately represents the faults which have been identified in the safety suhission.

7 The results of the evaluation of each discrete fault sequence or bounding case, comprising physical consequences and their frequency, should be used by the assessor to develop a diagram showing consequences against frequency for all foreseeable faults. In preparing such a diagram, unless alternative valid data are available, all sequences in any group represented by a bounding case should be assigned the characteristics 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.

The following general principles should be applied in making judgements concerning those components of the plant relevant to safety, and particularly in relation to those engineered features claimed to be effective barriers.

8 Well established and accepted standards applied in the design, construction, operation and maintenance of the safety features of plants in operation, and reliable operating statistics, contribute to 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 plant features under consideration. Fault tree and event tree analysis can be expected to provide a powerful means of conducting this assessment.

9 Practical experience with nuclear or other plant should be taken into account in considering the adequacy of design, manufacture and construction standards in the interest of achieving reliable and safe performance.

10 Recent proven advances in scientific and technological techniques relevant to safety should be considered where they are applicable to the proposals and their evaluation. Justification for any failure to use such techniques should be provided.

11 It should be demonstrated that the standard of design, manufacture or construction of features of the plant relevant to safety is or will be the best that is reasonably practicable.

12 It is unlikely that the reliability of those systems comprising an effective barrier could be claimed to be much better than one failure in 104 demands. The reliability of well proven effective barriers is expected to be of this order. The requirements of principles 1 to 3 of this section are based upon this assumption.

13 Engineered safety features should not be considered as effective barrier components if unfavourable interaction effects between systems during any fault sequence can be foreseen, or if any such safety features can be affected unfavourably by the fault sequence against which they are intended to protect.

14 Interconnection of effective barrier elements or sharing of diverse elements is acceptable provided it can be shown that the independent action of each effective barrier is not thereby prejudiced and that the overall reliability objective can be achieved by such an arrangement.

15 Established standards, as indicated in 8 above, can be accepted as a valid basis for judging effective barriers. However, should the potential radioactive release or increased radiation level be significantly greater than anticipated for the 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 4 above.

16 Where data on 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 be given in assessment for analysis using only such conservative data as can be justified in accordance with the principles of Sections 3.10 and 3.11.

3 ENGINEERING PRINCIPLES

Introduction

Part 3 is concerned with various safety-related aspects of plant engineering. The principles contained in its Sections are those engineering principles which, if satisfied in the design, would be expected 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 nuclear plant site.

In certain circumstances these principles will require interpretation. Guides will be produced to provide the assessor with detailed interpretations and examples of application of the principles together with such explanatory material as may be necessary.

The adequacy of any measure in design, manufacture, construction or operation, or the sufficiency of any analysis of plant condition or performance, should he 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. The engineering principles of Part 3 represent a set of objectives, most of which should be met as far as is reasonably practicable, bearing in mind the cost and social implications in relation to the safety benefit of meeting the requirements.

3.1 GENERAL PRINCIPLES

Introduction

The principles in this Section should be used by the assessor as a basis for considering safety-related aspects of plant engineering from the generic or conceptual stage through development, design, manufacture, construction, commissioning, operation, and modification, to eventual decommissioning. The assessor should judge the extent to which the safety submission shows conformity with these principles.

Response to Faults

1 The plant should be designed and operated in such a manner that no single failure should lead to infringement of principles 7 to 11 of Section 2.1. Where necessary, adequate protection should be shown to be provided for the purpose of achieving this objective.

2 To reduce the likelihood of common mode failure to as low as a level as is reasonably practicable, the design of the plant and safety-related features should incorporate measures of diversity, redundancy and segregation commensurate with reliability requirements.

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

(a) A fault should produce no significant operational response, apart from fault indication.

(b) A fault should produce a change towards a safer condition.

(c) Following a fault 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 fault the plant should be rendered safe by the action of engineered safeguards which need to be brought into service in response to the fault.

4 It should be shown that safety-related features are designed inherently safe or to fail in a safe manner.

5 The plant should be designed, constructed and operated so that when necessary it can be brought to a safe state within a reasonable time.

6 Where a choice of safety measures exists, it is preferred that reliance be placed primarily on engineered safety features rather than administrative action.

7 The achievement of a safe state should not be unduly delayed or prevented by any components of the plant or by mechanical failure, distortion, corrosion, erosion, cooling, etc of plant components or by the physical behaviour of the plant process materials during normal operation or any postulated fault condition.

8 Appropriate provision should be made for the protection of plant personnel so that they can maintain the plant in a safe condition or render it safe after a fault.

9 No single failure should prevent the functioning of any protection system in response to any fault sequence to which that protection system is relevant.

Plant Design Principles

10 The best standards of design, manufacture, construction, servicing and operation, commensurate with the required safety and reliability of the plant and its components, should be employed.

11 In the design of all safety-related features due allowance should be made for uncertainties in operating and fault conditions (including human error), and in data and design methods. The possibility of cumulative damage to the safety-related items, of change in environmental and operating conditions and of changes in performance of safety-related items during plant life, should also be considered. It should be demonstrated that any conservatism in design is appropriate to these requirements.

12 The reliability claimed for a safety-related feature should be specified and should be shown to take into account its novelty and the experience relevant to its proposed environment, and other factors such as uncertainties in operating and fault conditions, data and design methods.

13 It should be shown that all safety-related items would be able to perform their functions to the specified degree of reliability throughout their expected life, taking into account the different conditions which each item may experience.

14 Unauthorised access to and interference with safety-related features should be prevented by suitable measures.

Protection

15 In determining the protection requirements for any postulated fault sequence or in considering the likely progression of any postulated fault sequence, credit may be given for any assured inherent feature of the concept or design which can be expected to act to limit the consequences of that fault sequence. Where credit is claimed for remedial measures, the proposed procedures should be specified.

16 The basic objectives in providing protection are:

(a) to prevent the inadvertent movement of radioactive materials from their normal places of residence in both normal operation and fault conditions, and

(b) to preserve intact the shielding and containment provided.

The submission should describe how it is proposed to meet these objectives.

17 Where appropriate, safety-related items should be safeguarded by monitoring and protection systems against any operating mode or fault sequence liable to cause their specified operating limits to be exceeded.

18 Hazardous events and environmental conditions external to the plant, such as are discussed in Section 3.12, should be considered and where appropriate they should be treated as initiating events of fault sequences or in combination with faults originating in the systems.

Data Used in the Design Safety Case

19 Where it is reasonable to do so, theoretical models should be employed in support or confirmation of the design, or as a means of describing safety-related conditions in the plant at any time. Such analytical models should be based on sound principles. In general the models used should adequately represent the processes of interest. Any assumptions or approximations should be shown 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 constitute a reasonable analogue of the expected plant condition. Where uncertainty exists in the available input data or in the simulation, 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.

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

21 The data base used for plant design and analysis, as outlined in 20 above, should be reviewed periodically and checked against plant operational evidence and such new information from other sources as may be relevant.

3.2 RADIOACTIVE MATERIALS

Introduction

The prime objective of radioactive materials control in a nuclear chemical plant is to ensure that exposure of persons on the site and of the general public, to ionising radiations arising from operations on the site, is kept within specified limits and is made as low as is reasonably practicable. In order to meet this objective it is necessary to ensure the safe keeping and handling of the radioactive materials and to prevent unplanned criticality.

The following principles relate to the control of all radioactive materials except where the total mount of materials is so small, or it is in such a form, that certain principles can be shown to be inapplicable. The assessor should judge the extent to which the proposed design and control regime conform to these principles.

General Principles

1 The safety submission should outline the control regime, consisting of both administrative and physical means, by which the radioactive materials can be handled, processed, stored and inspected in a manner which conforms with the principles set out in Sections 2.1 and 3.5.

2 The administrative arrangements should include:

(a) a system of managerial and operator control in circumstances where physical means are not reasonably practicable, and

(b) a mnitoring system to ensure that the condition and performance of physical devices are satisfactory.

The design of the plant and its mode of operation should be such as to facilitate these administrative arrangements.

3 Specifications and flowsheets should be included for the radioactive materials which the plant is designed to contain, in tern of their physical, chemical and radioactive properties.

4 The control regime proposals should identify plant subdivisions and, where appropriate, individual plant items, and state their design and operational inventories in terms of the nature and quantity of radioactive mterials that represent the greatest hazard.

5 The submission should describe the proposed arrangements for the keeping of adequate records of the nature and quantity of radioactive materials within the plant. Where reasonably practicable an appropriate activity or mass balance should be kept. Where this is not reasonably practicable the submission should outline the procedures for establishing that the nature and quantity of the radioactive materials in process and in store are:

(a) consistent with the safe operation of the plant,

(b) within the radioactive materials specification, and

(c) for both plant items and subdivisions of the plant, within any relevant maximum inventory limitations.

General Desi

6 The quantity of radioactive materials within the process should be the minimum consistent with operational requirements.

7 Process and equipment design and the intended mode of operation should be such as to avoid unintended accumulation, and unplanned and uncontrolled movements, of radioactive materials. Where such accumulations or movements are possible the design should provide for inspection and detection, with alarms where appropriate, and facilities for taking corrective action.

8 The suhission should demonstrate that the design of the plant and its mode of operation is such as to ensure that under normal and fault conditions:

(a) radioactive materials are kept separate from incompatible materials,

(b) where appropriate, radioactive materials and non-radioactive reagents are adequately segregated and labelled, and

(c) radioactive and non-radioactive feed materials and reagents are, and remain, within specified limits and are compatible with the safe operation of the plant.

9 A schedule of monitoring and sampling with appropriate instrumentation and alarms, to facilitate the control of radioactive materials within the specified limits, should be suhitted.

10 There should be provision for controlling the temperatures of those radioactive materials where the heat of radioactive decay or chemical reaction may ke significant.

11 Arrangements for the management of liquid radioactive materials should be such that chemical reactions, precipitation, acidity, etc can be controlled to within specified limits.

12. Where facilities are proposed for bringing radioactive materials outside the plant containment, the design should:

(a) minimise the number of such facilities,

(b) minimise the risk of spillage or leakage,

(c) provide, where appropriate, local ventilation, shielding and remote-handling devices,

(d) facilitate the operation, decontamination and repair of any remote-handling devices, and

(e) facilitate, where necessary, the removal and reinstatement of shielding for maintenance purposes.

13 Where there is a need to make a temporary opening in any containment, the design should be such as to minimise personnel exposures and the spread of the radioactive materials.

14 The design of vessels, pipework, plant equipment, and containment structures should facilitate decontamination, *eg* after spillage, prior to maintenance or in the course of decommissioning. The respective merits of providing in situ decontamination facilities and the use of decontamination facilities at central locations should be considered.

15 Where appropriate, furniture, vehicles and buildings, and containments and their contents, should have surface finishes which will remain smooth and impervious throughout the design life of the plant, taking into account both operational and fault conditions and the need for effective decontamination. Corners, cavities and crevices in which radioactive materials may accumulate should be avoided.

16 Where a plant is required to handle a variety of different radioactive materials in successive batches and the plant has to **be** decontaminated between batches, specific arrangements should be made to minimise radiological exposure of the work force during decontamination operations.

17 Designs which provide for lifting operations in the proximity of pipelines, safety-related equipment or other vulnerable items of plant should receive special consideration.

Materials Containmwt

18 The excessive spread of radioactive materials during handling, processing, storage and inspection should be prevented by adequate containment.

19 Containment and packaging of radioactive materials should be designed to maintain their integrity throughout the design life of the plant or package. The design life should **be** stated and justified, and where the design life of individual items is less than that of the plant, or the package design life is less than the likely storage time, the programme and procedure for replacement should be outlined. Due consideration should be given in this regard to:

(a) deterioration of the containment or package with time due to external and internal conditions likely to be encountered during both normal and fault conditions,

(b) the likely duration of the containment,

(c) the nature and quantity of the radioactive materials, and

(d) the need safely to control temperature, pressure, hazardous gases, precipitation and other relevant factors during the intended period of containment.

20 Facilities should be provided for measuring or estimating the quantity of radioactive material in, entering or leaving the materials containment so that significant leakage or other loss may be detected.

21 Where appropriate, sampling and monitoring devices with alarms should be provided to ensure the detection of unplanned or uncontrolled changes in the volume or radioactivity within the materials containment.

22 The design should provide alarm devices to indicate that any approach to overflow from, or over-filling of, materials containment is occurring. The alarm level should be such as to enable corrective action to be taken before overflow or over-filling occurs.

23 It should be shown that, wherever radioactive materials are held in process vessels or pipework, adequate and suitable secondary containment capacity has been provided. Facilities should be provided such that, should its normal containment become defective or unsafe, the radioactive material can he safely retrieved, conditioned if necessary, and transferred into an adequate alternative containment.

24 There should be adequate provision safely to contain and recover radioactive material where overflow of materials containment is possible. Detectors, with alarms at appropriate locations, should be provided to indicate that overflow has occurred.

25 The submission should where appropriate include a schedule for the inspection and monitoring of secondary containment for leaks and spillage from the materials containment. Consideration should be given to the provision of alarms to give automatic warning of such leaks and spillages.

26 Where appropriate, pressure relief or ventilation should be available for those materials which can generate or release gases or vapour.

Fissile Materials Control

Fissile materials should be subject to the above principles, but in view of the possibility of unplanned criticality, the following principles also apply.

27 The applicant should review the potential for unplanned criticality during normal plant operation and fault conditions by considering all reasonably foreseeable circumstances and configurations. The safety submission should identify the most reactive case taking into account the following:

(a) Changes in geometrical arrangements (such as leakage of fluids, transfers between vessels, disruption of solids, overflow from materials containment).

(b) Changes in material composition (fissile material concentration, fissile material density, precipitation).

(c) Changes in neutron moderation (ingress of moisture, flooding, oil leakage, evaporation).

(d) Changes in neutron reflection (flooding, presence of personnel).

(e) Changes in quantities of fissile materials (transfers between vessels, double hatching, precipitation, accw.ulation in pipework).

(f) Changes in neutron absorption (loss of soluble poison, corrosion of solid absorbers, effect of plant mdifications).

(g) Changes in interaction effects (changes in spacing of fissile units, removal of intervening shielding, changes in plant in neighbouring spaces).

(h) Deficiencies in accounting procedures or in enrichment identification.

(i) Any other change which could cause the system to become mre reactive.

28 Determination of the mst reactive configuration or circumstances should take into account the possible range of variability of each of the factors listed in principle 27. If the proposed control regime is based on a configuration or circumstances other than the most reactive, this should be justified.

29 Engineered safety provisions are generally preferable to reliance upon administrative control. For example, the provision of vessels and equipment of favourable geometry or the use of physical restraints to prevent the mutual approach of mvable units are preferable to operational control, with or without instrument assistance. The system of controls chosen to prevent unplanned criticality should be described and justified.

30 Provisions for measurement, cleaning and inspection to facilitate the periodic establishment of the fissile material inventory should be incorporated in plant liable to contain fissile material.

31 The suhission should state by what means, and how often, the inventory of fissile material in the whole plant, and in component plant items, will be ascertained. In describing the methods used to determine the inventory the submission should indicate the expected accuracy of the various techniques.

32 The criticality data on which the submission is based should be clearly stated and justified.

33 Where it is possible to demonstrate safety by a simple approach, *eg* fissile material inventories or volumes too small for criticality, this is preferred to a more refined treatment. The depth of the scrutiny should be appropriate to the complexity of the system under consideration.

34 Methods or computer codes used in criticality calculations should have been validated over the range of interest, and their relevance to the circumstances in which they are used should be well established.

35 Adequate detection, annunciation and alarm systems should be provided at all places where significant amounts of fissile materials are present, unless an assessment shows that in the event of failure of those criticality controls which rely on human agency or on physical arrangements, criticality could not reasonably be expected, having regard to the nature of the particular operations and facility concerned.

36 Adequate detection and annunciation systems should be provided where significant amounts of fissile material are present unless, because of adequate shielding or remoteness, an excursion of the maximum foreseeable size could not produce a dose in man of more than 0.05 Sv (5 rem).

3.3 MOVEMENT OF RADIOACTIVE MATERIALS

The principles in this Section are concerned with the assessment of any procedure involving the movement within the site boundary of radioactive materials within, to and from the plant under review. They apply to movements inside and outside the plant containment by way of fixed devices such as pipework or by transportable packages, and to ancillary equipment associated with the movements such as cranes, transport vehicles, decontamination facilities, pumps, diverters, etc. The assessor should judge the extent to which proposals submitted conform to the principles in this Section.

General Principles

1 The movement of radioactive materials on the site should be minimised.

2 Arrangements for the movement of radioactive materials on the site should take account of the properties of the radioactive materials.

3 The radiological protection principles of Sections 2.1 and 3.5 should be observed.

4 Radioactive materials should at all times be protected against unauthorised access.

5 Packages of radioactive material should be physically secured and provisions should be made to ensure that they follow safely their intended route.

6 There should be arrangements for the keeping of accurate and up-to-date records.

Detailed Provisions for Movements Outside the Materials Containment

7 The safety suhission should identify movements of radioactive material outside the materials containment, stating the properties of materials and quantities being moved for both normal and abnormal conditions, and justifying the chosen m e of movement.

8 Processes and equipment associated with the movement of radioactive materials should, by design and choice of operating procedures, be such as to minimise radiological hazards.

9 Proposals involving the mvement of radioactive materials should take into account the physical and chemical states of the material, the possibility of criticality, their maximum possible residence time within the containment and the condition of that containment.

10 Equipment, including containment for moving radioactive materials, should be designed, manufactured, constructed and maintained such that:

(a) the risk of damage to the containment of such materials, or to any part of the plant, is minimised,

(b) the integrity of the containment is assured in the event of any fault in the movement, route or equipment,

(c) adequate protection is provided against radiation exposures or release of radioactive materials in the event of a fault in the movement, route or equipment, and

(d) servicing can be carried out in conformity with the principles of Section 3.15.

11 Whenever any machine or plant component is, for the purpose of materials movement, connected to or physically associated with a containment, its design, construction and operation should be such that the performance of the containment is not impaired.

12 The standards of containment and shielding for permanently installed means of materials movement *eg.* pipeworks and drains, should be the same as those for the rest of the plant.

13 There should be prior arrangements when radioactive materials are to be moved, to ensure their safe storage or receipt.

14 The location of radioactive materials should be recorded and there should be adequate provision for labelling and record-keeping.

15 Storage, and all actions in the materials movement routes, should be safe against fire, flooding, criticality, mechanical damage, unauthorised access, theft, and any other prejudicial effect. Interaction with other materials in transit and plants should be considered.

16 Movement facilities should be designed so that abnormal items, eg. materials of non-standard chemical or physical compositions, damaged fuel or containers, can be dealt with safely.

17 The arrangements for remedial action following faults in materials movement should be described.

18 Materials movement equipment and routes should be designed to minimise the possibility and consequences of damage to plant and service pipework, cables etc.

19 Protection devices associated with materials movement such as control, instrumentation, interlocks and monitoring equipment should be designed in accordance with the principles of Section 3.6.

20 The operational limits of materials movement processes or sequences should be specified in the submission.

21 For vehicular movements it should be ensured that there are adequate security, monitoring, decontamination and servicing facilities, out-of-use storage, access routes and cranage entailing minimum hazard to other plant.

3.4 RADIOACTIVE WASTE AND SCRAP CONTROL

Introduction

When carrying out an assessment of the safety submission for the control of radioactive waste and scrap, the assessor should judge the extent to which the design and the control regime conform to the principles set out in this Section and in Sections 3.2 and 3.3. The proposals should be assessed without prejudice to:

(a) any requirements arising from the application of the Radioactive Substances Act (ref. 7), and

(b) the final choice of method of disposal.

General Principles

1 The subission should identify the arisings of waste and scrap and demonstrate that they are compatible with the proposed storage facilities and disposal routes.

2 Radioactive waste or scrap should be contained to prevent radiolqical hazards in the event of handling and storage accidents.

3 The storage facilities, and where possible the disposal routes, intended to be used in the commissioning, normal operation and decommissioning of the plant should be outlined in the suh,ission.

4 Facilities for mnitoring and conditioning the arisings of waste and scrap, to ensure that they are and remain in a form compatible with the intended storage or disposal route, should be incorporated in the plant.

5 The design of the plant and the proposed administrative and physical control, should be such that the safe management of waste and scrap arisings is facilitated, and the radiological consequences of normal plant operations, recycling, salvage and storage operations are minimised.

6 To facilitate safe storage and handling ,waste and scrap should be segregated according to physical and chemical form, flanrmability, specific activity, half-life, fissile nature and type of radiation emitted.

7 The disposition of radioactive waste should be controlled within appropriate specified limits and should be managed in order to minimise the resultant radiological detriment to persons on and off the site.

Storage Design Principles

8 Where radioactive waste or scrap are to be stored the sutxnission should show that:

(a) appropriate locations are designated and reserved for that purpose and unauthorised access is prevented,

(b) the facility and its contents are adequately protected from any adverse environmental effects,

(c) each storage facility is adequate having regard to its capacity, the physical and chemical properties of the materials, the possible duration of the storage and any consequential long-term changes in physical or chemical form, and the radiological risk,

(d) the quantity and nature of the stored materials can be kept within specified limits,

(e) the accumulation and storage of radioactive waste and scrap is such that the materials are, and will remain, readily retrievable, and

(f) conditioning prior to disposal, and the eventual disposal, are facilitated.

9 Containers of waste or scrap, and locations where waste or scrap are likely to be kept or handled on a significant scale, should be clearly identified and marked.

10 Special actions needed in the event of incidents such as fire, flood, etc, should be specified.

11 The submission should include a servicing schedule for each store and the stored materials.

12 The safety variables and limits which require monitoring and controlling to ensure safe storage should be specified, and there should be provision for such monitoring and control.

13 The design should facilitate the:

(a) appropriate inspection of stored radioactive waste and scrap,

(b) recording of the quantity, type and form of the radioactive waste or scrap stored, conditioned, retrieved or consigned for disposal,

(c) estimating of the rate of arising and transfer, change of volume on conditioning, and the volume and activity of the waste or scrap in each store, and

(d) estimating of the storage space remaining available in each store.

14 The submission should include estimates of the quantities of radioactive waste and scrap in terms of volume, form and radioactive content together with any other information necessary for its safe handling, storage and disposal.

15 It should be shown that the capacity for the safe storage of radioactive waste and scrap will be sufficient to meet the needs of the plant.

16 The suhission should include a scheme to ensure that, should retrieval or relocation of stored materials become necessary, adequate storage would be available, and transfer to such storage could be effected, within an appropriate time.

17 The design of the plant and its mode of operation should **be** such as to minimise the time for which radioactive waste or scrap is held in short term storage prior to centralised long term storage, disposal, salvage or recycling.

Airborne Waste Discharge

18 The design of the plant and its mode of operation should be such that the discharge of airborne radioactive waste is made in such a manner as to minimise the radiological consequences to persons on and off the site.

19 Discharges to atmosphere should only take place via controlled routes which should **be** terminated by a suitable outlet.

20 The choice of a suitable outlet should take into account the characteristics of the surrounding terrain, prevailing weather conditions and the proximity of other buildings and stacks both with regard to the aerodynamics of the discharge and the compatibility of discharges and adjacent processes.

21 The submission should include a statement of the radioactivity in terms of total activity, concentration, and other physical and chemical properties of the materials with which any gas cleaning facility may have to deal during both normal operation and foreseeable fault conditions.

22 Where appropriate, discharge routes should be provided with gas cleaning facilities compatible with the physical and chemical environment inside and outside the system under both n o d and fault conditions.

23 Outline arrangements for monitoring the adequacy of performance of the gas cleaning system and ensuring that this performance is maintained should be presented.

24 The submission should include a schedule of the necessary sampling and monitoring facilities necessary to measure the activity before and after each gas cleaning facility and to monitor the radioactive discharge to atmosphere. The sampling and monitoring should, where appropriate, be continuous and have adequate alarms to initiate corrective action.

25 A schedule of alarm levels for devices sensing discharges should be included. It should also be shown that the levels chosen are such as to facilitate effective action.

26 Where appropriate, the sampling devices for gaseous discharges should facilitate the keeping of records of arisings from various locations of the plant as an aid to fault tracing and to estimating the discharge to atmosphere.

Licruid Waste Discharye

27 The design of the plant and its node of operation must be such that the discharge of liquid radioactive waste is made in such a manner as to minimise the radiological detriment to persons on and off the site.

28 The suhission should describe the methods that would be adopted to prevent:

(a) the inadvertent discharge of liquid waste,

(b) the inadvertent mixing of the various separate waste streams and stored waste,

(c) the mixing of incompatible materials with liquid waste streams or liquid waste in store,

(d) the discharge of liquid waste into an incompatible environment, and

(e) the discharge of liquid waste to the environment via routes not allocated and designed for that purpose.

29 Where appropriate, the design should provide adequate and reliable monitoring and sampling of liquid radioactive waste streams at source, into and out of storage, and ixrnnediately prior to discharge. These monitoring devices should where appropriate be continuously alarmed, with the alarm levels chosen to facilitate corrective action.

30 Adequate hold-up facilities should be provided at source, with provisions to condition, recycle or otherwise process the liquid waste to ensure its compatibility with its next location.

31 There should be arrangements for the keeping of appropriate records of arisings, storage and discharges of liquid radioactive waste for various locations of the plant, as an aid to fault tracing and to estimating accurately the discharge to the environment.

32 There should be appropriate provision for stopping discharges when tides, river flows, etc, are unsuitable.

33 The submission should consider all wet materials and sludges and justify any decision not to apply the assessment principles relevant to liquid wastes.

Solid Waste Disrx>sal

34 Where appropriate, solid radioactive waste should be conditioned before disposal in order to minimise radiological hazards during on-site transport and disposal.

35 The waste should **be** consigned, for disposal, in containment that will remain intact during foreseeable transport accidents, to the extent that radiological hazards are minimised.

36 It should be shown that account has been taken of the possibilities of fire or explosion, **both** inside and outside the waste containment, during transport to disposal.

37 Waste containment and methods of transport should be compatible with the disposal facilities.

38 The system proposed for keeping adequate records of the waste consigned to conditioning or despatched for disposal should be outlined in the suhission.

Radioactive Scrap

39 There should be appropriate and sufficient locations within the plant where process materials, plant items, construction materials and other items can be temporarily stored so that their ease of decontamination, level of contamination, chemical and physical properties and ease of repair can be assessed to determine whether the items are in fact waste or scrap.

40 Estimates of the arisings of such materials and items which might constitute scrap should be suhitted.

41 It should be demonstrated that the locations designated to hold possible scrap materials are:

(a) suitably situated, of adequate capacity, and provided with sufficient services and equipment to facilitate safe handling, sorting and processing, and

(b) provided with durable impervious surfaces, adequate ventilation facilities and appropriate changeroom facilities.

42 The proposals should describe the system for keeping adequate records of the arising of radioactive scrap, its levels of contamination and its ultimate destination.

3.5 RADIOLOGICAL PROTECTION PRACTICE

Introduction

The principles set out in this Section are intended to give practical guidance in the assessment of radiological exposure control in and around a nuclear chemical plant. Implementation of these principles can be expected to ensure a level of radiological protection consistent with the basic principles set out in Parts 1 and 2. In several instances numerical assessment levels have been defined to aid the assessor in judging the adequacy of the safety submission. These assessment levels are to be used without prejudice to the requirements of any Relevant Statutory Provision. The assessor should judge the extent to which the safety suhission shows conformity with the following principles.

General Princi~les

1 Protection of persons against radiological hazards should be achieved by the use of distance, shielding and containment between radioactive materials and persons, the use of ventilation, and the limitation of times of exposure. Engineered safety provisions are considered to be preferable to schemes involving administrative control.

2 Radiological surveillance should be based on the classification of work places into different restricted zones having various constraints on access, occupancy, protective equipment, etc, appropriate to the radiological hazard presented by the radiation, contamination and airborne activity within each zone.

3 The suhission should define the extent and categories of restricted zones and the necessary constraints within and around the plant during normal operation.

4 The design of the plant should provide for the necessary control of entry to, and exit from, these zones and for the observance of any necessary constraints.

5 There should be provisions for limiting and monitoring the spread of contamination, and also for monitoring and controlling direct radiation levels, within and outside each restricted zone.

6 For assessing the regime for controlling access to the various zones during normal operation, the following dose assessment levels apply:

(a)	Zones to which all persons on site have unrestricted access,	0.75, ~Sv/h. (75 rem/h)
(b)	Zones from which all persons other than exposed workers are normally excluded,	2.5 ,&Sv/h. (0.25 mrem/h)
(c)	Zones from which all persons other than classified persons are normally excluded,	7.5 ,aSv/h. (0.75 mrem/h)
(d)	Zones to which access may be required for no more than once every one or two years for periods lasting mre than a few hours,	0.5 mSv/h. (50 mrem/h)
(e)	Zones to which access may be required for no more than once every one or two years for periods lasting up to a few hours,	2.0 mSv/h. (200 mew)
(f)	Each discrete task in zones where the dose rate exceeds 0.5 mSv/h, (50 mredh)	1.0 mSv. (100 mrem)

7 The assessment levels for airborne contamination during normal operation are the following fractions of the time-averaged value (over 40 hours) of the derived air concentration **(DAC)** appropriate to the class of person under consideration and to the nature of the contaminant:

(a)	Zones to which all persons on site have unrestricted access,	three-tenths of the time-averaged value for persons other than exposed workers.
(b)	Zones from which all persons other than exposed workers are normally excluded,	one-tenth of the time-averaged value for exposed workers.
(c)	Zones from which all persons other than classified persons are normally excluded,	three-tenths of the time-averaged value for exposed workers.

8 The suhission should describe the administrative system for controlling work within the various restricted zones to ensure that doses are kept as low as is reasonably practicable. The system should establish a regime for environmental monitoring and a regime for imposing restrictions on access, occupancy, etc, progressively more stringent as the radiological hazard increases. Thus as the dose rates and frequency of such operations increase, account should be taken of the expected dose and also of the need for more careful control regimes. This latter consideration is particularly important in areas where the dose rate exceeds 0.5 mSv/h (50 mrem/h).

9 A schedule should be included which lists locations and tasks where a dose rate in excess of 25pSv/h (2.5 mrem/h) may be encountered. Occupancy of such zones should be restricted and appropriately documented.

10 Access to regions within shielding or zones where the dose rate would normally **be** expected to exceed 0.5 mSv/h (50 **mrem/h)** should be controlled by specific measures such as interlocks, locked doors or alarms designed to prevent unauthorised entry. Prompt escape by any person from such places should not be obstructed by any feature of the design. Where such control measures are not reasonably practicable eg. fuel ponds, transport containers, sample castles, etc, the submission should demonstrate arrangements to achieve an equivalent standard of protection.

Control of Direct Radiation

11 Special precautions should be taken in the design of containment, shielding and equipment to avoid:

(a) localised high levels of radiation,

(b) unplanned or uncontrolled movement of shielding,

(c) installation behind shielding of components requiring frequent handling or to which frequent access is required, except when such components are sources of radiation requiring shielding,

(d) unplanned or uncontrolled removal from behind shielding of any material or equipment which could give rise to a significant dose rate when unshielded,

(e) high doses of direct radiation to the extremities of workers during access to and manipulation of radioactive materials and equipment,

(f) the loss of liquids used as shielding material. (There should be provisions for detecting changes in such liquid levels and the build-up of radiolytic gas mixtures, and for an alarm in the event of any unsafe change), and

(g) the presence of locations which will result in the accumulation of solids of safety significance which cannot be removed as a result of the normal transport of material-in-process. (Where such locations cannot be avoided, the submission should describe the provisions for detecting the presence of such materials and effecting their safe removal and disposal.)

Control of Contamination

12 The spread of loose radioactive materials should be controlled by means of adequate local containment supplemented by appropriate ventilation and atmosphere clean-up systems.

13 The design of the plant should provide for:

(a) decontamination of zones to which access may be necessary,

(b) decontamination of articles which may have to be removed from contaminated locations,

(c) ventilation of contaminated zones to limit the spread of contamination,

(d) protection of persons entering and working in contaminated locations, and the prevention of the spread of contamination when persons leave a contaminated location,

(e) adequate sealing of containment penetrations, and

(f) monitoring for airborne contamination, with alarms when the levels exceed limits specified in the submission.

14 The submission should justify the choice of location and type of air sampling devices and include a list of those locations and the devices which perform the following functions:

(a) the monitoring of personnel exposure during frequent and regular tasks,

(b) the monitoring of personnel exposure during regular but infrequent tasks, and

(c) the monitoring of significant changes in ventilation conditions.

15 Details of the arrangements for providing air sampling facilities in the event of foreseeable faults should also be submitted.

16 Appropriate provisions should be made for the use of personal air sampling systems.

17 The derived limits of surface contamination and airborne contamination used as the basis for the design of plant containment and ventilation systems should be specified in the submission.

18 The submission should include estimates of surface and airborne contamination in the various zones during the component tasks of normal operations.

19 Manipulation of highly contaminated articles and highly radioactive materials should be carried out in enclosures designed to provide adequate protection against the spread of contamination. Where such enclosures are not reasonably practicable, the manipulation should be undertaken in locations chosen to minimise the radiological exposure of all persons.

20 Where reasonably practicable the manipulation of highly contaminated articles and highly contaminated materials should be carried out using remote handling devices so as to minimise the exposure of the operatives to both radiation and contamination.

3.6 PROTECTION SYSTEMS

Introduction

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

(a) Protection *systems*

The systems act directly to reduce risk in the event of any fault. Depending on the nature of the plant, the protection systems would act in various ways, which could include diversion of feed materials, diversion of radioactive materials and the bringing into operation of auxiliary equipment. The systems could, for example:

- interlock against unsafe modes of operation,
- prevent, limit or delay the escape of radioactive materials following a fault,
- automatically or manually control the plant when pre-set safety limits are exceeded,
- remove heat from radioactive materials and radioactive waste,
- activate any other safety-related protection system or equipment, or
- include the power supply to the protection system.

(b) **Safety Related Instrumentation**

This has a significant but indirect effect on safety. Examples are:

- 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, and plant variables and parameters,
- communications equipment for accident conditions, or
- equipment for monitoring abnormal radioactive releases from the site.

In carrying out an assessment of protection systems and safety related instrumentation the assessor should judge the extent to which the suhission shows conformity with the principles in this Section. Protective features of essential resources and containment are also dealt with in Sections 3.7 and 3.8 respectively and these should be read in conjunction with the principles in this Section.

Principles for Protection

1 Protection systems should be provided and maintained in a state of readiness adequate to ensure safety.

2 All systems which are required for protection against specified faults should be identified in the suhission. For each postulated fault it should be shown that the aggregate of all relevant protection systems comprises an effective barrier or barriers as described in Section 2.3. Such protection should be capable of rendering the plant safe and maintaining the plant in a safe state for as long as may be necessary following that fault.

3 Protection systems should be shown to provide the correct sequence of operations, and control the values of safety-related plant variables.

4 The submission should show that protection systems or components are designed to accommodate changes in performance resulting from physical or chemical effects such as changes of state, leaking, irradiation, geometrical changes, diffusion, corrosion, deposition etc.

5 No single failure within a 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 it.

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

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

8 All variables used to initiate protective action should be identified and shown to be sufficient for the purpose of protecting the plant. Appropriate safe limits for these variables should be specified which are relevant to the state of the plant at any time. It should be shown that the protection systems are designed to respond to the appropriate variables within the above limits and within a reasonable time, and that the resulting performance is adequate.

9 Where a directly related variable cannot be used for the purpose of initiating protective action against a fault, an indirectly related variable may be employed. In such cases it should be shown that the variable chosen has a known relationship with the main variable of concern and with the fault being detected.

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

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

12 Where protection system reliability is required to be very high, or when there is doubt about the effectiveness of a system, redundancy and diversity should be introduced.

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

14 Each protection system should be automatically initiated, and should carry out all actions required to put the plant into a safe state. The design should however be such that an operator could initiate protection system functions and perform the actions necessary to deal with circumstances which might prejudice the safe state of the plant. It should also be possible for the operator to negate protection system action, but only in certain circumstances that must be specified. Physical arrangements for preventing protection system action must be strictly controlled and kept to a minimum.

15 The required performance of components and subsystems should be stated and shown to be adequate for the purposes of providing protection. Limits should be defined outside which components should not be operated; provision should be made to ensure that these limits are not exceeded. It should be shown that the overall reliability and availability of each protection system is adequate.

16 Components selected for use in any protection system should have proven reliability and performance.

17 It is desirable that no single failure within any protection system should cause any plant variable to change to a significantly less safe value.

18 The minimum amount of operational protection equipment with which plant 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.

19 Where a common m e event 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. Additionally this principle should be applied to those mechanisms which could initiate a plant fault or failure of the associated protective functions.

20 The plant should be designed so that routine testing of installed protection systems is facilitated. Such tests, when supplemented as necessary by proof and reliability testing in external facilities, should adequately demonstrate the performance and reliability of the protection systems. The suhission should specify the proposed testing programmes.

21 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 intervals throughout the life of the plant, commensurate with the reliability requirements.

22 When equipment has several functions, one of which is to ensure safety, this equipment should be classed as protection equipment. The protective function should not be jeopardised by the other functions.

23 Alarms and annunciators should be provided to give warning that any safety-related system, component or variable is at any pre-set limit of its acceptable operational state. Where appropriate, alarms should be initiated in the event of any unsafe failure of any element of a protection system.

24 Where required on safety grounds all protection system equipment including pipework and cabling should be segregated from all other equipment and its function clearly indicated. Any system for which diversity is claimed should have diverse segregation. Where interaction with or proximity to non-protection equipment or cabling is required, this should be justified. The segregation of equipment and cabling within the protection system should be such as to satisfy principle 19.

25 The design should be such that the means of access to all protection equipment can be physically controlled in order to protect the availability of the minimum amount of operational equipnent referred to in principle 18.

Instrumentation

26 Indicating and recording instruments should be provided to inform the plant operators of the state of those items which have a significant influence on safety or 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 alarms when set limits are reached.

27. Sufficient information should be available to the plant operator to enable an accurate appreciation to be made of the plant state so that all actions necessary in the interests of safety can be taken promptly and effectively.

28 Where derived variables are used for safety related instrumentation, their physical relationship to the plant variable of interest must be defined.

29 The instrumentation provided to meet the requirements of this section should enable an operator to take all necessary actions from a central control room. Adequate protection against radiation, contamination, toxic hazards or 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 requirements of the radiological principles.

30 Consideration should be given to providing instrumentation and control equipment at locations other than the central control room to enable the plant to be safely brought to, and maintained in, a safe state should the central control room become inoperable or uninhabitable.

31 The minimum amount of safety-related instrumentation with which pl'ant operation may be permitted should be specified.

32 Suitable communications systems should be provided 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.

33 Where a protection system m y be affected by fire, a reliable fire warning system should be provided.

34 All instrumentation should be of a quality appropriate to the duty. Evidence should be provided of its satisfactory performance under the worst environmental conditions expected.

35 The reliability, accuracy, stability, response time, range, and where appropriate, readability, of all instrumentation should be adequate and appropriate for its required service.

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

37 Adequate means should be provided for the testing and calibration of safety-related instruments at any specified time without loss of any essential function.

Criticality Incident Detection (CID) Sys-

Where a proposal includes the provision of a CID system, the assessor should, where appropriate, apply the foregoing principles of this section. The following additional principles are to be applied to CID systems:

38 The specified objectives of the CID system should include:

(a) the detection of incidents involving a specified minimum number of fissions as an indication of operational failure, the choice of the minimum number of fissions being justified, and

(b) the detection of incidents of specified characteristics where necessary for the purposes of reducing doses to persons by initiating evacuation procedures.

39 The areas for which detection, annunciation or evacuation are required should be defined and justified, and account should be taken of related technical and managerial requirements (see Sections 3.2 and 3.9).

40 The CID system should indicate its functional or nonfunctional state by an automatic signal.

41 Upon initiation, the CID system should give an audible alarm of adequate strength throughout the whole area from which evacuation is required.

42 After initiation the audible alarm should continue to sound until manually reset. Access to the reset facility should be strictly limited, and it should be located outside the evacuation area.

43 The proposal should include estimates of the CID system reliability, including the reliability in respect of spurious alarms.

3.7 ESSENTIAL RESOURCES

Introduction

Essential resources include all those services and materials necessary to the attainment of a safe state in the plant. Those essential resources which form part of or supply any protection system should be regarded for assessment purposes as part of the protection system. The general principles set out in this Section, and where appropriate those of Section 3.6, apply to all essential tesources. The assessor should judge the extent to which the safety submission shows conformity with the principles in this Section.

Principles

1 The submission should include a comprehensive inventory of the essential resources together with brief descriptions of their roles.

2 The adequacy of each essential resource should be demonstrated in the submission. In particular it should be shown that each resource can be provided for a sufficient period of time and with adequate quality and availability to allow the plant to ke brought to a safe state when necessary and maintained therein. Where essential resources are shared with other plants, the effect of the sharing should be taken into account in assessing the adequacy of supply.

3 The reliability and quality of essential resources should preferably be achieved by engineered systems rather than by operational control or human intervention.

4 It should be shown that the reliability and adequacy of the various resources are maintained despite adverse conditions. In this context the principles of redundancy, diversity and segregation should be applied where appropriate. The adverse conditions considered should include:

(a) those generated by the plant during normal and fault conditions,

(b) those generated by other facilities on the same site,

(c) those generated by facilities off site, and

(d) those off site which may influence the availability and quality of those resources obtained from sources external to the site.

5 Protective devices provided for essential resource components or systems should be limited to those which are necessary, and consistent with plant requirements. Their possible action should be taken into account in the reliability assessment.

3.8 PLANT CONTAINMENT AND VENTILATION

Introduction

The following principles are concerned with those plant containment and ventilation features which are intended to ensure an acceptable level of radiological protection for persons on and off the site according to the basic principles of Parts 1 and 2.

The assessor should judge the extent to which the proposals in the safety submission conform to the principles in this Section.

General

1 The design should limit the dispersal of radioactive materials in accordance with the principles of Section 3.5 by containment and by appropriate ventilation and plant atmosphere clean-up systems.

2 Containment and ventilation systems should provide protection against the consequences of airborne contamination in normal operation and during and following specified faults, for persons on and off the site and for the environment. The safety submission should state and justify:

(a) the conditions, inside and outside the plant, that the containment and ventilation systems are designed to achieve.

(b) the safety limits on such conditions,

(c) the methods, instrumentation and design and operating variables proposed to effect control of these conditions, and

(d) the programme proposed for routine inspection and testing.

3 Fault analyses should take account of events which could impair the effectiveness of containment and ventilation systems.

The following principles should be deemed to apply unless it is shown that the total amount of radioactive materials concerned is sufficiently small or is in such a chemical or physical form as to make it inappropriate to apply a particular principle.

Plant Containment

4 Where containment systems form part of an effective barrier they should conform with the principles of Parts 1 and 2.

5 The safety suhission should show that t\e specified plant containment performance will be adequate for normal and fault conditions.

6 Containment boundaries should be defined. Waste storage, process vessels and piping which act as material containment barriers should where necessary be provided with further barriers so that failure or replacement of the material barrier does not result in undue hazard, in accordance with the principles of Section 2.3.

7 Piping, ducting and drains that may serve as routes for radioactive materials leaking from material containments should be provided with appropriate monitoring and alarm systems and means of isolation where feasible. Attention should be paid to the possibility of radioactive material backing up inactive feed lines.

8 Structures that house vessels and piping which normally hold radioactive liquids should include features designed to contain and recover these liquids in the event of leakage. The capacities of these features should be not less than the maximum possible leakage resulting from any discrete fault sequence. Allowance should also be made for additional liquids, such as cooling water, condensates, etc and any increase in volume needed for remedial action, **eg** dilution for cooling purposes. Means should be provided for the safe transfer of materials from these features to adequate reserve capacity in accordance with the principles of Section 3.2.

9 Sampling systems and other facilities should be provided to detect, locate, identify and quantify leakages of radioactive materials from the materials containment. Reflux due to condensation of vapour should be taken into account. There should **be** provision for appropriate environmental surveys in the plant proximity.

10 Systems should be provided for the removal where necessary of radioactive decay heat to prevent overheating and preserve the integrity of the containment systems under all foreseeable conditions.

11 Where appropriate, the design should take account of the possible generation, during normal and fault situations, of explosive mixtures including gases and vapours, so that the probability of containment impairment resulting from unplanned uncontrollable reactions is acceptably remote.

12 The containment design should take into account:

(a) the likelihood and extent of uncontrolled material accumulation over a period within the plant,

(b) the number and type of material movements, and the effect of transfer system malfunction or maloperation,

(c) processes involving possible significant energy release due to malfunction or maloperation,

(d) the quantity and location of combustible structural and process materials within the containment,

(e) external plant hazards,

(f) failure of essential resources, such as loss of ventilation air flow and pressure differentials,

(g) chemical and toxic properties,

(h) thermal and impulse loadings, including overpressurisation,

(i) any actions necessary following containment failure, and

(j) segregation and isolation of hazards where feasible.

13 Special precautions should be taken at the design stage to ensure that the requirements of principle 13 of Section 3.5 are met.

14 Consideration should be given to the need for servicing the plant containment and equipment and components in or associated with it. Access should be controlled and the exposure to radiation of persons involved in such servicing should be minimised by the design.

15 The need for access to the containment interior should be minimised. Such access facilities as m y be provided should be designed to ensure that the containment and ventilation systems are not thereby impaired.

16 Where routine access to the containment interior or other hazardous areas is permitted, appropriate emergency escape arrangements should be provided.

17 Provision should be made for inspecting and testing the plant containment.

Ventilation Systenrs

18 Ventilation of contaminated zones should be provided to limit the spread of contamination. The physical parameters on which this control is based should be specified.

19 Plant layout, the arrangements for personnel access and the ventilation of zones should be such as to minimise exposure to airborne contamination.

20 Appropriate provisions should be made for monitoring the variables referred to in principle 2(c), and for initiating alarms when limits specified in the suhission are exceeded. Special attention should be paid to the location of monitoring points and alarms.

21 Ventilation systems should be designed so that:

(a) clean and contaminated air streams are separate, with special consideration being given to the separation of process air and breathing air streams,

(b) discharges to the atmosphere are adequately cleaned,

(c) the flow of ventilation air within buildings is always from zones where the level of contamination is expected to be comparatively low to those where it is expected to be higher,

(d) the deleterious effects of toxic fumes and smoke are minimised,

(e) the build-up of dangerous gases in the containment systems and vessels is avoided,

(f) explosive mixtures of gases and vapours may be safely dealt with,

(g) the mixing of ventilation streams of different hazard potentials, *eg* explosive, toxic, radioactive, is prevented,

(h) overpressurisation is avoided, and

(i) condensation is controlled.

22 Ventilation systems for zones where there is the possibility of a significant combustible inventory should be provided with fire detection and alarm equipment.

23 Where there is the possibility of fire impairing or breaching the containment, fire suppression equipment should be provided.

24 The location of plant air intakes, should take account of possible air pressure fluctuations caused by aerodynamic disturbances from nearby structures. In addition, intakes should be sited so as to avoid contamination of intake air during normal and fault conditions, and consideration should be given to the inclusion of filters.

25 Facilities for the in-service testing of air cleaning systems should be provided where appropriate. It should be possible, periodically, to test the ventilation systems to determine whether the performance meets the design requirements. The submission should describe the proposed test arrangements and programme.

26 The ventilation system should ensure a suitable working environment for safety-related equipment during both normal and fault conditions, in accordance with the principles of Sections 3.4 and 3.6.

27 Attention should be paid to the location of discharge points so as to minimise the radiological consequences of releases, in accordance with the principles of Sections 3.2 and 3.4.

28 Special attention should be paid to the ventilation of control rooms to ensure satisfactory working environments.

29 Special attention should be paid to the design of glove boxes and their ventilation systems. The submission should state the measures proposed to prevent overpressurisation, and the provisions for coping with containment failure, especially the loss or failure of gloves.

30 Means should be provided for the isolation of ventilation systems in the event of fire or large releases of radioactive materials. Particular attention should be paid to zones here there are identified fire or explosion hazards. The ventilation system should be shown to be adequate after allowing for damage to local filters or other clean-up devices.

31 Consideration should be given to the consequences of interaction between ventilation systems.

32 The location of ventilation filters should be chosen so that high dose rates to plant personnel are avoided. Where necessary, shielding should be provided. Consideration should be given to the safe replacement of filter elements and the safe storage of contaminated filters.

3.9 mANTOPERATIm

Introduction

The principles in this Section are concerned with proposals for the safe conduct of operations. The safe control of plant requires the formulation and implementation of operating rules based on safety analyses carried out in accordance with the principles of Section 3.10, taking into account the state of the plant at any time during its lifetime. The safety submission should provide sufficient information on the proposed conduct of operations to enable the assessor to:

(a) evaluate the consequences of plant operation, with particular regard to the radiological exposures to which persons could be subjected, and to the extent and nature of radioactive wastes arising,

(b) identify all deleterious effects of plant operation on safety-related components that might lead to short term or cumulative damage such that the plant safety may be unacceptably reduced,

(c) ensure that the conditions in the plant at all times and the assumptions used in the relevant analyses are mutually consistent, and

(d) ensure that, notwithstanding the provision of managerial arrangements for the control of safety, adequate arrangements will be made to deal with emergencies.

In carrying out the assessment, the assessor should judge the extent to which the safety submission shows conformity with the principles in this Section.

Principles

1 The submission should identify flowsheets and flow diagrams, and the plant variables subject to conditions and limits, which are relevant to safe operation.

2 The proposed operating ranges, alarm and trip levels, and any other values of plant variables affecting safe operation should be stated and justified with regard to reasonably foreseeable extremes of plant behaviour.

3 Account should be taken of relevant combinations of the values of plant variables which may be expected, together with changes in plant.

4 Allowance should be made for the effects of abnormal situations on instrument and operator response times.

5 The submission should show how the plant will be operated to keep within the proposed conditions and limits. Allowance should be made for uncertainties in determining the state of the plant and for any foreseeable changes in the plant that may affect plant variables during its lifetime.

6 Conditions and limits should be incorporated in the operating rules, which should be readily available to the operator and written in such a way as to minimise the operator error.

7 The degree of operator involvement during fault conditons must be identified and assessed.

8 The operating rules should provide unambiguous guidance to the operator as to the correct response to any departure of the plant from its intended operating state.

9 The data specified in principles 1 and 2 should be reviewed, and revised when appropriate, to take account of:

(a) modifications to the plant during construction and commissioning;

(b) changes in the flowsheet data and technical information on which the plant design was based, and

(c) revisions of fault analyses.

10 The safety submission should outline the procedures for dealing with plant emergencies, and show that relevant plant procedures are consistent with existing site-wide arrangements for dealing with Site Emergencies and District Emergencies.

11 There should be arrangements for producing and implementing any emergency instructions required for the plant.

3.10 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 faults or abnormal conditions.

This Section is concerned with the assessment of analytical processes, as described in the safety submission, for discovering, characterising and evaluating postulated fault sequences for any plant. For the purpose of the principles these processes are referred to as fault analysis. The aim of fault analysis is to predict, when reasonably practicable, the behaviour of the plant and associated equipment in specific fault conditions, and to estimate the consequences of such faults and the likelihood of their occurrence, in quantitative terms.

In assessing analyses of faults, transients and abnormal conditions, the assessor should judge the extent to which the submission shows conformity with the principles in this Section.

Principles

1 Significant sources of radioactivity likely to be in the plant when a fault occurs should be identified and quantified and their form stated.

2 A systematic search should be made for routes and mechanisms, including chemical reactions, whereby these sources could give rise to a radiological hazard. Plant items which could have an effect on safety should be considered, together with a range of conditions covering the operation of the plant over its lifetime. The scope and limitations of this search should be stated. The fault analyses in any safety submission should be based on systematic and detailed studies which span a range of discrete faults, including common mode faults as accident initiating events, combinations of discrete faults and situations beyond the design basis of the plant. The assessor should be satisfied that the range of faults selected by the designer to make the safety case is sufficiently wide having regard to the range of all foreseeable faults.

3 Fault analyses should take into account predictable changes in the plant or its mode of operation during plant life.

4 The necessary technical information and data used for the purposes of fault analysis should be stated and justified.

5 Techniques using fault tree or event tree analysis should be regarded as aids in logical evaluation of the safety of any plant. Evidence from such analysis, where used, should be presented in the safety submission. These techniques should also be regarded as basic tools to be employed where appropriate by an assessor in examining certain cases where this seems to be justified.

6 Fault analysis should include an examination of those plant characteristics from which both the likelihood of the various discrete fault sequences and their consequences can 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 and operators. The analysis should take into account the possibility that safety-related items have become unreliable or inoperative before the fault sequence, or become so as a result of it.

7 The assumptions made in the fault analysis should be clearly stated and their validity demonstrated.

8 Fault analysis should be carried through until acceptable dose-frequency relationships as described in Section 2.1 have been demonstrated and long term plant stability has been shown to be assured.

9 Analysis of the behaviour and integrity of the plant and the protection systems provided to prevent or 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 sequence,

b) the importance of the safety feature to the overall safe course of the fault sequence,

c) the consequences of the fault sequence.

10 Where statistical data is employed to substantiate a reliability claim, it should be obtained from a relevant and sufficiently large population. The principles in section 3.11 should apply.

11 Consideration should be given to the need for an independent check of any fault analysis, using different methods and analytical models.

12 There should **be** confirmation, based on experience, 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, theoretical models and computer codes should be validated by appropriate experiments or tests.

13 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 reasonably foreseeable discrete fault sequences has been made,

(b) the groupings of fault sequences and the bounding case for each group of sequences are relevant to the particular fault under examination, and

(c) interaction between different groups of fault sequences is not significant.

14 The fault analysis should yield information relating to the behaviour of the plant during the fault sequences, in particular on:

(a) the performance required of the protection system and the plant operator *(eg* protective actions and functions such as safe shutdown, emergency cooling or containment), and of other safety-related items such as instrumentation,

(b) the margins to failure of safety-related components and the sensitivity of the predicted outcome of an accident to 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 basic principles relating to fault condition and protective system evaluation set out in Part 2,

(e) the frequency-consequence relationship for each fault sequence or bounding case to enable the requirements of principle 7 of Section 2.3 to be observed, and

(f) the magnitude of the radiological consequences of each fault sequence or bounding case, for comparison with the radiation exposure assessment levels given in principles 7 to 11 of Section 2.1.

3.11 RELIABILITY ANALYSIS

Introduction

Guidance is given in this Section on the conduct, presentation and assessment of system or component reliability analysis where this is required in a safety case relating to the safety of any nuclear plant.

In reviewing reliability analyses, where these form part of the safety suhission, the assessor should judge the extent to which they conform with the principles in this Section.

Principles

1 The reliability should be estimated for all reasonably foreseeable combinations of plant systems for which operation will be permitted. As an alternative to considering separately all permissible system combinations, they may be grouped where appropriate and a bounding case may be identified for each group. Such procedures should conform to the principles of Sections 2.3 and 3.10 relevant to the use of bounding cases.

2 The assumptions and claims which affect the conclusions of the reliability analysis should be justified and listed with the conclusions.

3 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 system 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, and

(f) other information needed for an understanding of the system operation.

4 The basis for any quoted failure rate, statistical distribution or other necessary factor should be stated.

5 The applicability of data used in reliability analyses to the components under analysis and their working conditions should be assessed. Where data has been extrapolated, it should be shown that such extrapolation is minor, or that appropriate allowance has been made. The data source, sample size, sample components and the working conditions assumed should be specified.

6 Reliability analyses should take account of possible variations, with time, of expected failure rates of systems or components.

7 The measures proposed, including test conditions, intervals between tests, and quality assurance, whereby the claimed reliability of systems and components will be achieved in practice, should be stated.

8 The relevant servicing procedures proposed, and their frequency and duration, should be stated.

9 Allowance made in the analysis for the time taken for off-line testing and maintenance of system components should reasonably reflect the tasks involved.

10 The reliability claimed for any human actions involved, such as servicing, should be based on the complexity of the task, the stress involved and other relevant factors. Repetitive actions should be suitably weighted.

11 When independent behaviour of components or operators is assumed, the basis for the assumption should be stated.

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

13 The possibility of common mode failure limits the reliability of a system no matter how much redundancy, diversity or separation is incorporated, and reliability claims should be assessed accordingly. For protection equipment the claimed reliability should be expected lie within the range corresponding to one failure per 10pto lo5 demands, depending on the novelty or complexity of the system.

14 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.

15 An examination should be made to determine whether the reliability of any component has a critical effect on the reliability of the system. For example, one method is to examine the effect on a system of putting the reliability of a component to zero. Where it is found that the component reliability is critical, special consideration should be given to the evidence on which the component reliability estimate is based.

3.12 EXTERNAL HAZARDS

Introduction

This Section is concerned with effects or events, whether natural or man-made, originating outside the plant, which could adversely influence plant safety.

The assessor should judge the extent to which the safety submission shows conformity with the principles in this Section.

General Principles

1 The submission should show that the plant would be located safely or designed to be safe in respect of external hazards.

2 Account should be taken of possible interactions between the plant and other plants on or near the site, particularly the effects of accidents in adjacent plants.

3 The simultaneous occurrence of external events should be considered only where there is a common m e connection, *eg* flooding resulting from an earthquake.

4 In analysing the effect of an external hazard the assumption should be made that the event occurs simultaneously with the maximum normal operating loads.

Extreme Weather Conditions

5 Consideration of the effects of extreme weather should be based on the best meteorological data available for the area. The submission should state the source of the meteorological data used in the safety analyses and describe any modifications to it that may have been necessary to adapt it to the site and its environs.

6 The assessment of the effects of abnormal weather should, as far as is reasonable in the light of meteorological evidence, take account of appropriate combinations of conditions such as:

(a) abnormal wind loadings,

(b) accumulated ice deposits on surfaces, inlets and outlets,

(c) high rainfall,

(d) heavy snowfall,

(e) lightning,

(f) spray, and

(9) fog,

7 Account should be taken of the effect of plant layout, building size and shape in localising wind loads sustained by various parts of the plant.

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

Seismic Effects

9 The data describing ground motion and its frequency of occurrence (ie the Seismic Design Basis) used for the aseismic design and analysis of the plant and subsequent testing and qualification of components should be specified and justified.

10 The plant should be designed adequately to withstand the motions and forces represented by the Seismic Design Basis.

11 The Seismic Design Basis should provide for the consideration of aftershocks.

12 Overall evaluation of the effect on the plant of any particular seismic event should take account of local ground conditions, including existing or projected man-made features, which could add to or modify the effects of an earthquake on the plant.

Water Ingress

13 For the purposes of design and analysis of the plant a maximum flood level and its frequency of occurrence should be specified and justified. In determining this level the best available data for the locality should be used. Furthermore, account should be taken of:

(a) for coastal sites, tides, 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 and tidal river sites, the combined effects of tide and flow as outlined in (a) and (b) above, and

(d) for sites in general, the maximum height of the local water table and the presence of perched water.

14 The plant design should be such that the specified flood shall not result in any adverse effects on plant safety.

15 Suitable drainage systems should be provided for the collection and disposal of water reaching the site from any source, including

(a) rainfall,

(b) flood defence overtopping by waves,

(c) flood defence leakage,

(d) spray,

(e) burst water mains,

(f) cooling towers, and

(g) subterranean drainage from the local water table and perched water,

and reasonable simultaneous ingress of water from these sources should be considered.

Fire, Brplosion, Missiles, etc

16 It should be shown that the plant, its protection systems and associated services are adequately protected from adverse effects resulting from fire, explosion, missiles, etc inside or outside the nuclear site. Existing and planned future developments should, where appropriate, also be considered.

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

18 The on-site use and storage of combustible materials in areas adjacent to, or containing, items im@rtant to safety should be controlled and accounted for, and kept to a practical minimum. Precautionary measures should be taken to reduce the amunt of combustibles, including vegetation, in the vicinity of the plant or near access routes.

19 Where hazardous substances or high pressure systems are used on the site it should be shown that the 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.

20 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 plant and personnel,

(b) the separation and isolation of hazardous substances,

(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 equipment or materials for use in emergencies, and

(g) servicing of each part of the plant containing a hazardous substance.

Aircraft Impact

21 The effect on the plant of aircraft impact on or near the nuclear site should be considered at the design stage.

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

23 Overflying of the site by aircraft is covered by the Air Navigation (Restriction of Flying) (Atomic Energy Establishments) Regulations 1976 (ref 8). The suhission should show that these regulations are taken into account in determining the need for protection.

3.13 LAYOUT

Introduction

The assessor needs to be satisfied that adequate consideration has been given to the disposition of buildings, structures, items of plant and equipment so as to minimise unwanted interaction and the effects of internal &d -external hazards. The safety suhission should also show that unauthorised access is prevented.

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

Principles

1 Entry to the site should be controlled. Any site or part of a site to which it is necessary to control access should be enclosed by a suitable fence or barrier, and security arrangements should be provided to prevent unauthorised entry.

2 Alternative means of access should be available for use as required, and these should be suitable for the types of vehicle that may be required on site in the event of an accident occurring on or adjacent to the site.

3 Vehicular and pedestrian traffic should be physically separated at the access locations.

4 Measures should be taken to prevent unauthorised access or interference to plant, safety-related plant, inactive feed plants and stores etc.

5 The layout of plant and associated changerooms within the site should be such that the area between plants may be classed as unrestricted for radiological exposure control purposes.

6 Site and, where necessary, building layout should provide adequate clearance, manoeuvring and parking space for large vehicles and their loads *eg.* flasks. Disposition of plants should facilitate and minimise flask movements. Plant layout should provide low radiation areas for flask monitoring.

7 Cranage provision must accommodate the particular requirements of each specific lifting operation. The disposition of plant and crane loads should be such as to minimise the hazards associated with load movements and crane failure. Proposals to use mobile cranes should receive special attention.

8 The layout of buildings and drains, particularly where large underground structures are involved, must take account of the flooding potential of the site, possible changes in water table and ground water mvements.

9 Building layout should, where possible, take advantage of natural features to facilitate drainage of both individual buildings and the site.

10 Essential services should be routed so that no single incident can cause disruption of supplies.

11 The layout of plants and plant services such as cooling towers, ventilation systems and drains should be such as to minimise interactions during both normal and fault situations. In accordance with principle 24 of Section 3.8,

(a) ventilation system discharges should have minimum impact on other plants, and

(b) ventilation system intakes should be designed so that the induction of engine exhaust gases, toxic gases or other harmful gases or vapours is avoided.

12 The layout of plants and plant interconnections such as pipe bridges and ducts should be arranged so as to minimise the effects of external hazards (including vehicles) and of any interactions between a failed structure, system or component and other safety-related structures, systems or components.

13 The disposition of the protection system equipment, ***eg.*** engineered safeguard systems, heat remval systems and essential resources including associated pipe and cable routes, should be such that no fault or other incident affecting the site will prevent the plant from being readily brought to a safe state or maintained therein.

14 Radioactive, toxic, explosive and flamnable materials, or processes involving such materials, should be separated from each other and from safety-related plant so that any accident to, or release of, such materials will not prevent the plant from being readily brought to a safe state and maintained therein.

15 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 that the plant could be readily brought to a safe state and maintained therein.

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

17 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, in particular from criticality incidents in unshielded facilities,

(d) site personnel will be physically protected from direct or indirect effects of the incident, and

(e) escape routes and assembly and decontamination areas will be available for contaminated personnel during evacuation; attention should be paid to the segregation of such personnel.

3.14 [illegible] (3HECRS AND CXMMISSIaJING

Introduction

This Section sets down assessment principles for those safety submission proposals for the post-construction activities which are designed to ensure that the plant, including its protection systems, will be adequately and safely commissioned and will operate as intended.

The assessor should judge the extent to which the suhitted proposals for installation checks and commissioning show conformity with these principles.

Principles for Installation Checks

1 Installation checks for a plant or section of plant should be completed prior to the commissioning of the plant or section of plant.

2 Installation checks should be adequately documented.

3 The assessor should be satisfied that on completion the plant would not differ significantly from the designs on which the safety analyses were based, or that the safety analyses have been modified satisfactorily to take account of any changes made.

4 Installation checks should determine either that the plant is acceptable for commissioning, or that modifications are required where the plant is found not to conform to the expected state. The submission should define the responsibilities and arrangements for acceptance or modification, and these activities should be based on any necessary reappraisal of the safety case for the plant or part of the plant concerned.

5 The effects of any modifications arising out of installation checks should be taken into account in the preparation of the schedule of commissioning activities.

6 The safety submission should describe the provision made for the continual updating, at all stages, of plant drawings and other records as modifications are introduced.

Principles for Mssioninq

7 The commissioning programne should define:

(a) the stages of commissioning, e.g. section-by-section, inactive, trace active, active, etc.,

(b) the procedure for mving from one stage to the next, and

(c) the allocation of responsibilities at each commissioning stage.

8 The procedure referred to in principle 7(b) should include the production of commissioning reports at each stage, together with the formal procedures for authorisation of commencement of the next stage of commissioning.

9 The sutssnission should define the point at which commissioning would be deemed to be complete.

10 Details of responsibilities and arrangements for plant modifications arising out of commissioning activities should be included in the general procedures for modifications. These arrangements should include the introduction and removal of temporary mdifications. There should be provision for the keeping of records of temporary modifications.

11 The plant should be safely commissioned so that no stage of the testing and commissioning would lead to an unacceptable risk. In particular, any modification or temporary system used £.or the purpose of commissioning should not impair plant safety.

12 The testing, commissioning and safety assessment documents should **be** mutually consistent in respect of modifications that are made during installation checking and commissioning.

13 The commissioning schedule should be designed to demonstrate adequately that the safety provisions will operate as intended.

3.15 SERVICING

The requirement to keep the plant in a reliable and safe state necessitates servicing, and arrangements have to be made at the design stage and throughout the plant life for this function to be adequately performed.

In carrying out an assessment of servicing proposals, the assessor should judge the extent to which the submission shows conformity with the principles in this Section

Principles

1 The submission should review the probable need, extent, periodicity and duration of servicing work on the plant. The review should apply particularly to those items of plant which have a significant effect on safety or on productive capacity, or where significant exposures may be given to persons carrying out the servicing work.

2 It should be shown that the plant and safety-related structures, systems and components are designed so as to facilitate servicing safely, and to the extent predicted to be necessary by the above review.

3 The expected initial state of the plant should be capable of confirmation by appropriate tests and inspection before the plant is put into operation. These results should be used as a basis for evaluating those of subsequent tests and inspections during plant life.

4 Safety-related structures, systems and components should, where reasonably practicable, be capable of being type-tested under conditions at least equal to the m s t severe expected in service.

5 Safety-related structures, systems and components should be capable of being monitored and inspected in operation or at intervals throughout plant life commensurate with the expected reliability of each item. In especially difficult circumstances, it may be acceptable for additional design measures to be taken to compensate for any inability to monitor or inspect.

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

7 Provision should be made for routine inservice functional testing of all safety-related systems. Where complete system testing is not reasonably practicable the best subsystem tests and closest representation of required operating conditions should be employed. It should be pssible to carry out these tests without degradation of plant protection.

8 Provision should be made for periodic sampling of material properties where changes in such properties could adversely affect safety.

9 The submission should show that during servicing the plant can be kept in a safe state, and that radioactive releases will be minimised. Special attention should be paid to the possibility of servicing activities causing common mode failures in supply systems.

10 The proposals should be such that adequate supervision will be available to ensure that servicing is carried out correctly and that the plant is returned safely to its proper working state.

11 The design of the plant should be such as to minimise both individual and collective radiation doses from servicing during the life of the plant, provided that these proposals would not result in unacceptable increases in doses during normal operation.

3.16 DECOMMISSIONING

Introduction

At the end of its operating life a nuclear chemical plant would be maintained in a safe state for some time and then be dismantled and disposed of. It is important that for a new plant these activities should be considered at an early stage so that the proposed design and the operating procedures do not impede or prevent the safe decommissioning of the plant. The safety submission for a new plant should therefore describe the provisions made at the design stage for facilitating safe decommissioning, and the storage and eventual disposal of waste which arises during decommissioning.

A detailed decommissioning plan and associated safety submission would not be expected to be available until shortly before decommissioning was to be undertaken, and therefore there may be two stages of assessment, at which different principles will apply. For this reason the principles of this Section are divided into two parts, namely, those which apply before a new plant is built, and those additional principles which apply when an existing plant is to be decomissioned. It should be noted that the assessment principles set out in other parts of this document should also be applied where they are relevant to any decomissioning proposal.

The assessor should judge the extent to which a decommissioning safety submission shows conformity with the principles of this Section.

Principles wlicable to Proposals for New Plant

1 The submission should show how the plans for decommissioning relate to operator's policy for decommissioning redundant plant and restoration of the plant site.

2 The safety submissicr s??uld show that it will be possible to empty the plant without causing excessive exposures. It should cover removal from the plant of hazardous materials, their conditioning where necessary, and their appropriate storage or disposal.

3 It should be made evident that no aspect of design or m e of operation is likely to impede or prevent the safe decontamination of plant and buildings and their surroundings.

4 The proposed design should make possible the safe access necessary to carry out planned dismantling after decontamination.

5 The submission should show that the proposed design would not obstruct the eventual safe removal of plant, buildings and radioactive materials, and the restoration of the plant site.

6 The proposed design and operation of plants and buildings should be such that, following the end of their operational lives, they can be maintained in a safe condition with minimum surveillance until they are dismantled. Where it is intended to defer the start of dismantling, or to interrupt the dismantling at intermediate stages, the plant and buildings should be capable of being safely maintained during each stage.

7 There should be provision for the keeping of records of methods and details of construction and modification of the plant with particular regard to the proposed methods of dismantling. In this context films, video tapes and photographs of the "as built" and "as mdified" status of the plant should be used.

8 The potential effects, on decomissioning, of reasonably foreseeable accidents and spillages during operation should be discussed in the safety suhission. In particular, consideration should be given to the need to retrieve and contain process material, solid, liquid and gaseous effluents, and other waste and scrap.

9 The safety submission should describe:

(a) the means by which unnecessary contamination of items of plant or structures during operation would be avoided,

(b) the provisions for monitoring plant variables relevant to decommissioning, and in particular for taking measurements and samples to establish an accurate inventory of radioactive materials,

(c) the proposed procedures for measuring and recording, during the plant lifetime, radiation and contamination levels, and spillages of radioactive materials, and

(d) the provisions adopted to facilitate decontamination, plant dismantling and building demlition.

10 The waste storage facilities and, where possible, the disposal routes intended to be used during decommissioning, should be outlined in the safety submission.

Principles Applicable to Prapsals for Existinq Plant

11 The safety submission should include a clear statement of the objectives of the decommissioning project with particular regard to the extent to which decommissioning is to be carried out.

12 When partial decomissioning is proposed, the policy for the eventual attainment of unrestricted use of the site should be outlined.

13 The radiation and contamination levels and the radioactive inventory at the beginning and end of each stage of decomissioning should be specified.

14 A detailed decommissioning programme should be submitted, indicating the times at which existing facilities, and the various installed services, may be required to be modified or replaced.

15 Arrangements should be specified for the monitoring of the continued adequacy of facilities and services as decommissioning proceeds.

16 The submission should show that access routes for vehicles, plant and equipment during decommissioning have been selected with due regard for the safety of adjacent plants and services. The means and routes for transporting active and inactive wastes to storage or disposal should be described.

17 The submission should identify and quantify the arisings of active and inactive wastes and scrap. For each material the submission should describe:

(a) the arrangements for segregating various arisings,

(b) any conditioning process that may be proposed, and

(c) the proposed methods of storage and disposal.

18 Adequate information should be provided on:

(a) proposed methods of removing inadvertent contamination,

(b) arrangements for in situ decontamination, and

(c) methods of isolating the plant from other radioactive systems or sources on the site.

19 The work which needs to be carried out remotely should be identified, and the stage at which man access is required should be indicated.

20 The proposal should specify the methods to be used for controlling the arisings and subsequent safe treatment of materials used during decontamination, such as detergents, reagents, large volumes of water, etc.

21 Arrangements should be described for measuring and recording the radiation and contamination levels, and the radioactive inventory, during the course of decommissioning, to assist in dose control, the monitoring of progress and the planning of future activities.

22 The proposal should give details of an appropriate surveillance programme for the decommissioned plant or site. Where only partial decommissioning is planned, the programme should include measures for ascertaining the rates and modes of deterioration of plant and buildings and the consequent radiological hazard following decommissioning. Where only some sections of a plant are to be decommissioned or refurbished, the surveillance programme should provide for monitoring to ensure that interactions between plant sections would not adversely affect subsequent decommissioning activities.

4 MANAGEMENT PRINCIPLES

4.1 THE MANAGEMENT OF SAFETY

Introduction

Nuclear chemical plants can vary widely in size, function and location, and hence can have marked differences in the safety aspects of design, construction and operation. Furthermore an individual plant m y be isolated or it may be part of an interrelated system of plants on a single site.

It would not be reasonable or desirable to provide detailed assessment principles to cover the management of safety for the whole range of possibilities, and therefore this section has been limited to basic principles applicable to a new plant on a site which is assumed to accommodate other plants and to have an existing site-wide safety management organisation.

The assessor should examine the proposed safety management organisation and its responsibilities on the new plant and also the relationship between plant-specific and site-wide organisations, and judge the extent to which the safety management proposals conform with the principles in this Section.

Principles

1 The safety-related responsibilites of line management should ke clearly assigned for all phases of plant design, construction, commissioning and operation, and there should be arrangements for the delegation of authority. These responsibilities should be assigned prior to their assumption and in sufficient time for them to be included in the assessment.

2 The responsibilities of the plant management and the roles of associated departments should ke specified for all phases of the plant's life. The physical boundaries of each management responsibility should be shown, s that the various responsibilities of, and the interfaces between, plant management and the management of other plants, site management, service departments and contractor's personnel are clearly delineated.

3 The safety submission should specify the resources available, both directly and indirectly, which would enable the plant management to discharge its safety-related responsibilities.

4 There should be procedures for authorising and implementing safety management systems, such as the permit-to-work system.

5 At each stage of the project there should be made available a list of safety documents which had been or would be produced.

6 There should be procedures for identifying, updating and preserving documents and records relevant to plant safety. Particular attention should be paid to those documents which would assist management in the event of incidents, modifications and decommissioning, or which would contribute to improvements in plant design.

7 Arrangements should be specified for the production and updating of a comprehensive plant manual containing a plant description with sketches or photographs. This should include base-line data so that the extent of departures from the original condition of the plant may be ascertained.

4.2 QUALITY ASSURANCE

Introduction

Quality assurance is a management system used to provide assurance that there is adequate control of the design, manufacture, construction, commissioning and operation of plant. Its function is to ensure as far as is practicable that all specifications for the achievement of safe conditions 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.

Principles

1 An effective quality assurance programme should be in force in respect of safety-related aspects of a plant during design, procurement, manufacture, construction, commissioning, operation and decommissioning.

2 The proposed quality assurance programme and the organisation to implement it should be described in the safety submission presented in respect of the plant. The relationship of that quality assurance system to any existing quality assurance organisation should be described.

3 The plant should be designed, constructed, commissioned and operated in such a manner as to allow the requirements of the quality assurance programme to be effectively implemented.

4 The overall requirements and principles set out in the programme referred to in principle 2 should form the basis for subordinate programmes proposed by main contractors and subcontractors in any project to design and construct plant.

5 The occupier should be responsible for planning and implementing quality assurance in his own organisation and for ensuring that agreed quality assurance is implemented by each contractor and his sub-contractors.

6 Any quality assurance organisation and all persons having responsibilities for quality assurance should be independent of the commercial requirements of production and progress.

7 Quality assurance personnel shall have the authority within their own organisation to recommend a stoppage of work through appropriate management in the event of unauthorised departures from agreed procedures.

8 Requirements of the quality assurance programme should be carried out in accordance with appropriate procedures and the results documented so that they can be easily retrieved and verified independently.

9 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 by the occupier within his own organisation and within those of the main contractors who should in turn similarly demonstrate the effectiveness of their audits on their sub-contractors.

10 Internal audits should be conducted by persons who have no responsibilty for the function under audit.

11 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.

12 Quality assurance should be applied to modifications, additions or changes to the plant.

REFERENCES

1 Safety Assessment Principles for Nuclear Power Reactors. Health and Safety Executive, 1979.

2 Nuclear Installations Act 1965 (as amended).

3 Health and Safety at Work etc Act, 1974.

4 The Nuclear Installations Regulations, 1971. Statutory Instrument No. 381.

5 Recommendations of the International Commission on Radiological Protection, ICRP Publication 26, 1977.

6 EEC Directive of 15 July 1980, giving the revised basic safety standards for the health protection of the general public and workers against the dangers of ionising radiation.

7 Radioactive Substances Act, 1960.

8 Air Navigation (Restriction of Flying)(Atomic Energy Establishments) Regulations, 1976. Statutory Instrument No. 1986

9 Limits for Intakes of Radionuclides by Workers, I C E Publication 30, l979/8l.

10 Radiation Quantities and Units, International Commission on Radiological Units, ICRU Report No.33, 1980.

11 Report of the Task Group on Reference Man, ICRP Publication 23, 1975.

12 Redgrave's Health and Safety in Factories, 1982. Butterworth, Shaw & Sons.

13 Specifications in relation to Emergency Reference Levels. National Radiological Protection Board. **ERL** 2 (1981).

14 Cmnd 6820. The Government's Response to the Sixth Report of the Royal Commission on Environmental Pollution (Cmnd 6618), May 1977..

15 The Ionising Radiations (Unsealed Radioactive Substances) Regulations, 1968. Statutory Instrument No. 780.

GLOSSARY

In this document the terms listed below have the following meanings respectively, unless otherwise required by the context.

ABSORBED DOSE	–	The amount of energy deposited in a substance exposed to radiation.
ADEQUATE	–	The necessary and sufficient extent of any measure designed to achieve compliance with these principles.
ANNUAL GROUP AVERAGE DOSE	–	The collective dose received in any one year, divided by the number of persons in the group.
ANNUAL LIMIT OF INTAKE (ALI)	–	Maximum permissible annual intake by a person of a radionuclide, as recommended in **ICRP** 30. (ref 9)
ASSESSOR	–	Person assigned by **HMNII** to review proposals for nuclear installations in order to judge their compliance with principles in this document and elsewhere.
BECQUEREL **(Bq)**	–	Special name for the unit of activity. One **Bq** is equivalent to one disintegration per second. See ICRU Report 33. (ref 10)
BEST ESTIMATE	–	When used to describe the results of any fault analysis, it means that the analysis has been made using data directly applicable to the type of fault under consideration. The Best Estimate would, therefore, be expected to provide the most accurate, although not the most conservative, descriptions of the fault and its consequences that could be achieved within the limitations of the analytical model employed. (See Conservative Estimate.)
BOUNDING CASE	–	The case which represents the extreme, in respect of the condition of interest in a particular study, of a group of discrete fault sequences.
CHANNEL	–	A non-redundant chain of equipment to the point of combination with other identical channels or single output function.
CLASSIFIED PERSONS	–	Those exposed workers who might receive during their employment annual doses in excess of three-tenths of the maximum annual dose permitted for workers aged 18 years or more.
COLLECTWE DOSE	–	Sum of individual doses of a specified type received by a specified group of persons.
COMMITTED DOSE	–	The dose that will be accumulated in a given organ or tissue over 50 years following a single intake of radioactive material by a member of a specified population.

COMMON MODE FAILURES	–	Failures in different plant components or systems due to a single initiating event or cause.
COMPATIBLE MATERIALS	–	Materials that do not react deleteriously when brought into contact.
COMPONENT	–	Any part of a plant which represents the smallest unit considered in the assessment.
CONSERVATIVE ESTIMATE	–	Used where there is sufficient reasonable doubt in the accuracy of data to prevent a Best Estimate from being made. In this case, the data, assumptions and methods used for the analysis of a fault and its consequences would be such as to give a result bounding the Best Estimate on the safe side.
CONSEQUENCES	–	The results of an accident in terms of detriment to the health of persons.
CRITICALITY	–	An assembly of fissile material is said to have achieved criticality when it becomes just capable of sustaining a nuclear chain reaction.
CURIE (Ci)	–	Unit of radioactivity, equivalent to 3.7 x 10l0 disintegrations per second. (1 Ci = 3.7 x 10l0 *Eq)*
DECAY HEAT	–	The energy liberated during radioactive decay manifested as heat.
DERIVED AIR CONCENTRATION (DAC)	–	The DAC for any radionuclide is that concentration in air which, if breathed by Reference Man (re£ 11) would give the Annual Limit of Intake by Inhalation (re£ 9).
DERIVED LIMIT	–	The values of surface and airborne contamination derived from consideration of working conditions that would give to any person a total dose (direct plus committed) equal to the appropriate limit.
DISCRETE FAULT SEQUENCE	–	Any specific chain of successive events starting from an initial fault and proceeding to that pint at which the sequence and its consequences are fully developed.
DISPOSAL	–	The dispersal of radioactive waste into an environmental medium, or emplacement in a facility, either engineered or natural, with the intention of taking no further action apart from necessary monitoring. (re£ 14)
DIVERSITY	–	Dissimilar means of achieving the same objective. Usually refers to the use of different methods, components, materials, etc, in redundant safety systems to minimise the probability of simultaneous failure from the same cause.

DOSE	-	Dose equivalent, which is the absorbed dose weighted by modifying factors intended to make the dose equivalent correlate better with the m r e important deleterious effects os exposure to radiation than does absorbed dose alone. (re£ 5)
DOSE RATE	-	Dose received per unit time.
DOSE LIMITS	-	The maximum doses permitted for various classes of persons under statutory provisions.
EFFECTIVE BARRIER	-	A passive or active engineered provision, or group of provisions, provided to prevent or terminate any discrete fault sequence which might otherwise cause a radiological hazard.
EFFECTIVE IX)SE	-	Effective dose equivalent, which is the sum, for certain tissues of the human body, of the products of dose to a particular tissue and the weighting factor for that tissue, to take account of the different sensitivities to biological damage of different tissues. (ref 5.)
ENVIRONMENTAL SURVEY	-	A programme of monitoring for radioactivity in the vicinity of a nuclear installation.
EQUIPMENT	-	Items of plant, components, instrumentation and appliances but not major structures.
ESSENTIAL RESOURCES	-	Those services and materials necessary to ensure the attainment and maintenance of a safe state in the plant. These may include electricity, steam, energy storage systems, water, gases, etc
EXPOSED WORKERS	-	Persons who might receive, during their employment, annual doses in excess of one-tenth of the annual dose limits for workers aged 18 or over.
EXPOSURE	-	The state of being subjected to ionising radiation above normal background level.
FAILURE	-	When used in safety analyses, a failure is said to have occurred when part of the plant equipment ceases to operate in the correct manner or does not operate when called upon to do so. Failure may also describe unplanned isolation of plant from external supplies.
FAULT	-	Any unplanned departure from the specified operating mode of a system or component because of failure or maloperation. Fault condition describes the status of a plant after a fault has occurred and before it has been corrected.

FISSILE MATERUG – Material which contains quantities of elements of atomic number greater than 91 capable of sustaining a nuclear chain reaction.

MALOPERATION – The result of operator error.

M A T E m CONTAINMENT – All those receptacles, items of equipnent or plant components, that may contain radioactive materials during normal operation, which normally prevent or limit the spread of such materials into the plant containment or the environment.

MINIMISE – To reduce to as low a level as is reasonably practicable.

MONITORING – Continuous or continual observation of the state of a plant, site or its environs, particularly with regard to radiation levels.

NON-BREAK ELECTRICAL SUPPLY – A supply that is designed to be available with high reliability.

NORMAL OPERATION – The state of a plant when it is not in a fault condition and not being decommissioned. Normal operation includes servicing, commissioning, experimentation and shutdown.

NUCLEAR ASSEMBLY, NUCLEAR INSTALLATION – See refs 2 and 4.

NUCLEAR CHEMICAL PLANT – any installation designed or adapted for:-

a) the carrying out of any process which is preparatory or ancillary to the production or use of atomic energy, and which involves or is capable of causing the emission of ionising radiations; or

b) the storage, processing, or disposal of nuclear fuel or of bulk quantities of other radioactive matter. (See Section 1 (1)(b) Nuclear Installations Act 1965.)

OCCUPIER – The corporate body responsible for the safe operation of a nuclear installation.

PLANT CONTAINMENT – Any structural membrane other than materials containment which is capable of limiting the accidental or planned release of radioactive materials to the environment.

POSTULATED FAULT – Any discrete fault sequence assumed as a basis for accident analysis. A postulated fault may be used to determine the probability and consequences of an accident, to provide a basis for the design of a plant (including its protective features) or to evaluate the response of a plant to such a fault.

PROTECTIVE ACTION – A single action performed by an operator or a channel or group of parallel channels as a step towards maintaining or restoring safe conditions, *eg* closing a containment isolating valve.

PrnCTIvE FUNCTION – The primary purpose of taking one or more protective actions, *eg* to seal off the contaiment.

PROTECTION SYSTEM – All the equipment designed to act in response to a fault to prevent or control the development of any unsafe state of the plant. Each protection system is assigned a particular function, although protection against certain fault conditions may require the action of more than one system.

PROVEN – A plant design may be said to be proven when convincing evidence exists that a sufficiently similar plant has been satisfactorily operated, or that sufficient confidence in the design of proposed novel features has been established by the testing of any significant departures from accepted practice.

RADIOACTIVE MATERIAL – Any substance whose specific activity exceeds 0.002 microcuries per gram of substance (74 Bq/g). (re£ 15)

RADIOACTIVE SCRAP – Any radioactive material other than spent fuel which it is intended to recycle or salvage. (Ref 14).

RADIOACTIVE WASTE – Radioactive material for which at the present time there is no known, anticipated or feasible economic use. (Re£ 14).

RADIOLOGICAL PrnCTION – *Any* measure that m y be taken to limit, reduce or estimate exposure to ionising radiation.

REASONABLY PRACTICABLE – Has the meaning assigned to it within the context of the Health and Safety at Work etc Act. (re£ 3) See also ~edgrave's Health and Safety in Factories (**re£** 12). This generally implies that in order to demonstrate that measures for reducing a risk are not reasonably practicable it must be shown that the expense, time and trouble that would be incurred in taking such measures would significantly outweigh the benefit that would result from reducing the risk..

REDUNDANCY - The provision of equipnent in excess of the minimum required to perform a given function.

REFERENCE MAN - A set of anatomical and physiological standards used to define an adult person as a basis for setting limits to radioactive intake. (ref. 11)

RELFVANT SITE - Has the meaning assigned in Section 26 of ref. 3.

RELEVANT STATUTORY PROVISIONS - The provisions of Part 1 of the Health and Safety at Work etc Act, 1974 and any Health and Safety Regulations made under that Act, and those Acts, and Regulations made under those Acts, specified in Schedule 1 of the Health and Safety at Work etc Act 1974.

RELIABILITY - A measure of the probability that equipnent will continue to function correctly or will function correctly when called upon to do so.

REM - Roentgen-equivalent-man. A special unit of dose equivalent. Use of the rem is being phased out in favour of the sievert. (ref. 10.)

RISK - The probability of a defined adverse event.

SAFE - A plant or part of a plant is considered to be safe (or in a safe state) when it is in all respects stable, under control and within the operating limits specified for limiting the risks due to that plant.

SAFETY-RELATED - Any aspect of plant design, construction or operation which could influence the initiation, detection or limitation of a fault and its consequences.

SAFETY **PARAMETERS** - Those physical quantities that are measured for the purpose of ensuring a safe state.

SAFETYSUBMISSION - All the information suhitted to HMNII for assessment prior to the construction, operation or deco~ssioningof any nuclear installation.

SECSECATION - The physical separation of corrq?onents, systems, circuits, etc, to reduce the probability of common mode failures.

SERVICING - An cannibus term used in this document to denote maintenance, inspection, testing, modification, repair, and replacement. Servicing is part of normal operation.

SI- (Sv) - The special name for the unit of dose equivalent (1 Sv = 1 Joule/kilcgram = 100 rem) (ref 10)

SINGLE FAILURE - The failure of a single component, channel or system to perform its designed function.

SITE - For licensed sites, the area defined by the nuclear site licence and delimited by the site boundary; for other relevant sites, the area to which the occupier controls access.

STORAGE - The anplacement in a facility, either engineered or natural, with the intention of taking further action at a later time, and in such a way and location that such action is expected to be feasible. The action may involve retrieval, treatment in situ or a declaration that further action is no longer needed, and that storage has thus become disposal. (ref 14).