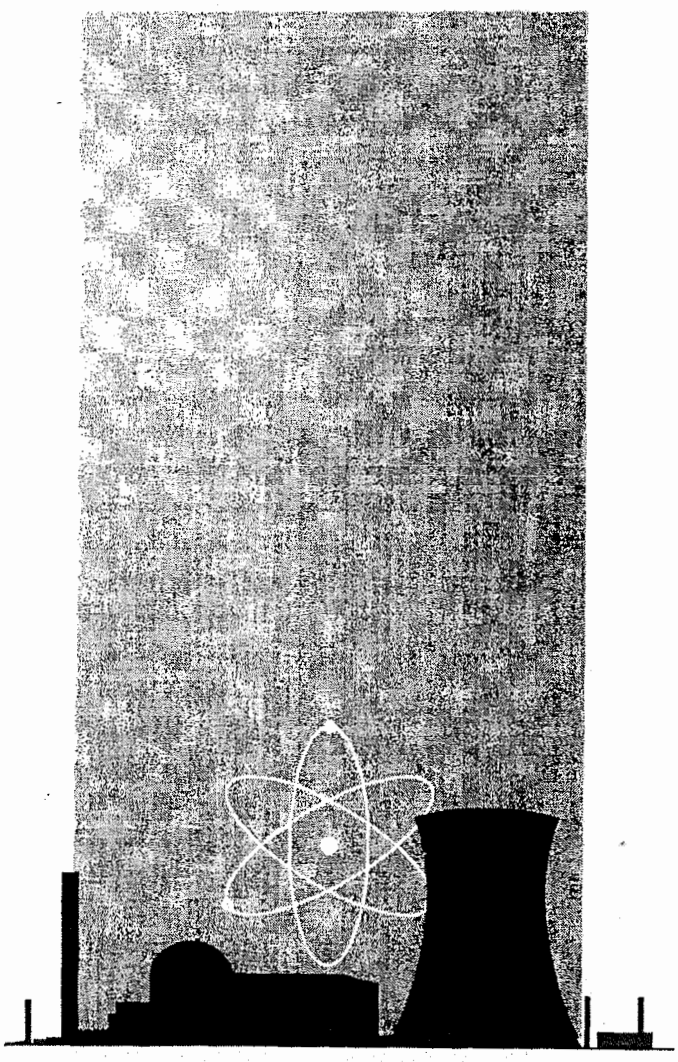
HSE
Health & Safety Executive

This version of the SAPs has been superseded by the 2014 version.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

SAFETY ASSESSMENT PRINCIPLES FOR NUCLEAR PLANTS



First published 1992
Reprinted 1998

ISBN 0 11 882043 5

Safety assessment principles for nuclear plants

CONTENTS

PREFACE

The Nuclear Installations Inspectorate (NII) is employed as part of the Health and Safety Executive (HSE) to regulate the safety of nuclear installations in the UK. Under UK law, certain nuclear plants prescribed under the Nuclear Installations Act (1965) must be licensed. The safety of a nuclear plant is the responsibility of the licensee, who is required to submit to the NII a written demonstration of safety, the safety case, which is periodically updated to reflect changing conditions. Assessment is the process by which NII, on behalf of HSE, establishes whether the safety case is adequate and the Safety Assessment Principles are used for that purpose.

NII Safety Assessment Principles (SAPs) were first published in 1979 for nuclear reactors. Corresponding principles for nuclear chemical plant followed in 1983. The principles were amended in 1988, following a recommendation by Sir Frank Layfield arising from the Sizewell 'B' inquiry. Layfield noted that differences existed between the CEGB Design Safety Criteria and the NII SAPs and recommended that "NII's Safety Assessment Principles and CEGB's Design Safety Criteria and Guidelines should be re-examined to eliminate avoidable inconsistencies." He also recommended that HSE should publish for discussion its thinking on risk asessment. The HSE paper *The Tolerability of Risk from Nuclear Power Stations* (1988, revised in 1992) emerged in response. It provides guidance on levels of tolerability by comparison with other risks which are borne by society in return for certain benefits. It thus provides a more systematic and unified approach to risk assessment, so helping the assessor to decide "how safe is safe enough?".

Events have moved on since the Sizewell inquiry. It has been decided to undertake a thorough revision of all the SAPs with the following objectives:

(a) consolidate the revisions made as a result of the recommendations of the Sizewell 'B' inquiry;

(b) implement lessons learned since first publication;

(c) ensure greater consistency with international criteria (IAEA Safety Standards, Codes and Guides);

(d) implement suggestions made in HSE's 'Tolerability of Risk' paper (1988) and also in its 1992 revision;

(e) combine power reactor and chemical plant SAPs.

The present Safety Assessment Principles are the result of this revision.

Dr S A Harbison
HM Chief Inspector
Nuclear Installations Inspectorate
Baynards House
1 Chepstow Place
Westbourne Grove
London W2 4TF

INTRODUCTION

Regulatory background

1 The operators of nuclear plants in this country are like their counterparts in other industries, and places of work in general, in that they must conform to the general health and safety standards laid down in the Health and Safety at Work etc Act 1974 (HSW Act). In particular it is their duty:

> to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all their employees (Section 2 of the HSW Act); and
>
> to conduct their undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in their employment who may be affected are not thereby exposed to risks to their health or safety (Section 3 of the HSW Act).

This means that measures necessary to avert risk must be taken until or unless the cost of those measures, whether in money, time or trouble, is grossly disproportionate to the risk which would thereby be averted. In short, risk must be reduced to a level which is as low as reasonably practicable (ALARP): this is the 'ALARP principle'.

2 The nuclear industry differs from other industries in that it must also comply with the Nuclear Installations Act 1965 (as amended). The NI Act is a piece of legislation, subsidiary to the HSW Act, which applies specific regulatory controls to nuclear plants. Under this Act, apart from certain exceptions, no site may be used for the purpose of installing or operating any nuclear installation unless a licence has been granted by the Health and Safety Executive (HSE). Licensed installations currently in operation include nuclear power stations and research reactors, nuclear fuel manufacturing and isotope production facilities, fuel stores, fuel reprocessing plants, radioactive waste stores, and a site for both storage and disposal of radioactive waste.

3 Inspectors are appointed under the HSW Act to administer the NI Act. The Nuclear Safety Division of HSE exercises that reponsibility through HM Nuclear Installations Inspectorate (NII). The NII has within its remit the responsibility for granting licences, for attaching appropriate conditions to the licences and for making judgements on the acceptability of responses made by licensees to the requirements of those conditions. (The term 'licensee' is used in this document to include applicants for licences as well as those who already hold licences.)

4 HSE published the NII's safety assessment principles (SAPs) for nuclear power reactors in 1979[1] and for nuclear chemical plants in 1983[2] and issued an amendment to the SAPs in 1988[9]. Since that time HSE has advanced its thinking on the tolerability of risk from nuclear power stations in a paper, *The Tolerability of Risk from Nuclear Power Stations*[3b], a revised version of which has recently been published. This follows an earlier discussion paper[3a] published in 1988. Its general approach to the regulation of risks, in which the ALARP principle again plays a central role, may be summarised in the following way:

(a) For any activity the level of risk may be so great that the activity cannot be allowed to continue. This upper limit defines the boundary between risks which are just tolerable and those which are intolerable.

(b) Even when the level of risk is tolerable, it must be reduced to a level which is as low as reasonably practicable.

(c) A point is reached at which the risk is, or has been made, so small that no further precaution is necessary.

5 This approach is followed by the NII in its assessment work and, for the purposes of that work, is translated into more specific requirements, which are described below.

Safety assessment

6 The process adopted by the NII in making decisions on the granting of a licence requires a safety case and supporting reports to be submitted by the licensee for assessment by the NII. The Inspectorate needs to adopt a consistent and uniform approach to the assessment process; to this end it is necessary to provide a framework which can be used as a reference for the technical judgements that the assessors have to make. The NII's safety assessment principles (SAPs) form such a framework. This document updates and consolidates the earlier publications of its nuclear power plant and nuclear chemical plant principles.

7 In carrying out an assessment, the NII assessors need to judge the extent to which the safety submission shows that the design of the plant is in conformity with the principles. Not all of the principles are relevant to every plant, but the extent to which the relevant principles are met will be an important factor in any decision on licensing. The law requires the plant to be as safe as reasonably practicable. Some of the principles embody specific statutory limits. Apart from

these, the principles in this document should be met as far as is reasonably practicable, and that expression could have been written, at the risk of being tediously repetitive, into almost every SAP. There cannot, therefore, be a rigid interpretation of the principles. On the other hand, the engineering principles in particular represent the NII's view of good practice and we would not expect modern plants to have difficulty in satisfying the majority of them.

8 The revised SAPs are aimed primarily at the safety assessment of proposed (new) nuclear plants, but they will also be used in assessing existing plants. In so far as the principles are drafted for application to designs rather than hardware and to the safety analysis of those designs, the principles are forward-looking in nature. However, following the granting of a licence, the proposed plant in due course goes through construction and commissioning stages into operation and ultimately decommissioning. The assessment principles have to look further into the future, therefore, in order to recognise those developments and seek preparatory work by the licensee at the design stage in anticipation of them; but the principles have to avoid imposing in the pre-licensing stage the regulatory requirements which will apply when the design becomes a reality.

9 Drawing this line can cause conceptual problems particularly because, as indicated above, the SAPs will also be used in the assessment of existing plants. Assessment continues through all phases of a plant's life - when a modification is proposed to an operating plant for example. The principles will be used through all of those phases, both for plants that will be built in the future and for plants which exist today. The important point to note is that, in this use, the principles will be augmented by licence conditions which will then require arrangements to be made, procedures written etc, that take some of the forward-looking requirements of the SAPs into a form more appropriate to an actual plant.

10 For the assessment of plants which exist today ('old plants') there is a further point to be considered in that the safety standards used in their design and construction may differ from those used in plants currently being designed and built. The existence of such differences has to be recognised by our assessors when applying the SAPs in the assessment of old plants. The ALARP principle is of particular importance to such assessments, and the age of the plant and its projected life are important factors to be taken into account when making judgements on the reasonable practicability of making improvements to those plants.

11 The principles are written bearing in mind existing and anticipated plant designs and the form of safety cases likely to be submitted to the Inspectorate. As far as safety cases are concerned, however, licensees may wish to put forward a submission which differs from this expectation and, as in the past, the NII will be prepared to consider such an approach. There are also other possible designs: novel plant concepts and novel plant features are currently being developed by the nuclear industry. Again the Inspectorate will be flexible in its response. In the past there have been plant items whose safety was difficult to justify in such a way as to readily satisfy the SAPs, the pressure vessel being the most obvious example. That possibility was catered for in the existing SAPs by having a principle which allowed for such plant items to be justified on a special case basis and this route has been used on a number of occasions. An amended version of the 'special case' principle is included in these revised SAPs and is available for similar use in the future on difficult plant items or on quite novel design features. If, however, situations arise which call for a different assessment approach, the principles will be re-examined and revised as appropriate. In summary, therefore, the revised SAPs are intended to cater for non-standard as well as the standard approach. In no case, however, should this flexibility be seen as a means of bypassing the rigours of the assessment process; special cases receive particularly close scrutiny.

12 For a proposed new plant, it is generally the case that not all safety questions can be answered at the pre-licensing stage. In such a situation, construction can only proceed if it is judged that there is little risk of significant additional costs being incurred for safety reasons at a later stage. This judgement is important because a great deal of work to answer outstanding questions may remain to be done after a licence has been granted. Conversely, a process in which all questions were answered before a licence was issued would require considerably more detailed work being done at the start with a consequential lengthening of the pre-licensing process.

13 As with earlier versions of the SAPs, the principles here are, with one or two detailed exceptions, aimed at the individual plant rather than at the site, which might contain two, three or four plants. In practical terms, the risk posed by a plant which satisfies these principles should be sufficiently small that the few times higher risk from such a multi-plant site would still be acceptable. There are already in existence one or two sites which contain a larger number of plants, but many of those plants afford significantly less risk than, for example, a large power station. Furthermore, there is a general trend towards reducing those risks and, as new plants replace old, the risk is likely to be further reduced. For these reasons it is judged acceptable for the revised SAPs to be drafted with respect to individual plants.

14 Not all of the principles in this document apply to every plant; clearly, reactor specific principles do not apply to chemical plants. Less obviously, not all of the reactor principles apply to all reactors: research reactors are different from power reactors and need to be treated differently, and a modification to a plant (reactor or chemical) obviously does not require the full panoply of the principles to be applied. In short, the principles are a reference set from which the assessor must choose those to be used for the job in hand.

15 As a final point on the question of application, the principles are intended for use as a basis for the Inspectorate's own safety assessment work, but clearly it will be helpful for licensees to have knowledge of the safety principles against which their plants will be judged. Additionally, of course, they can readily appreciate where the principles will cause problems for them. We recognise the industry's interest and expertise and have sought, without commitment, their views on the revised principles.

Risk analysis and engineering principles

16 Risk analysis is an important part of a licensee's safety case as it is of the design process. The plant has to be safe in normal operation and the design has to be robust enough to ensure any departures from normal operation do not lead to accidents, or it should include provisions to intercept accidents as they develop or to mitigate their consequences. To this end a list of design basis faults is developed to explore the need for safety provisions and to set limits on the plant's operating conditions. These design basis faults are analysed in parallel with the engineering design as it progresses.

17 Probabilistic safety analysis (PSA) is the final step in the accident analysis process which produces numerical estimates of the risk from the plant. PSA provides a comprehensive logical analysis of the potential for things to go wrong on the plant and of the roles played by the safety provisions. To carry out such analysis the design of the plant and the engineering intentions need to be known in some detail. Failure rates of plant items are an important input to the analysis, but in some cases such data may not be available. Physical and chemical processes may need to be predicted for conditions beyond those specified for the design or even achievable in tests. Therefore, a great deal of engineering knowledge and expert judgement has to be used in deriving probabilistic figures for comparison with the PSA standards.

18 Such judgements are possible because of the considerable effort which the NII devotes to engineering assessment and for which a comprehensive set of engineering principles is provided in this document. The engineering principles, however, do far more than provide a means of checking the reliability figures used in the PSA. They represent the NII's view of good nuclear engineering practice. They point to the provisions that in our view would achieve a safe plant. PSA by comparison provides a numerical measure of the safety of the design or a means of indicating deficiencies in it. The principles as a whole may be seen therefore as a yardstick against which the plant is judged: the PSA principles are the numbers marked on the yardstick; the engineering principles are the solid basis of the stick itself.

19 Where items of plant can be represented in the PSA by failure rate data this link between the engineering principles and the basic safety standards is clear. For those items whose contributions to the risk cannot be quantified, the link is less obvious and the engineering judgements are more difficult. Reference has been made earlier to an assessment process known as the 'special case' procedure which may be applied to some of those items. Particular attention needs to be addressed to these cases in order to be satisfied that they do not make an excessive contribution to the overall risk from the plant.

Structure of the principles

20 The principles presented here relate only to nuclear safety. Other conventional hazards are excluded except where they have a direct effect on nuclear safety. In paragraphs 22-27 there are certain internationally recognised fundamental safety principles. The following section deals with risks from normal operation and accident conditions and the standards against which those risks are assessed. Although the risk of accidents may be small, the choice of site can have a bearing on the consequences; paragraphs 93-102 therefore, give the principles applied in the assessment of a site. The following section comprises the major part of this document: those principles that cover the design of nuclear plants. The principles in the final section are intended to round off the assessment of a future plant by ensuring that lessons learned, commitments made in and requirements derived from the safety case, are properly fed into the construction, commissioning, operation and eventual decommissioning of the plants.

21 A glossary is presented at the end of the document to assist understanding of the principles. Throughout the document individual paragraphs are numbered, but for clarity of presentation those paragraphs which present principles are additionally numbered P1, P2 etc and printed in bold type.

FUNDAMENTAL PRINCIPLES

Introduction

22 In the earlier publications of the SAPs, five fundamental principles were presented at the beginning of the documents. Those principles derived from recommendations of the International Commission on Radiological Protection which were subsequently implemented by the Ionising Radiations Regulations 1985[4]. They embody the requirements for statutory radiation dose limits to be satisfied and for the ALARP principle to be applied to radiological exposures resulting from normal operation and to the risks from accidents. The fundamental principles are still relevant today and, indeed, the principles in the subsequent sections are aimed at ensuring that, when a proposed plant comes into operation, these principles will be satisfied.

Principles

23 (P1) No person shall receive doses of ionising radiation in excess of statutory dose limits as a result of normal operation.

24 (P2) The exposure of any person to radiation shall be kept as low as is reasonably practicable.

25 (P3) The collective effective dose to operators and to the general public as a result of operation of the nuclear installation shall be kept as low as is reasonably practicable.

26 (P4) All reasonably practicable steps shall be taken to prevent accidents.

27 (P5) All reasonably practicable steps shall be taken to minimise the radiological consequences of any accident.

SAFETY ANALYSIS

Introduction

28 Reference was made earlier to HSE's tolerability of risk (TOR) paper. The approach described in that paper has been carried through into these principles. The concept of a limit of tolerability has been translated into basic safety limits (BSLs) for the risks from normal operation and from accident conditions. A proposed plant must satisfy these limits in order to be considered for licensing. Having satisfied the BSLs, the ALARP principle comes into play to drive the risks from the plant even lower.

29 This process necessitates the making of decisions by designers and operators on a case-by-case basis, and no generally applicable numerical interpretation is appropriate. However, there comes a point at which further consideration of the case would itself be more costly in NII resources than the benefit from applying that effort to other tasks. Each BSL is complemented, therefore, by a Basic Safety Objective (BSO). The BSOs define the point beyond which the assessors need not seek further safety improvements from the licensee in his quest for ALARP; instead, they can confine their studies to the validity of the estimates put to them by the licensee. The licensee on the other hand is not given the option of stopping at that point. ALARP considerations may be such that he is justified in stopping before he reaches the BSO level; but if it is reasonably practicable for him to provide a standard of safety better than that of the BSO, he is obliged to do so.

The BSLs and the BSOs are related to individual and societal risks, and cover:

(a) radiation doses likely to be received by workers or members of the public in the course of normal operation; and

(b) the chances of accidents leading to radiation doses to workers and the public, releases of radioactive materials, or damage to plants which might lead to such releases.

30 The BSLs and BSOs therefore provide measures against which the NII assessors can make judgements on the safety of proposals put to them. There is considerable advantage in having such numerical standards, but the correspondng numbers which describe the plant depend on many judgements and are subject to uncertainties. Predicted radiological exposures during normal operation (which need to be compared with the BSLs and BSOs) are supported by experience from existing plants and can therefore be reasonably accurate. However, the risks from accidents are more difficult to estimate and for these predictions the uncertainties are greater.

Normal operation

31 The first three of the fundamental principles of paragraphs 22 to 27 provide the foundations upon which the principles of this section are based. Radiation doses may be received by people on the site and also by people outside it as a result of normal operations on the site. As well as doses from direct radiation, workers may receive radiation doses from inhalation and ingestion of radioactive material. Though they are clearly less exposed than the workers, people outside the site may

also receive doses by those routes and through the food chain as a result of discharges and disposals of radioactive waste liquids and solids.

32 Engineering and administrative provisions are used to control the doses. But all safety provisions have associated costs, and a line will be drawn at some point where the licensee judges it is not reasonably practicable to reduce the predicted worker and public doses by further provisions on his plant. The NII assessor's task is to compare those predictions with the levels in the BSOs. If the BSOs are satisfied, the assessor needs only to assess the validity of the predictions. If the BSOs are not satisfied he must also consider whether the right balance has been struck by the licensee between the costs and the benefits, in other words, whether the risks from normal operation have been made as low as reasonably practicable.

33 The principles presented below are concerned with the validity of predicted doses. They are followed by the BSLs and BSOs associated with risks to workers and the general public from normal operations. The limits on doses are derived from Ionising Radiations Regulations, 1985[4], and from the proposals in the TOR paper[3]. However, in view of the latest ICRP recommendations[5], the principles anticipate changes likely to be made to the Regulations. Explanatory notes on some of the principles are given in Appendix 1.

Principles

34 (P6) An analysis of the overall plant design and system of operation should be carried out to predict the radiation doses likely to be received by workers and the public and presented to demonstrate that the plant will meet Principles P11 to P14.

35 (P7) All dose predictions should make appropriate allowance for uncertainties associated with calculations of internal and external exposure and make use of relevant operational data. Where dose predictions depend on dose rates arising from build-up of contamination and from material in process, the maximum values expected to occur during the life of the plant should be used.

36 (P8) Predictions made of the doses likely to be received from normal operation of the plant by people working with ionising radiations should be based on the specific operations involved in the running and servicing of the plant, and evaluations of the duration, frequency and numbers of people involved in each component task, and should show both the highest individual annual dose and the annual group average dose.

37 (P9) The doses which could be received by those people on the site not working with ionising radiations may be simple bounding estimates.

38 (P10) Predictions of the doses likely to be received from normal operation of the plant by people outside the site should be based on calculated doses to the relevant critical groups as a result of direct radiation and from discharges of activity to air and other media.

39 (P11) No person on the site should receive in any year from all sources of radiation on the site a radiation dose greater than the values in the following table:

	BSL	BSO
Persons working with ionising radiations	20 mSv	2 mSv
Other workers on site	5 mSv	0.5 mSv
Members of the public	(see P14)	

40 (P12) No person working with ionising radiations should receive doses to individual organs greater than the relevant statutory dose limit[4].

41 (P13) The average radiation dose received in any year from normal operations by the group of persons working with ionising radiations should not be greater than the values in the following table:

	BSL	BSO
The group of persons working with ionising radiations	10 mSv	1 mSv

42 (P14) No member of the public should receive in any year from all sources of radiation on the site a dose greater than the following:

BSL	BSO
1 mSv	0.02 mSv

Note. Off-site doses resulting from discharges and disposals from nuclear sites are controlled by MAFF and HMIP (or in Scotland by HMIPI) by means of authorisations granted under the Radioactive Substances Act 1960. The criteria applied by these Authorising Departments are set out in the White Paper "Radioactive Waste" (Cmnd 9852).

Accident conditions

43 Fundamental Principles 4 and 5 underlie the assessment of safety in accident conditions. The principles in this section develop them into more specific standards against which the safety of the plant will be judged.

44 It is fundamental to achieving a safe plant that the engineering design should be sound. The likelihood of faults occurring should be minimised by conservative design, by the mode of operation, and by adequate maintenance, inspection and testing. Despite this, faults may occur and a plant must be capable of tolerating a range of faults without unacceptable consequences, by inherent safety in the design concept, defence-in-depth and the provision of effective safety systems.

45 Nuclear plants are, therefore, designed to cope with a wide range of potential accidents (design basis accidents - DBAs), but it may not be reasonably practicable to make design provision against the more unlikely accidents. The analysis of accident conditions follows two complementary approaches: deterministic and probabilistic. The deterministic approach is used in the analysis of design basis accidents which is required, in line with international practice, as a robust demonstration of the fault tolerance of the plant, of the effectiveness of its safety systems and with the aim of determining the limits to safe plant operation. For the purposes of design basis accidents, uncertainties in the transient and radiological analyses are covered by the use of appropriate conservatism in the treatment.

46 A deterministic approach is also followed for those accidents which are beyond the design basis and hence are liable to have serious consequences. But the analysis of these accidents differs from that of DBAs in that it should be performed preferably on a best-estimate basis, since it is required primarily to give realistic guidance on the actions to be taken in the unlikely event of such an accident occurring, and also to provide an input to the PSA.

47 Since the design basis accident analysis and the severe accident analysis give no quantitative indication of the risk posed by the plant, those analyses are complemented by a third category, probabilistic safety analysis (PSA), which addresses the full range of possible accidents. The PSA is required in order to search out any weaknesses in the plant where improvements might be called for, to provide estimates of the overall risks from the plant and to check on the provisions for defence-in-depth. For these purposes the PSA should preferably be performed on a best-estimate basis but, where this is not practicable, any bias should be in the pessimistic direction.

48 For the PSA, the accident frequency principles for the most part do not address directly either individual risk or the risk to society as a whole, but are chosen to provide surrogates for these risks - surrogates which are related to the design and operation of the plant in question. Thus a full risk analysis of all off-site effects is not required, although the licensee may see it as worthwhile to provide such an analysis, particularly for major new installations.

49 The layout of the principles in this section is that, first, a set of general principles is given, applicable to the fault analysis as a whole. These are used in the development of the principles that follow which cover in turn the three categories of analysis: design basis accident analysis, severe accident analysis and PSA. Finally there is a set of principles which, like the first, are of general applicability but which are related to assuring and maintaining the validity of the fault analysis.

50 The principles call for a considerable amount of analysis. In particular, the PSA principles require some reworking of faults that have previously been covered in the DBA and severe accident analysis. In order to reduce the size of the task, the Inspectorate is prepared to consider the use of the earlier analysis in the PSA, where this can be done without undue distortion of the risk estimates. Also, it is recognised by the Inspectorate that different plants carry different risks and that this may be reflected in the effort expended on the analysis: where the risk is high, the scope and quality of the analysis should be of an appropriately high standard; where the risks are lower, a somewhat lower standard may be accepted.

51 Some notes relevant to the principles in this section are presented in Appendix 2.

Fault analysis - General

52 (P15) An analysis of possible accidents on the plant should cover:

(a) *all significant sources of* radioactivity associated with the plant, and

(b) all planned operating modes of the plant.

53 (P16) The analysis should start with a list of initiating faults, including internal and external hazards and faults due to personnel error, which can be identified as having the potential to lead to any person receiving a significant dose of radiation. The safety case should demonstrate a systematic process for establishing the list of faults, which should aim for completeness. The fault sequences arising from these initiating faults should be

identified as described in P22 and P33.

54 (P17) Transient analysis or other analyses should be carried out as appropriate to determine the effect on the plant of these fault sequences.

55 (P18) For fault sequences which lead to a release of radioactive material or to a dose of direct radiation, radiological analysis should be performed which determines the maximum effective dose to a worker on the site and to a person outside the site directly downwind of the release. (The detail of this analysis differs according to its application, see P24 and P36.)

56 (P19) For the purpose of analysis the fault sequences may be grouped and a 'bounding case' for each group specified. Bounding cases should be selected having regard to the relevant physical and chemical processes involved and the demands made on the safety systems, and should have consequences at least as severe as every member of the groups of fault sequences which they are claimed to bound.

Design basis accidents

57 (P20) The analysis of design basis accidents should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety systems.

58 (P21) The safety case should present a list of all initiating faults which are included within the design basis of the plant. All initiating faults identified under P16 should be considered for inclusion in this list, but the following need not be included:

(a) faults internal to the plant which have an expected frequency lower than about 10^{-5} per year; and

(b) failures of structures, systems or components for which acceptable special case arguments have been made in accordance with P70.

(c) hazards excluded in accordance with P119.

59 (P22) The design basis fault sequences should then be identified, starting with each design basis initiating fault and including as appropriate: failures consequential upon the initiating fault, failures expected to occur in combination with it due to having a common cause, and single failures in the safety systems in accordance with P78. The worst normally permitted configuration of equipment outages for maintenance, test or repair, should be assumed, and correct performance of safety-related and non-safety equipment should not be assumed where it would alleviate the consequences. Sequences with very low expected frequencies need not be included.

60 (P23) The transient and other plant analyses (see P17) of design basis fault sequences should be performed on a conservative basis, sufficient to provide a high degree of confidence that the requirements of P25 will be met.

61 (P24) For each design basis fault sequence or bounding case (see P19) leading to a release of radioactive material, the radiological analysis to determine the maximum effective dose to a person outside the site should be performed on a conservative basis. In addition to the general requirements of P18, it should assume:

(a) the person remains at the point of greatest dose for the duration of the release, although for extended releases more realistic occupancy may be assumed after a suitable interval;

(bi) the weather conditions have characteristics which produce the highest dose to that person; and

(c) no off-site emergency countermeasures are effected, other than certain food bans whose implementation is shown to be highly likely.

62 (P25) It should be shown that, following any design basis fault sequence:

(a) none of the physical barriers to the escape of radioactivity is breached or, if any are, then at least one barrier remains intact;

(b) there is no release of radioactivity except in the most severe cases and, even then, no person outside the site will receive an effective dose of 100 mSv or more; and

(c) no person on the site will receive an excessive dose from the release of radioactive material or by direct radiation including that from criticality incidents.

63 (P26) The design basis analysis should establish the minimum safety system requirements for each initiating fault within the design basis and present the results in a schedule of safety systems, and should also identify the operator action requirements.

64 (P27) The design basis fault analysis should also provide information relevant to:

(a) the trip settings and performance requirements for the safety systems and safety related equipment;

(b) the determination of the plant operational limits (see P325) and the formulation of the operating rules;

(c) the preparation of the plant operating instructions for fault conditions.

Severe accidents

65 (P28) Fault sequences beyond the design basis which have the potential to lead to a severe accident should be considered, and analysed (by means of bounding cases if appropriate - see P19). The analysis should identify the failures which could occur in the physical barriers to the release of radioactive material or in the shielding against direct radiation, and should determine the magnitude and characteristics of the radiological consequences.

66 (P29) The analysis of severe accidents should be sufficiently realistic to form a suitable basis for the accident management strategies in P331 et seq. Where the uncertainties are such that a realistic analysis cannot be performed with confidence, reasonably conservative assumptions should be made to avoid optimistic conclusions being drawn.

67 (P30) The severe accident analysis should also provide information relevant to the preparation of the site emergency plan for the protection of people outside the site in the event of a large release of radioactivity.

68 (P31) Where severe accident uncertainties are judged to have a significant effect on the assessed risk, research aimed at confirming the modelling assumptions should be performed.

Probabilistic safety analysis (PSA)

69 (P32) A probabilistic safety analysis of the overall design and system of operation should be performed to enable an assessment of the risk arising from the plant to be made, and a judgement as to its acceptability against the accident frequency principles, P42 to P46. The PSA should also confirm that a balanced design of the plant has been achieved, such that no particular class of accident or feature of the plant makes a disproportionate contribution to the overall risk.

70 (P33) The PSA should take as its starting point the list of initiating faults from P16 and should go on to identify the complete range of fault sequences which could occur, including severe accidents, taking account of the possibilities of component failures, component unavailabilities during maintenance or testing, common cause failures (see P81), personnel errors and failures which could occur as a consequence of preceding events.

71 (P34) The frequency of occurrence and consequences of each of the fault sequences identified should be estimated. Where a bounding case is used to represent a group of sequences, it should be given a frequency equal to the summed frequency of the group.

72 (P35) Best-estimate methods and data should preferably be used for the transient and other plant analyses (see P17), for the radiological analysis, and for the frequencies and probabilities used in the PSA. Where this is not practicable, reasonably conservative assumptions should be made.

73 (P36) The maximum effective dose to a person outside the site should be calculated for a person situated at the nearest habitation or at a distance of 1 km from the plant, whichever is nearer, or at the point of greatest dose if that is further away.

74 (P37) Where statistical data are used, they should be shown to be appropriate to the design and operating conditions of the plant and should relate to a relevant and sufficiently large population. The source of the data, the sample size and the uncertainty in the data should be specified. If changes to the source data are made to take account of differences between the available data and the plant conditions, these should be justified.

75 (P38) Where no relevant statistical data are available, judgements should be made and their basis stated. Particular attention should be paid to determining the sensitivity of the results of the PSA to such judgements.

76 (P39) Probability data for personnel errors should take account of the specific task demands, psychological influences (eg stress, degree of supervision and working practices), the physical environment, and potential dependencies between separate activities (either by the same or by different operators). Any equipment or procedural

requirements to promote reliable human performance should be identified.

77 (P40) For some fault sequences, it will not be possible to calculate the frequency of occurrence because the data are inadequate or no appropriate models are available. For example, for certain structural components such as pressure vessels, where failure could lead to severe consequences, the failure frequency required to meet the accident frequency principles may be well below the values which can be justified by standard statistical estimation techniques. In all such cases, a considered judgement should be made of the contribution to the predicted frequencies from such faults.

78 (P41) The PSA should also provide information relevant to the requirements on the reliability, maintenance and testing of safety and safety-related systems.

Doses to the public

79 (P42) The total predicted frequencies of accidents on the plant, which would give doses to a person outside the site, should be less than the values given in the following table:

Maximum effective dose, mSv	*Total predicted frequency, per year*	
	BSL	*BSO*
0.1-1	1	10^{-2}
1-10	10^{-1}	10^{-3}
10-100	10^{-2}	10^{-4}
100-1000	10^{-3}	10^{-5}
> 1000	10^{-4}	10^{-6}

Note. A subsidiary aim should be for no single class of accident to contribute more than about one tenth of the total frequency in any dose band, to avoid placing excessive reliance on particular features of the plant or on particular assumptions in the analysis.

For further explanatory notes on this principle see Appendix 2, paragraph 4.

Risk to workers

80 (P43) The total predicted individual risk of death (early or delayed) to any worker on the plant attributable to doses of radiation from accidents should be less than:

BSL	BSO
10^{-4} per year	10^{-6} per year

Note 1. It is recognised that the calculation of individual risk to workers may be difficult and hence only a broad estimate will normally be required, sufficient to show that the BSL is very unlikely to be exceeded and that ALARP has been appropriately applied.

Note 2. This principle is not intended to apply to personnel returning to perform recovery actions after an accident.

Large release

81 (P44) The total predicted frequency of accidents on the plant with the potential to give a release to the environment of more than:

10 000 TBq of Iodine 131
or 200 TBq of Caesium 137
or quantities of any other isotope or mixture of isotopes which would lead to similar consequences to either of these

should be less than:

BSL	BSO
10^{-5} per year	10^{-7} per year

Plant damage

82 (P45) The total predicted frequency with which the plant suffers damage and a significant quantity of radioactive material is permitted to escape from its designed point of residence or confinement, in circumstances which pose a threat to the integrity of the next physical barrier to its release, should be less than:

BSL	BSO
10^{-4} per year	10^{-5} per year

Note. Such plant damage is interpreted as a degraded core in the case of a reactor. For other plant, it would include a major breach of vessel pipework etc, together with the potential for events such as fire, explosion, or aggressive chemical attack which might lead to degradation of the containing cell or its ventilation/filtration system even though there may be a safety system provided to prevent such degradation.

Criticality incidents

83 (P46) The total predicted frequency of an accidental criticality excursion on a plant other than a nuclear reactor should be less than:

BSL	BSO
10^{-3} per year	10^{-4} per year

Note. This principle also applies to plants handling or storing fissile material outside the reactor core on a nuclear power station.

Assurance of validity

84 (P47) It should be shown that the calculational methods used for the analysis adequately represent the physical and chemical processes taking place. Where possible, the methods should be validated by a comparison with actual experience, appropriate experiments or tests. If this is not possible, a comparison with other, different calculational methods would be acceptable.

85 (P48) The radiological analysis should include any direct radiation and any inhalation, absorption and ingestion of radioactive material and should take account of the physical and chemical form of the radioactive material released.

86 (P49) The analysis should also establish that the adverse conditions which may arise as a consequence of the fault sequence would not jeopardise the claimed performance of safety system actions.

87 (P50) The personnel activities to be considered in the analysis should include monitoring of plant, diagnosing plant state, making decisions and implementing actions. Task analysis should be carried out to demonstrate that these activities are feasible and can be performed in the time available.

88 (P51) The data used in the analysis should be shown to be valid by reference to established physical data, experiment or other means and any extrapolation of data should be shown to be valid.

89 (P52) Studies should be carried out by the licensee to determine the sensitivity of the fault analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation. Where the predictions of the analysis are sensitive to the modelling assumptions, they should be supported as far as practicable by additional analysis using independent methods and computer codes.

90 (P53) In order for there to be adequate confidence in the results of the fault analysis, an independent check should be made by the licensee, where possible using different methods or analytical models.

91 (P54) The fault analysis carried out at the design stage should be reviewed and where necessary revised to take account of:

(a) changes to the plant or the system of operation at the design or construction stage and during its operating life;

(b) any new relevant technical and scientific knowledge concerning plant behaviour and fault potential; and

(c) any material property changes and deterioration due to ageing not previously taken into account.

92 (P55) Data should be collected by the licensee throughout the operating life of the plant to check or update the fault analysis. This should include plant performance and failure data such as statistical data on initiating fault frequencies, component failure rates and plant unavailability during periods of maintenance or test.

SITING

Introduction

93 If a company wishes to build a plant, it has to satisfy the NII first in relation to the site - that it conforms with the Government's siting policy and that the site characteristics are acceptable - and then in relation to the plant to be built on it. An important element of Government policy is that the first plant of a new type should be built on a remote site. This is deemed to be a prudent approach until sufficient experience is gained to allow more relaxed siting. With regard to site characteristics, to a large extent the site can be considered independently of the plant design. The objective as far as the design is concerned is that accidents should be prevented and their consequences contained. For the site, on the other hand, consideration has to be given to measures which would mitigate the effects of an accident in the unlikely event that a radioactive release occurred.

94 All nuclear plants are required, therefore, to have an emergency plan. For major plants such as power reactors, large reprocessing facilities and fuel stores, the plan should address the design basis accident which

gives the most significant off-site release or, if the accident results in doses below the lower emergency reference level[10], should cover a minimum planning zone of 1 km. Off-site plans for minor plants should be made commensurate with the level of potential hazard they present. The principal aspects on which the NII requires to be satisfied are the demographic characteristics which have a bearing on accident mitigation, in particular the size, nature and distribution of the population around the site. The fewer people there are living, working or at leisure in the vicinity of the site, the smaller will be the number likely to be affected by an accidental release of radioactive material and for whom it may be necessary to initiate measures, such as evacuation from the area, if an accident occurs. Institutions with relatively large numbers of immobile people such as hospitals or old people's homes could present difficulties in the event of an emergency.

95 A second aspect for consideration comprises those features of the topography of the area around the site which can affect the dispersion of radioactive materials discharged from a plant in normal operation or released in the event of an accident. Other aspects of the topography which might affect the movement of people or of goods, the first being relevant to evacuation and the second to the normal movement of radioactive materials to and from the site, need also to be considered.

96 There is a third category of site related characteristics on which information will be required and these are the natural and man-made hazards in the area. Earthquakes, flooding, drought, high winds and extremes of ambient temperature are examples of natural hazards which need to be considered. Man-made hazards include the possibility of an aircraft crash on the site and the storage, processing or transport of hazardous materials in the vicinity. Interruption of essential services to the plant, such as power and water, could also jeopardise its safe working.

97 In general, these hazards will be dealt with as appropriate in the design of the plant. These aspects of the site-related risk are therefore covered in the hazards section of the engineering principles. The following principles are those specific to a site which need to be satisfied in order to obtain approval of the proposed site. Information required under the hazards principles must also be supplied, but generally that would lead to design provisions in the plant rather than being a determining factor in approval of the site.

Principles

98 (P56) Allowing for some natural growth of the population in the area over the life of the plant, the size and distribution of the population in the vicinity of power reactors and other major plants should be such that:

(a) it would be possible to evacuate all persons from an affected area of up to 1 km around the site in about two hours from the time a decision to evacuate is taken, and to take other emergency measures on an appropriate timescale;

(b) there are no institutions with large numbers of relatively immobile people within 1 km of the plant or, if there are, the emergency planning authority is satisfied that evacuation of such people could be carried out within two hours;

(c) emergency plans (evacuation and other measures) should be capable of extension to deal with larger but more unlikely accidents should the need arise.

99 (P57) Once a site has been approved for a nuclear plant, controls should be exercised, as far as is reasonably practicable, to prevent the population in the vicinity of the site increasing in such a way that the requirements of Principle P56 might be exceeded.

100 (P58) Aspects of the topography and geology of the area around the proposed site which would affect the dispersion of radioactive materials released from the plant in normal operation and in the event of accidents should be identified and their effects assessed.

101 (P59) The assessment should determine the dispersion of such radioactive releases via the atmosphere, surface water and ground water and their transfer to the population by various mechanisms and exposure pathways using established and well-researched models.

102 (P60) Aspects of the topography of the area around the site which may affect the movement of people and goods should be identified and their effect on the safety of the plant examined. This examination should determine whether the topography and road and rail systems are such as to create difficulties if it became necessary to evacuate people from the area around the plant. The suitability of the transport facilities for the movement of radioactive materials to and from the site should also be examined.

ENGINEERING PRINCIPLES

Introduction

103 These principles comprise the major part of the SAPs and are complemented by the safety analysis principles in paragraphs 28-92: the engineering standards need to be high in order to achieve the necessary high level of safety which can then be checked against the safety analysis principles. Not all of the engineering principles make an equal contribution to the safety of a plant; indeed, assessing the individual contributions would be difficult if not impossible. However, some are of greater importance than others. They may have a major influence on the cost of the plant; or they may not have such an effect on cost but are seen as a fundamental engineering requirement in a safe plant. They may be in neither of these categories but are nevertheless of prime importance - the need for the plant to be based on a sound concept, for example. All of these 'key' principles have been brought together as the first part of this section. (In cases where the structure of later parts of the section would be distorted by their omission, the key principles are repeated again and marked with asterisks in those sections).

104 While not in the same class as the key principles, there are a number of other principles which have a wide (general) application in the assessment of a plant. These are presented in the second part of the section and cover: safety categorisation; codes and standards; reliability; human factors; equipment qualification; plant ageing; plant layout; design data and models; maintenance, inspection and testing; and radiological protection.

105 There are some topics whose importance is such that they are given their own sections, external and internal hazards, structural integrity, and safety systems and safety related instrumentation.

106 Finally, the section presents plant specific principles under a number of sub-headings; reactor core, heat transport systems etc.

107 The ALARP principle has been discussed in the introduction to the principles and again in Fundamental Principles and Safety Analysis. ALARP applies equally in assessments made against the principles in this section. These principles are intended to assist our assessors, but in using them the assessors need to exercise their judgement in deciding whether the licensee has gone far enough in relation to each of the relevant principles.

Key principles

108 (P61) Potential hazards from operation of the proposed plant should be identified. The design concept should be such that these *hazards are avoided* and safe conditions are maintained through inherent and, where appropriate, passive features of the design without reliance on control or safety systems.

109 (P62) The design concept should be such that the *sensitivity* of the plant to potential faults *is minimised.* The expected plant response to any initial fault event should be as near to the top of the following list as can reasonably be achieved:

(a) a failure or maloperation should produce no significant operational response, or should produce a change in the plant state towards a safer condition;

(b) following a failure or maloperation, the plant should be rendered safe by the action of passive features or engineered safeguards which are continuously available in the state required to control the fault;

(b) following a failure or maloperation the plant should be rendered safe by the action of active engineered safeguards which need to be brought into service in response to the fault.

110 (P63) For reactor plants, the following *characteristics* should be incorporated as far as reaonably practicable:

(a) temperature coefficients of reactivity, power coefficients and coolant voidage co-efficients should be such as to ensure stable reactor behaviour at all times;

(b) there should be adequate margins between the normal operational values of safety-related parameters and the values at which the physical barriers to release are challenged;

(c) the thermal characteristics should be such that operational perturbations in power or coolant flow do not cause large or rapid temperature changes, or unacceptable changes in the physical state of the coolant, the fuel and the fuel canning material.

111 (P64) For chemical plants:

(a) strongly exothermic, or high pressure reactions should be avoided, and any source of energy released into the system should be adequately controlled as should the state of the nuclear matter in the plants;

(b) the choice of process materials, their inventories, the process conditions and containment materials should be such as to minimise the consequences of potential faults, and the use or generation of hazardous or toxic materials should be avoided; and

(b) the process flowsheet should ensure that process deviation will not move the plant towards an unsafe state.

112 (P65) A nuclear plant should be so designed that *defence in depth* against potentially significant faults or failures is achieved by:

(a) multiple physical barriers to the release of radioactive materials to the environment; and

(b) the provision of several levels of protection which will prevent the breach of any barriers or mitigate the consequences of a breach. These levels of protection include not only engineered control and safety systems but also aspects such as conservative design, quality assurance, accident management strategies and off-site emergency response.

113 (P66) *Novel designs* may be accepted provided they are supported by appropriate research and development, and the novel features are adequately tested before coming into service and monitored during service.

114 (P67) Due account should be taken of the need for structures, systems and components important to safety to be designed to be *inherently safe* or to *fail in a safe manner.* Potential failure modes should be identified, using a formal analysis where appropriate.

115 (P68) The design should make the best use of *diversity, redundancy* and *segregation* in the structures, systems and components which are important to safety.

116 (P69) All structures, systems and components should be allocated a *safety categorisation* which takes account of the consequences of their potential failure and of the failure frequency requirements placed on them in the safety analysis. This categorisation should be used to determine the standards to which those items should be constructed. See paragraph 131.

117 (P70) Where a structure, system or component forms a principal means of ensuring nuclear safety and it is not practicable to demonstrate that the accident frequency principles P42 to P46 are satisfied in the event of its failure, the plant may only be accepted after the application of a *special case procedure* agreed as an alternative demonstration. The procedure should include a comprehensive examination of all the relevant scientific and technical issues, taking account as appropriate of precedents set under comparable circumstances in the past.

118 (P71) Where the special case procedure is applied or where any safety system is required to achieve a high reliability, an *independent assessment* of the item should be carried out in addition to the checking provided as part of the design process. The object of the assessment should be to confirm the adequacy of design specification and that the manufacture, construction and commissioning satisfies that specification.

119 (P72) *External and internal hazards* which could affect the safety of the plant should be identified. They should be treated as potential initiating events of fault sequences and, where appropriate, taken in combination with other plant faults.

120 (P73) Whenever nuclear matter is present in the plant, *adequate safety systems* should be available to reduce the frequency or limit the consequences of fault sequences. No fault, internal or external hazard, should disable the safety system(s) provided to safeguard against that event. *Control systems and safety systems* should therefore be physically *separate* and should share no equipment or services.

121 (P74) The *layout* of safety system equipment and safety-related plant and services should be such as to minimise the effects of internal and external hazards and of any interactions between a failed structure, system or component and other safety-related structures, systems or components.

122 (P75) A *qualification procedure* should be in place to confirm that all safety systems and safety related equipment will perform their required safety functions throughout their operational lives, under the operational, environmental and accident conditions specified in the design. The procedure should, where reasonably practicable, include a demonstration that individual items can perform their required functions under the specified conditions.

123 (P76) Provision should be made for *monitoring and inspecting* safety systems, safety-related structures, and components in service or at intervals throughout plant life commensurate with

the reliability required of each item. In especially difficult circumstances where this cannot be done, either *additional design measures* should be incorporated to compensate for the deficiency, or it should be demonstrated that adequate long-term performance will be achieved without such measures.

124 (P77) Normally, a safety system should be automatically initiated. *No human action* should be necessary for approximately *30 minutes* following the start of the requirement for protective action. The design, however, should be such that plant personnel can initiate safety system functions and can perform necessary actions to deal with circumstances which might prejudice safety, but cannot negate correct safety system action at any time.

125 (P78) *No single random failure* assumed to occur anywhere within the safety systems provided to perform a safety function should prevent that function being performed during any normally permissible state of plant availability. Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure.

126 (P79) *Redundancy* should be incorporated within the designs of safety systems so as *to achieve required high levels of reliability* unless it can be demonstrated with high confidence that the reliability can be achieved by other means.

127 (P80) Diversity and segregation should be used as appropriate where the possibililty of *common cause failures* would otherwise threaten the achievement of the reliability required for a safety function.

128 (P81) Where high reliability is sought from a safety system through the use of redundant identical components, measurements or actions, a *common cause failure limitation* should be placed on the claimed reliability of the system. This limit should not be lower than one failure in 100 000 demands and may need to be higher depending on the complexity and novelty of the system.

Note. The figure of one failure in 100 000 demands represents a judgement by NII of the lowest value of the limit which could reasonably be supported by currently available data and methods of analysis. Nevertheless, it is conceivable that the continuing accumulation of good data and advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the licensee for a lower figure. Such a case would not then be ruled out of consideration.

General principles

129 These are the principles which have a wide, and in many cases general, application throughout the engineering assessment.

Categorisation, codes and standards

130 (P82) The design should be conservative and follow appropriate national or international codes and standards and the plant should satisfy the requirements of the best practicable standards of manufacture, construction, inspection, maintenance and operation, commensurate both with the safety categorisation and with any relevant reliability requirements of its component parts.

131 (P69)* All structures, systems and components should be allocated a safety categorisation which takes account of the consequences of their potential failure and of the failure frequency requirements placed on them in the safety analysis.

The safety categorisation should be determined on the following basis:

(a) Category 1 - any structure, system or component which forms a principal means of ensuring nuclear safety;

(b) Category 2 - any structure, system or component which makes a significant contribution to nuclear safety;

(c) Category 3 - any other structure, system or component.

132 (P83) All structures, systems and components should be designed, constructed and inspected to the highest standards commensurate with their safety categorisation as follows:

(a) Category 1 - Conservative design and construction standards should be adopted for this, the highest category together with a strict interpretation of these assessment principles in line with the ALARP requirement. For some items (such as those whose failure would lead directly to an event beyond the design basis) the special case procedure (P70) may need to be used;

(b) Category 2 - Appropriate national or international codes or standards should be

adopted, with particular consideration being given to demonstrating the ability of the item to perform the required safety function;

(c) Category 3 - Normal industrial standards can be applied.

133 (P84) Where there is no appropriate code or standard a full justification should be given for the design method adopted. The combining of different design codes and standards for an individual component should be avoided where practicable and should be justified when used.

134 (P85) Due allowance should be made in the design for degradation processes, including corrosion, erosion, creep, fatigue, and ageing, and for the effects of the chemical and physical environment. The design should allow for any uncertainties in determining the initial state of components and the rate of degradation.

Design data and models

135 (P86) Theoretical models should be employed as appropriate in support or confirmation of the design or as a means of describing safety-related conditions in the plant at any time. Such models should be based on a sound scientific understanding and any necessary assumptions or approximations should demonstrably bias results in a safe direction.

136 (P87) Analytical models should be validated as a whole or, where this is not practicable, on a module basis, against experiments which replicate as closely as possible the expected plant condition. Care should be exercised in the interpretation of such experiments to take account of uncertainties in replicating the range of anticipated plant conditions. Where appropriate, an independent check of an analysis should be made using different methods or analytical models.

137 (P88) 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 physical 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 it. Extrapolation from available data should not be used without good justification.

138 (P89) Provision should be made to keep under review new data, scientific knowledge and information from operating experience and incidents occurring on other plants to ensure that the safety case is not invalidated.

Equipment qualification

139 (P75)* A qualification procedure should be in place to confirm that all safety systems and safety related equipment will perform their required safety functions throughout their operational lives, under the operational, environmental and specified (usually design basis) accident conditions. The procedure should, where reasonably practicable, include a demonstration that individual items can perform their required functions under the specified conditions.

140 (P90) The equipment qualification procedure should ensure that adequate arrangements exist for the recording and retrieval of lifetime data from the manufacture, testing, inspection and maintenance of safety systems and safety related structures and components to demonstrate that any relevant assumptions made in the safety case remain valid, throughout the design life of the plant.

Human factors

141 (P91) For personnel with safety responsibilities, the safety functions required of them should be defined. The definitions should include the responsibilities of operations personnel responsible for monitoring and controlling plant and for responding to faults, and of personnel carrying out maintenance, testing and calibration activities.

142 (P92) Analysis should be carried out of the tasks that will be involved in performing these safety functions to determine the demands on personnel in terms of perception, decision making and action, with a view to evaluating the feasibility of the tasks and providing an input to the design of interfaces in accordance with human capabilities. Task analysis should also provide a basis for developing the design of procedures and of personnel training.

143 (P93) The design of all interfaces between operating personnel and the plant should follow good human factors and ergonomics practice, to ensure compatibility with human psychological and physical characteristics, and to enable the required human tasks to be performed reliably and efficiently. This requirement includes the design of central control rooms and local control stations on the plant, and the provisions for maintenance and testing; particular attention should be paid to display systems, panel layouts and workspace access for maintenance operations, and the physical environment.

144 (P94) Interactions with other aspects of human factors should be addressed. Training

arrangements for operations personnel and other staff, and the development of operating procedures, should be fully compatible with the design of tasks and of equipment. Operating instructions will need to be validated for reliable interpretation and implementation by the relevant personnel. The influence of proposed staffing levels should be taken into account. Implications for safety management systems should be considered, and any opportunities for promoting the plant safety culture identified.

Layout

145 (P74)* The layout of safety system equipment and safety-related plant and services should be such as to minimise the effects of internal and external hazards and of any interactions between a failed structure, system or component and other safety-related structures, systems or components.

146 (P95) The layout of buildings and roadways on site should be such that in the event of any internal or external hazard, fault or incident affecting the site:

(a) an alternative means of access will be available to plant and controls essential to safety which may require local manual intervention;

(b) alternative access for personnel rescue equipment will be available to all normally manned areas;

(c) safe means of escape will be provided from all buildings or plant areas which may be affected by the incident;

(d) where reasonably practicable, site personnel will be physically protected from direct or indirect effects of the incident.

147 (P96) Unauthorised access to or interference with safety systems and their reference data and with safety-related structures and components should be prevented.

Maintenance, inspection and testing

148 (P97) All safety-related structures, systems and components should, where practicable, be type-tested under conditions at least equal to the most severe expected in all modes of normal operational service before they are installed. For components of particular concern and where it is not possible to confirm the ability to operate under the most onerous design conditions, reference data from commissioning or rig testing should be established for comparison against in-service test results.

149 (P98) Commissioning and in-service inspection and test procedures should be adopted which ensure initial and continuing quality and reliability. Such inspection should be of sufficient extent and frequency to give adequate confidence that degradation will be detected.

150 (P99) The design and layout of the plant and all safety-related structures, systems and components should be such as to facilitate inspection, testing, maintenance, modification, repair and replacement in the interest of preserving the plant in a safe state at all times during the plant life.

151 (P76)* Provision should be made for monitoring and inspecting safety systems, safety-related structures, and components in service or at intervals throughout plant life commensurate with the reliability required of each item. In especially difficult circumstances where this cannot be done, either additional design measures should be incorporated to compensate for the deficiency, or it should be demonstrated that adequate long-term performance will be achieved without such measures.

152 (P100) Wherever reasonably practicable, provisions should be made for in-service functional testing of all safety systems and other safety-related equipment sufficient to prove the complete system and the safety-related function of each component. Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated. It should be possible to carry out these tests without loss of any safety function.

153 (P101) Provision should be made for periodic measurement of relevant properties of fully representative materials and parameters relevant to the design of the plant where such properties or parameters could change with time and affect safety.

Plant ageing

154 (P102) The safe working life of all components, structures and systems which are important to safety should be evaluated and defined at the design stage, with particular emphasis on those components which are judged to be difficult or impracticable to replace. Adequate margins should be built into the design to allow for the effects of time dependent degradation.

155 (P103) There should be an adequate margin between the intended operational life and the predicted safe working life of such components, structures and systems.

Radiological Protection

156 (P104) Adequate protection against radiation and contamination in normal operation, and against these and other consequences of fault conditions, should be provided in all parts of the plant to which access can reasonably be gained, preferably by the use of engineered controls and design features. Such protection should permit access to and occupancy of any control room required to achieve and maintain a safe plant state.

157 (P105) There should be appropriate personal provisions for the measurement of radiation doses to individuals and devices suitably located for the purposes of monitoring radiological conditions and the assessing of personnel exposures.

158 (P106) Provision should be made on the basis of levels of radiation, contamination and airborne activity for the classification of workplaces into suitable zones, each having appropriate controls on access, occupancy, and the need for protective equipment.

159 (P107) The design of the plant should be such that short term radiation exposure of people can be limited by appropriate controls over the occupancy of relevant plant areas and by ensuring that the plant can be operated without the need for access to areas of high dose rate.

160 (P108) Where doses are likely to be received which are a significant fraction of an annual limit, access should be controlled by physical means such as interlocks, locked doors or alarms 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 an equivalent standard of protection should be ensured by other arrangements.

161 (P109) There should be appropriate provisions for protecting persons entering and working in contaminated areas and for monitoring and controlling the spread of airborne activity, contamination and direct radiation within and beyond each zone. The provisions should include the ventilation of contaminated areas to limit the spread of contamination and appropriate arrangements for preventing the spread of contamination by people.

162 (P110) Provision should be made for the decontamination of zones to which access may be required and for decontamination of articles removed from contaminated locations. Local decontamination facilities should be provided unless it can be demonstrated that in the particular circumstances a centralised decontamination facility is more appropriate.

163 (P111) Manipulation of items exhibiting high surface radiation dose rates should be carried out using remote handling devices. Manipulation of highly contaminated items should wherever possible be carried out in enclosures which provide adequate protection against the spread of contamination.

164 (P112) Vessels, pipework, plant equipment and containment structures which could become contaminated with radioactive material should be designed to facilitate decontamination.

165 (P113) Instrumentation should be provided where appropriate to give prompt, reliable and accurate indication of radiation and of airborne activity levels in operating areas, and should be fitted with alarms to indicate significant changes in levels. All such equipment should be capable of providing reliable indications and alarms taking into account prevailing environmental conditions.

Reliability

166 (P114) The reliability claimed for any safety-related structure, system or component should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.

167 (P115) The measures proposed, including quality assurance, whereby the claimed reliability of systems and components will be achieved in practice should be stated. Evidence should be provided to demonstrate the adequacy of any such measures. All assumptions made in the course of the reliability analysis should be justified.

168 (P80)* Diversity and segregation should be used as appropriate where the possibility of *common cause failures* would otherwise threaten the achievement of the reliability required for a safety function. See also P81.

169 (P116) The assumed reliability of a component should reflect the environmental conditions specified throughout its lifetime. Where data are shown to be inadequate, appropriate measures should be taken to ensure that the onset of failure

can be detected, and that the consequences of failure are minimised.

170 (P117) Where reliable and rapid protective action is required, engineered safety features should be provided. For requirements which are less demanding or on a longer timescale, administrative control or personnel actions may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state.

171 (P118) Where multiple safety-related systems and/or other means (including physical processes and human actions) are claimed to reduce the frequency of a fault sequence, the reduction in frequency should have a clear margin of conservatism with appropriate allowance for uncertainties.

External and internal hazards

172 This set of principles amplifies the requirements of key principle P72, starting with the general principles applicable to all hazards and following with their development into principles to be applied to specific hazards. Internal hazards (eg fire) can arise as a consequence of faults internal to the plant and will be included, therefore, in the relevant fault sequences. They are, however, also subject to the following principles.

General

173 (P119) It should be shown for all hazards that the design basis analysis principles and the PSA principles are satisfied as appropriate, unless it can be demonstrated that the frequency of an event being exceeded is less than once in 10 million years, or if the source of the hazard is sufficiently distant that it cannot reasonably be expected to affect the plant.

174 (P120) For natural hazards, the uncertainty of data may prevent reasonable prediction of events for frequencies less than once in 10 000 years. In these cases, plants should meet the requirements of P25 for a design basis event that conservatively has a predicted frequency of being exceeded no more than once in 10 000 years. Plants which cannot give rise to doses as high as those specified in P25 may be designed against more frequent, ie less onerous, events.

175 (P121) It should be shown that there will not be a disproportionate increase in risk from an appropriate range of events which are more severe than the design basis event.

176 (P122) Hazards should be assumed to occur simultaneously with the most adverse normal plant operating condition and the analysis should also take into account:

(a) that hazards may occur simultaneously or in a combination which can reasonably be expected;

(b) that a hazard may occur simultaneously with a plant fault, or when plant is out for maintenance.

177 (P123) Support services and facilities such as access roads, water supplies, fire mains and site communications important to the safe operation of the nuclear plant should be designed and routed so that, in the event of a relevant hazard or other incident, sufficient capability to perform their emergency functions will remain.

178 (P124) Account should be taken of the extent to which the severity of the hazard experienced by the plant is affected by plant layout, and building size and shape.

179 (P125) In all cases either site specific or, if this is not appropriate, best available relevant data should be used to determine the magnitude of the hazard.

Aircraft impact

180 (P126) The predicted frequency of aircraft and helicopter crash on or near safety-related plant at the nuclear site should be determined. The risk associated with the impacts, including the possibility of aircraft fuel ignition, should be determined to establish whether principle P119 is satisfied.

181 (P127) The calculation of crash frequency should include the most recent crash statistics, flight paths and flight movements for all types of aircraft and take into account forecast changes in these factors if they affect the risk. Relevant bodies should be consulted by the licensee with the object of minimising the risk from aircraft approaching or overflying the plant.

Earthquakes

182 (P128) The seismology and geology of the area around the proposed site and the geology of the site should be evaluated. Information on historical and instrumentally recorded earthquakes which have occurred in the region should be established. The extent of the studies carried out by the licensee

should cover all those aspects which could affect the estimation of the seismic hazard at the site.

183 (P129) A design basis earthquake (DBE) should be determined in accordance with Principle P120. This DBE should be defined in terms which will enable buildings, structures and plant in the nuclear installation to be designed to withstand safely the ground motions involved.

184 (P130) An operating basis earthquake (OBE) should also be determined so that no safety-related plant, system or structure would be impaired by the repeated occurrence of ground motions at the OBE level. Where possible the plant should be shut down and brought to a safe state whenever the OBE is exceeded and not restarted until inspection has shown that it is safe to do so.

185 (P131) In determining the effect of a seismic event on any plant the simultaneous effect of that event on any other plant in the vicinity and on any system or service which may have a bearing on safety should also be taken into account.

Electro-magnetic interference

186 (P132) An assessment should be made to determine whether any source of electro-magnetic interference in the vicinity of the site could cause malfunction in or damage to, safety related equipment or instrumentation. If such interference is possible the design of the plant should be such that protective measures are provided.

Extreme weather conditions

187 (P133) A design basis event for each type of extreme weather condition should be determined in accordance with principle P120. These conditions should include abnormal wind loadings, precipitation, accumulated ice and snow deposits, lightning, extremes of high and low temperature and drought.

188 (P134) The design basis event should take account of combinations of extreme weather conditions reasonably expected to occur and of the effect of failure of non-safety related plant on safety-related plant during such conditions.

Fire, explosion, missiles, toxic gases etc

189 (P135) The on-site use and storage of hazardous materials should be kept to a practical minimum, and controlled and located so that any accident to or release of the materials will not jeopardise the establishing of safe conditions on the plant.

190 (P136) All sources in the plant or outside it which could give rise to fire, explosion, missiles, toxic gases etc should be identified, specified quantitatively and their potential as a source of harm to the nuclear plant estimated. Projects and planned future developments on and off the site should be considered where appropriate.

191 (P137) It should be shown that the nuclear plant is adequately protected from the effects of any incident in an installation, means of transport or pipeline either inside or outside the nuclear site.

Flooding

192 (P138) The area around the site should be evaluated to determine the potential for flooding due to precipitation, high tides, overflowing of rivers, failure of dams, tanks or water-carrying systems, seiches and tsunamis.

193 (P139) A design basis flood should be determined in accordance with principle P120. This should take into account as appropriate the combined effects of high tide, wind effects, wave actions, duration of the flood and flow conditions depending on the hazard under consideration.

194 (P140) The design of the plant should include adequate provisions for the collection and discharge of water reaching the site from any design basis external event or failed systems on site and as far as reasonably practicable to prevent it spreading and hence affecting safety-related plant.

Protection against fire

195 (P141) Fire detection and fire-fighting systems of adequate capacity and capability should be provided where appropriate. They should be designed and located so that any damage they may sustain or their spurious operation does not affect the safety of the plant.

196 (P142) To satisfy principle P141 a fire hazard analysis should be made of the plant to:

(a) identify safety systems and safety-related plant;

(b) analyse the potential for fire initiation and growth and the possible consequences on safety systems and safety-related plant;

(c) determine the need for segregation of plant and the location and required fire resistance of boundaries to limit the spread of fire;

(d) determine the capacity and capability of the fire

detection and fire-fighting systems to be provided.

197 (P143) Non-combustible or fire retardant and heat resistant materials should be used wherever practicable throughout the plant.

198 (P144) Not used.

Structural integrity

199 This section is concerned with the engineering assessment of the integrity of structural components such as pressure vessels, boilers, pressure parts, coolant circuits, metal structures, concrete structures, foundations, pumps, valves, etc, ie structural components using metal, concrete and other materials. Any specific differences are stated in the appropriate principles. Where a structural component also forms a containment, principles P222 to P238 should also be used.

200 The general lack of adequate reliability data for structural components leads to assessment being based primarily on established engineering practice. Even when there is some confidence in assessing reliability on the basis of existing data and a probabilistic safety case is possible, it is unlikely to be acceptable without substantial support from theoretical analyses and engineering judgement. As a result, although the radiological consequences of failure of structural components may be significant, it is often not possible to calculate the risk for inclusion in the PSA.

201 Reference has already been made in paragraph 117 to those special cases where the component forms a principal means of ensuring safety; the reactor pressure vessel is an example. For such components there are two particularly important aspects to be addressed: that the structure should be as defect free as possible, and that it should be demonstrated to be defect tolerant, in particular that the critical crack sizes should be large with respect to the inspection technique. In order to achieve these fundamental requirements, several related but independent arguments should be used, based on the following:

(a) the use of sound design concepts and proven design features;

(b) the analysis of the potential failure modes for all conditions arising from design basis faults;

(c) the use of proven materials;

(d) the application of high standards of manufacture, including in-process inspection, and construction, for the materials and processes used;

(e) high standards of quality assurance throughout all stages of design, procurement, manufacture, construction and operation;

(f) pre-service and in-service inspection to detect defects at sizes below those which have the potential for causing or developing into a failure mode, and to size these defects conservatively;

(g) the provision of in-service plant and materials monitoring; and

(h) the existence of a leak-before-break case.

202 For components which are not of major safety significance, this list of requirements is also relevant, though the stringency of their application should reflect the safety categorisation of the item. Principles covering those various requirements are presented below, with the exception of those on quality assurance which are in Life-cycle Requirements.

General

203 (P145) All structures important to safety should be designed, constructed and inspected to the best practicable standards commensurate with their safety categorisation in accordance with P69 and P83.

204 (P146) It should be demonstrated that all safety related structures are as defect free as possible, are tolerant to any remaining defects, and that the existence of defects can be established by inspection throughout the operational life.

Design

205 (P147) For safety-related structures, a schedule of all loading combinations within the design basis together with their frequency should be used as the basis for the design against operating, testing and accident conditions. For more severe loadings, predicted failure modes should be gradual and detectable.

206 (P148) The product form of metal components or their constituent parts (ie plate, forging or casting) should have regard to inspectability and to minimising the number and length of welds in the component where appropriate.

207 (P149) A metal pressure retaining boundary should, where appropriate, have design characteristics which prevent fast propagation of any defect. Designs and conditions in which components of the coolant pressure boundary could exhibit brittle behaviour should be avoided.

208 (P150) Where the safety categorisation of a closure or penetration to a pressurised component or system is such that the consequences of its failure could lead to a major release of radioactivity then adequate redundancy and, where reasonably practicable, diversity of closure method should be provided.

209 (P151) Provision should be made in the design to ensure that mechanical closures cannot be unlocked and removed when it is unsafe to do so and that the correct sequence is followed at all times.

210 (P152) Isolation valves should be provided where appropriate in the primary, secondary and auxiliary coolant circuits of nuclear plants. Where practicable, they should be positioned so that their operation minimises the consequences of postulated breaches in the circuit. Piping systems which are connected to or form branches from the primary pressure circuit should be provided with valves as close to the main primary circuit as practicable. The design should include adequate redundancy and diversity of such valves.

211 (P153) Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic calibration checks. Where there is need for overpressure protection suitable means should be provided to ensure that any release of radioactivity from the plant to the environment is minimised.

Manufacture and construction

212 (P154) All materials employed in the manufacture and construction should be shown to be suitable in all respects for the purpose of enabling an adequate design to be constructed, operated, inspected and maintained throughout the life of the plant.

213 (P155) The manufacture and construction should use appropriate materials, proven techniques and approved procedures to minimise the occurrence of defects which might affect the required integrity of structures or components.

214 (P156) Provision should be made for inspection during manufacture (in-process inspection) to demonstrate that the required high standard of workmanship has been achieved.

215 (P157) Where non-conformities with the procedures are judged to have a deleterious effect on integrity or significant defects are detected by in-process inspection and remedial work is considered necessary, the remedial work should be carried out to an approved procedure and should be subject to the same design requirements as the original work.

Operation

216 (P158) Means should be available to detect, locate, monitor and manage leakage which could indicate a potentially unsafe condition or give rise to a significant radiological effect.

217 (P159) Where a leak before break argument is employed for metal components, the capability and frequency of the monitoring should be commensurate with the fatigue and fracture analysis. It should also be shown by analysis that the escaping fluid itself does not present an unacceptable hazard.

218 (P160) It should be shown that safety-related components can be operated and controlled within a safe operating envelope throughout the operating life. The parameters of the envelope should be consistent with the type of construction, potential modes of failure and operational considerations.

219 (P161) For metal pressure vessels and circuits, the operating regime should ensure that they display ductile behaviour when significantly stressed.

Pre- and in-service inspection and testing

220 (P162) Provision should be made for inspection capable of demonstrating that the structure or component is manufactured to the appropriate standard and at all times fit for purpose during service. For metal components an adequate margin should exist between the capability of the defect detection and the defect sizes of structural concern.

221 (P163) Inspection techniques for structures and components should be sufficiently redundant and diverse. Personnel and equipment performance and procedures should be validated. The safety categorisation (see paragraph 131) should be taken into account, when determining the appropriate level of these measures.

222 (P164) Structures and components should be proof tested before service, where this is a code requirement or an essential part of the safety case. Where pressure retaining components must not exceed a specified leak rate, this should be confirmed by test.

Stress analysis

223 (P165) Stress analysis should be carried out to support the design and should demonstrate that the

component has an adequate life, taking into account time dependent processes. The analysis should use methods that have been verified and validated, using model tests if necessary.

224 (P166) The data used in any analysis should be demonstrably conservative. In particular, the uncertainties associated with material properties affected by degradation should be taken into account.

225 (P167) Where appropriate, studies should be carried out to determine the sensitivity of analytical results to the assumptions made, the data used, and the methods of calculation.

226 (P168) For components subject to the 'special case' procedure, and where appropriate for other metal components, the sizes of defects of structural concern should be calculated, using verified and validated fracture mechanics methods.

Additional civil engineering principles

227 (P169) Investigations should be carried out to determine the suitability of the natural site materials to support the foundation loadings specified for normal operation and fault conditions. Such investigations should follow codes and standards applicable to the structures proposed.

228 (P170) The design of foundations should utilise information derived from site and geological investigation. This information should include soil dynamic properties and any potential for liquefaction.

229 (P171) The foundations should be shown to be adequate for supporting the structural loadings specified for normal operation and fault conditions.

230 (P172) The design should be such that excavated slopes adjacent to nuclear installations are stable, and ground water draw-down will not affect such installations.

231 (P173) The design should take account of the possible presence of naturally occurring explosive gases or vapours in underground structures such as tunnels, trenches and basements.

232 (P174) All civil engineering structures should be identified and it should be determined whether they are directly or indirectly safety-related. They should be categorised according to the potential consequences of their failure and their safety functions should be stated. The required performance of the structures under all normal operating and fault conditions should be specified on the basis of this classification.

233 (P175) Where analyses have been carried out on civil structures to derive static and dynamic structural loadings for the design, the methods used should be adequately verified and validated, if necessary by model test.

234 (P176) Civil engineering structures which retain or prevent liquid or gaseous leakage should be tested against the leak tightness requirements prior to operation to demonstrate that the design intent has been met. Where appropriate, drainage systems with sampling and/or detection provisions should be provided to confirm the containment integrity of the structures or to collect and quantify leakages.

235 (P177) Provision should be made for the routine inspection of sea and river flood defences to determine their continued fitness for purpose. This provision should cover such aspects as erosion and degradation of materials and structures which protect the site.

Safety systems and safety-related instrumentation

236 Nuclear plants use a variety of systems concerned with safety. At the highest level of importance there are the safety systems. These are provided to detect potentially dangerous plant failures and to implement appropriate safety actions. The 'safety systems' principles below apply to all of the engineered systems upon which any safety function depends. They encompass, therefore, (a) protection systems which sense unsafe conditions in the plant and automatically initiate the operation of the appropriate systems for maintaining a safe condition, (b) safety actuation systems, such as heat removal systems and reactor shutdown systems which are brought in to assure the preservation of a safe condition within the plant and (c) essential services (or safety system support features) which provide electrical or pneumatic power, cooling and lubrication required by the protection system and the safety actuation systems.

237 The primary task of the essential services (or safety system support features) is that of serving the protection and safety actuation systems, but they may additionally serve specific safety-related systems and also be linked to systems external to the plant. Some further principles, therefore, are applicable to essential services and they are covered under that heading at the end of this section.

238 There are other systems, known as safety-related systems, which, while having a significant influence on safety, do not have a direct fault sequence termination function. Some safety-related systems such as ventilation and containments systems, fire-fighting etc, are covered elsewhere in the principles. However,

because of its close relationship with safety systems, safety-related instrumentation (which includes the plant control system, indicating and recording instrumentation, alarm systems and communications systems) is included in this section.

239 There is also a group of safety-related instrumentation used for the detection of criticality incidents, ie incidents involving the inadvertent accumulation into a critical mass of material which can undergo nuclear fission. This group of instruments is covered by a separate set of principles in this section.

240 Not all of the principles relevant to safety systems and safety-related instrumentation are included here, however. Additional principles which also should be applied are to be found under the heading General Principles in this section. In particular, where a computerised safety system is used, because the technology is not amenable to the traditional methods of reliability assessment, the special case procedure of P70 applies. P179 presents the elements of such a procedure to demonstrate the adequacy of a safety system using software-based technology.

Safety systems

General

241 (P178) The extent of safety system provisions, their functions, and required reliabilities should be determined from a safety schedule using the analysis specified in P26. For each system there should also be a demonstration of adequacy of the system design as the means of achieving the specified function and reliability.

242 (P179) Where the design is such that the system reliability is significantly dependent upon the performance of computer software, the establishment of, and compliance with, appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by:

(a) the thorough application of technical design practice consistent with accepted standards for the development of safety critical software;

(b) the implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards;

(c) complete, and preferably diverse, checking of the finally validated production software by a team which is independent of the system suppliers;

(d) the application of a comprehensive and independently assessed testing programme formulated to check every system function and to demonstrate the system reliability.

Capability

243 (P180) A reactor should be provided with systems which can shut it down safely in normal operating and fault conditions and maintain it in the shutdown condition with a margin of reactivity that allows for systematic changes and uncertainties in nuclear characteristics, variations in plant state and other processes or mechanisms which might affect the reactivity of the core. The safety systems of non-reactor plant should similarly be capable of achieving and maintaining a defined safe state.

244 (P181) All variables used to initiate a safety system action should be identified and shown to be sufficient for the purpose of protecting the plant. The limiting conditions for these variables for which the safety system has been qualified should be specified. The safety system should be designed to respond so that these limiting conditions are not transgressed.

245 (P182) The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.

246 (P183) The capability of a safety system, and of each of its constituent sub-systems and components, should exceed by a clear margin the maximum service requirement(s), which should be defined. The selected margin should make due allowance not only for uncertainties in plant characteristics but also for the effects of all foreseeable degradation mechanisms.

247 (P184) Adequate provisions should be made to prevent the infringement of any service requirement of a safety system, its sub-systems and components. Where prevention, or acceptably low likelihood, of infringement cannot be demonstrated, features should be incorporated to ensure a fail-safe outcome.

248 (P185) Adequate provisions, which should be classified as safety or safety-related systems as appropriate, should be made:

(a) in a central control room; and

(b) at emergency locations (preferably a single point) which will remain habitable during all

foreseeable plant emergencies;

to enable the monitoring of the plant state in relation to safety and the taking of any necessary safety actions.

249 (P186) There should be a clear and preferably direct means of confirming to operating personnel

(a) that a demand for safety system action has arisen;

(b) that the safety actuation systems have operated fully; and

(c) either directly or otherwise whether any limiting condition for which the safety system has been qualified has been exceeded.

250 (P187) Safety system actions, and all associated alarms, should not be self-resettable irrespective of the subsequent state of the initiating fault.

251 (P188) Where practicable, following the establishment of safety system action, the maintenance of a safe plant state should not depend on an external source of energy.

Failure independence

252 (P189) All foreseeable faults within a safety system which could cause any single plant variable, or combination of variables, to change to significantly less safe values should be identified and, as necessary, avoidance measures or appropriate protective features provided.

253 (P190) There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between the safety system and other plant equipment which, in the event of a fault, might jeopardise the safe working of the safety system.

Functional independence

254 (P191) The interfaces required between a safety system and the plant in order to detect any fault sequence and bring about a safe state should be engineered by means that have a direct, known, timely and unambiguous relationship with plant behaviour.

255 (P192) In those cases where it is not practicable to use a directly related variable to detect a fault sequence, the actual variable chosen should have a known relationship with the fault sequence and the physical and temporal coupling between the two should be as close as possible. Any mechanism for the transmission of misleading information should be analysed and appropriate countermeasures adopted.

256 (P193) A safety system should be dedicated to the single task of performing its safety function. Where it is necessary for other functions to be encompassed, the whole system should be classified as a safety system and the safety function should not be jeopardised by the other functions.

257 (P194) No means should be provided, or readily available, by which the configuration of a safety system, its operational logic or the associated data (trip levels, etc) may be altered other than via a specifically engineered, and adequately safe-guarded, maintenance/testing facility, used under strict administrative control.

258 (P195) Connections between any part of a safety system, other than the safety system support features, and a system external to the plant should be avoided if possible, but otherwise should be restricted in function to that of monitoring only. The temporary or permanent connection to such external equipment should incorporate adequate isolation features so that no fault associated with that equipment or its connections will jeopardise the safety system.

Reliability

259 (P196) As far as practicable the design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing faults from their times of occurrence.

260 (P197) The design of a safety system should be such as to avoid a frequency of spurious operation which might directly or indirectly degrade safety.

Testing and maintenance

261 (P198) In determining the safety system provisions (see Principle 178) allowance should be made for the unavailability of equipment due to:

(a) testing and maintenance; and

(b) non-repairable equipment failures.

The minimum amount of operational safety system equipment for which any specified plant operation will be permitted should be defined and shown to meet the single failure principle (P78).

262 (P199) It should be ensured in the design that the maintenance and testing of a safety system has no potential to initiate a fault sequence within safety-related plant.

263 (P200) As far as possible, the vetoing or the taking out of service of any safety system function should be avoided. Where nevertheless such action is proposed, each need should be justified and the adequacy of its implementation demonstrated. In a safety system comprising several redundant or diverse sub-systems no single such action should affect more than one sub-system.

Safety-related instrumentation

264 (P201) Sufficient indicating and recording instrumentation and controls should be available to the plant operator in a central control room, and as necessary at appropriate locations on the plant to provide:

(a) adequate monitoring of the state of the plant and the status of all plant equipment;

(b) timely and conspicuous early warning of any safety-related changes of state; and

(c) the means of identifying, initiating and confirming all necessary safety actions.

The provisions should encompass the circumstances both of normal operation and of postulated fault conditions including, where reasonably practicable, severe accidents.

265 (P202) Adequate 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. These communication systems should not have any adverse effect on safety systems or other safety-related instrumentation systems.

266 (P203) All safety-related instrumentation should be operated from power supplies whose reliabilities are consistent with the functions being performed. In the cases of monitoring, warning, and communication functions the supplies should be uninterruptable.

267 (P204) Instrumentation should be provided to enable monitoring of the locations and quantities of radioactive materials which may escape from their engineered environment.

268 (P205) The minimum safety-related instrumentation for which plant operation may be permitted should be specified and its adequacy justified.

269 (P206) Control systems should respond in a timely and stable manner to normal plant disturbances without causing demands on the safety systems.

270 (P207) An analysis should be provided which identifies the foreseeable ways in which control systems under fault conditions, including multiple control faults, could generate demands on plant safety systems. Faults in control systems and other safety-related instrumentation should not cause an excessive frequency of demands on a safety system.

271 (P208) Where computers or programmable devices are used in safety-related systems evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards, in accordance with the categorisation of paragraph 131.

272 (P209) The reliability, accuracy, stability, response time, range and, where appropriate, the readability of all safety-related instrumentation should be adequate for its required service.

Criticality incident detection (CID) systems

273 Safety systems should be provided to deal with criticality incidents in line with the requirements of the principles presented above and they should be the primary defence against such events. However, in many operating situations it is not possible to be confident that all the potential criticality fault sequences have been foreseen and, therefore, that the safety systems will be adequate. A CID system provides an additional layer of safety by causing prompt evacuation of personnel and therefore limitation of consequential dose.

274 A CID system is strictly an alarm system and therefore is classified as safety-related instrumentation for the purposes of the application of safety assessment principles. The following specific principles also should be applied.

Principles

275 (P210) Adequate criticality incident detection (CID) systems should be provided at all places where fissile material is present, unless an assessment shows that a criticality excursion of the maximum foreseeable size could not give any individual a whole body dose exceeding the annual dose limit or that the predicted frequency of the excursion is acceptably low.

276 (P211) The areas from which evacuation is required should be defined. When triggered the CID system should give an audible alarm of adequate strength throughout the whole of that area and should continue to sound until manually reset. The reset facility should be located outside the evacuation area and access restricted to authorised personnel.

277 (P212) The electrical power supply to the CID system should be capable of maintaining effective surveillance and support of its alarm operation for a period sufficient to ensure safety following loss of normal electrical supplies.

278 (P213) The reliability requirements of the CID system should be specified and justified. Reliability assessments should be provided which demonstrate that the system meets these requirements.

Essential services

279 Essential services are all those resources necessary to maintain the safety systems in an operational state at all times; and they may also provide supplies to safety-related systems. The services may include electricity, gas, water, compressed air, fuel and lubricants, and may need to satisfy two requirements. The first requirement is to provide a guaranteed, or non-interruptable short term supply to ensure continuity until the long-term essential supply is established, and the second is to ensure that there is adequate capacity to supply the service until normal supplies can be restored. The following principles are additional to the safety system principles above, which also apply to essential services.

Principles

280 (P214) Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and fault conditions.

281 (P215) Where a service is obtained from a source external to the nuclear site that service should where practicable also be obtainable from a back-up source on the site.

282 (P216) Each back-up source should have the capacity, availability and reliability to meet the maximum requirements of all of its dependent systems and to provide that service for a sufficient period of time to allow the plant to be brought to a safe state and maintained therein until such time as the normal supply is restored.

283 (P217) Where essential services are shared with other plants on a multi-plant site, the effect of the sharing should be taken into account in assessing the adequacy of the supply.

284 (P218) Alternative sources of essential services should be designed so that their reliability would not be prejudiced by adverse conditions in the normal services to which they provide a back-up.

285 (P219) Protection devices provided for essential service components or systems should be limited to those which are necessary and which are consistent with plant requirements. Their possible action should be taken into account in the reliability assessment.

286 (P220) Where a source external to the nuclear site is employed as the only source of the essential services needed to provide adequate protection, the specification and in particular the availability and reliability should be the same as for an on-site source.

287 (P221) For essential electrical systems, the services should be so designed that the simultaneous loss of normal and on-site a.c. electrical power will not lead to unacceptable consequences in the short term.

Plant specific principles

Containment and ventilation

288 Containment and ventilation systems are provided to control the spread of nuclear matter within the plant and its escape to the environment, in normal operation and fault conditions. The term 'containment' encompasses a wide range of structures and plant items, from the massive buildings surrounding power reactors to glove boxes. Containments often have associated systems, such as cooling systems and sprays, which are considered to be part of the containment system.

289 Ventilation systems are also important in limiting the spread of radioactive contamination. To this end, the plant may be divided into zones separated by barriers. Each zone is ventilated so that there is a pressure gradient between adjacent zones, the aim being to ensure that any movement of radioactive material is from the zone with the lowest to that with the highest potential for contamination. The ventilation system includes any equipment such as filters or other gas cleaning facilities which may be provided to mitigate the consequences of radioactive release.

290 Where equipment forming part of containment and ventilation systems serves as part of a safety

system the general principles applicable to engineering and safety systems should also be applied.

291 The potential for a fire can have a major impact on the design of the ventilation and containment system, influencing for example the position, number and type of fire dampers. In addition to the principles in this section, other impacts of fire may need to be considered, and reference should be made to Protection Against Fire (P141 to P143)

292 The principles in this section apply generally unless the wording makes it clear that limited application was intended or unless it can be shown that the total amount of nuclear matter concerned is sufficiently small or is in such a chemical or physical form as to make it unnecessary to apply any one or more of the principles.

Containment

293 (P222) Containment and associated systems should be provided as appropriate for nuclear plant to limit radioactive releases to the environment in normal operation and fault conditions and to protect the plant from external hazards.

294 (P223) Nuclear matter should be adequately contained and ventilated until it is discharged or disposed of as radioactive waste under an authorisation granted in accordance with the Radioactive Substances Act 1960.

295 (P224) Containment boundaries should be defined. The containment should be capable of withstanding the effect of internal and external hazards in accordance with the provisions of principles P119 to P143 above so that the safe state of the plant is maintained.

296 (P225) There should be adequate provision for making the plant safe following any incident involving the release of nuclear matter within or from a containment, and the necessary equipment should be provided so that if necessary decontamination and post-incident re-entry can be safely carried out.

297 (P226) Attention should be paid to the possibility of nuclear matter escaping from containment via routes installed for other purposes. Penetrations of the containment should be minimised in size and number and adequately sealed, and piping, ducting and drains which may serve as routes for escape or leakage from containment should themselves be contained and provided with an appropriate means of isolation, monitoring and alarm systems where feasible.

298 (P227) The use of ducts which must be sealed by isolating valves under accident conditions should be avoided as far as reasonably practicable. The facilities provided for the isolation of such penetrations should be consistent with the required containment duties and should not prejudice adequate containment performance.

299 (P228) The containment may be provided with a pressure relief system if a safety advantage can be shown. In the event that the relief system operates during or following faults the performance of the containment should remain adequate.

299 (P229) Pressure relief devices should be provided with an appropriate treatment system to reduce the radioactive releases to acceptable levels. The system should be capable of operating under fault conditions.

300 (P230) Waste storage vessels, process vessels, piping and other plant items which act as containment for nuclear matter should be provided, where appropriate, with:

(a) a further barrier or barriers (secondary containment) having sufficient capacity to deal safely with the leakage resulting from any design basis accident;

(b) mechanisms for the safe relocation of the bulk material from both primary and secondary containments;

(c) redundant storage with sufficient capacity and associated services to ensure prolonged safe storage of the maximum anticipated volume of material requiring relocation, allowing for any volume increase due to the method of transfer (eg the use of ejectors).

301 (P231) Monitoring devices with alarms, and facilities for sampling should be provided as necessary to ensure detection and aid assessment of unplanned or uncontrolled changes in the volume of nuclear matter (caused for example by a leakage of cooling water or swelling of ion exchange resins) or in the radioactivity of the materials within the containment.

302 (P232) Where facilities are required for bringing nuclear matter out of the plant containments, the number of such facilities should be minimised and the design should ensure that the overall containment and ventilation standards are not degraded and, where appropriate, it should:

(a) provide remote handling devices and means to facilitate their operation, decontamination and repair; and

(b) provide additional containment, local ventilation, and shielding.

303 (P233) Appropriate sampling and monitoring systems and other facilities should be provided to monitor safety-related conditions within the containment and to detect, locate, identify and quantify leakages of nuclear matter from the containment under normal and accident conditions. There should be provision for environmental surveys in the vicinity of plant.

304 (P234) The need for access by personnel to the containment should be reduced to the minimum that is reasonably practicable. There should be no requirement for access to the containment to ensure the safety of the plant in either the short term or long term following an accident. Such access facilities as may be provided should be designed so as to ensure that at all times the containment will perform its safety function adequately.

305 (P235) Where routine personnel access to the containment interior or other hazardous areas is necessary, appropriate emergency escape and rescue facilities should be provided.

306 (P236) Where appropriate, the plant design should facilitate the removal and reinstatement of shielding and containment for maintenance purposes.

307 (P237) The design of glove boxes and their ventilation systems should be such as to prevent over-pressurisation, and accommodate failure of the glovebox pressure envelope.

308 (P238) Movement of material into and out of gloveboxes should be by means of an engineered transfer system.

Ventilation

309 (P239) The plant design should incorporate a ventilation system, including filtration or other appropriate treatment systems, which will under normal operating and fault conditions:

(a) provide a suitable working environment for personnel and safety related equipment particularly in the control rooms;

(b) ensure that the flow of ventilation air within buildings is always from zones of lower to higher levels of potential contamination, and maintain the segregation of process and breathing zone air streams;

(c) control the dispersal of contamination, and reduce the concentration of airborne activity in the plant atmosphere and in aerial discharges;

(d) control the temperature, pressure and composition, including where appropriate the moisture content, of the atmosphere inside the containment as necessary;

(e) segregate and isolate hazards and prevent the mixing of ventilation streams of different hazard potentials, eg explosive, toxic and radioactive, until they have been neutralised;

(f) minimise the risk arising from the chemical and toxic properties of process materials and from explosive mixtures, including gases and vapours, which may be generated;

(g) facilitate, where appropriate, permanent or temporary access to plant zones without impairing the performance of the system;

(h) restrict the outward flow of building air to appropriately controlled discharge points.

310 (P240) In the design, account should be taken of wind velocity, of possible air pressure fluctuations caused by nearby structures and discharges from other plants. Intakes should be sited so as to avoid contamination of intake air during normal and fault conditions in the plant and on the site. Inlet filters should be provided where appropriate.

311 (P241) The location of ventilation filters should be such that dose rates to plant personnel are minimised; where necessary, shielding should be provided. There should be provision for the safe replacement of filter elements and the safe storage of contaminated filters. Facilities should be provided to enable filters to be changed while maintaining the effectiveness of the ventilation system.

312 (P242) The design should provide for:

(a) monitoring and testing of ventilation systems and associated filters and gas treatment systems to ensure that they continue to meet the design requirements;

(b) appropriate alarm/control systems on key plant parameters.

Heat transport systems

313 The principles in this part relate to the systems required to transport heat within the plant both in normal operation and fault conditions.

314 The general principles cover the full range of heat transfer applications in reactors, chemical plants, fuel storage ponds etc. These are followed by some principles applicable only to reactors.

General

315 (P243) The various sources of heat to be added to or removed from any system and its component parts under normal and fault conditions should be quantified and the uncertainties estimated in each case. Heat transport systems should be designed so that heat may be added or removed at an adequate rate at all times.

316 (P244) Inherent cooling processes such as natural circulation can be taken into account in assessing the effectiveness of the heat transport system, provided they are shown to be effective in the conditions for which they are claimed.

317 (P245) In the case of liquid heat transport systems there should be an adequate margin against failure of the operating heat transfer regime under all anticipated normal and fault conditions and procedures. The minimum value of this margin should be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.

318 (P246) The properties of any heat transport fluid, its composition and impurity levels should be so specified as to minimise adverse interaction with plant components and any degradation of the fluid caused by radiation. Appropriate chemical and physical parameters should be monitored and filtration, processing or other plant provided to ensure that the specified limits can be maintained.

319 (P247) Safety-related structures and plant should be protected as appropriate from the radiation, thermal and dynamic effects of any fault involving the heat transport fluids.

320 (P248) Where mutually incompatible heat transport fluids are used within the plant, provision should be made to prevent their mixing and, where appropriate, to prevent harm to personnel and safety-related structures in the event of such mixing.

321 (P249) The design, construction and operation of the plant and the choice of heat transport fluid should be such that the amount of radioactive material in that fluid is kept to a minimum. Facilities should be provided where appropriate to remove radioactive materials from the heat transport fluid and associated containment.

322 (P250) Adequate provisions should be made in the design to prevent failure of the heat transport system, of its containment or changes in geometry which could adversely affect the heat transfer process, or safeguards should be available to maintain the plant in a safe condition and prevent any release in excess of safe limits.

323 (P251) Provision should be made to minimise the effect of faults within the plant which may propagate through the heat removal (and ventilation) systems.

324 (P252) Unless monitoring or analysis demonstrates it to be otherwise, any potentially contaminated heat transport fluid which leaks from its containment and all potentially contaminated spent fluid should be regarded as radioactive waste and handled in accordance with the requirements of principles P294 to P307.

325 (P253) Adequate provision should be made for the detection of significant loss of heat transport fluid or any other adverse change in heat transport which might lead to an unsafe state.

326 (P254) Where appropriate, provision should be made for a sufficient and reliable supply of reserve heat transfer fluid, separate from the normal supply, to be available in adequate time in the event of any significant loss of heat transfer fluid.

Reactor specific principles

327 (P255) Provision should be made for removal of the decay heat from the reactor to an adequate heat sink at any time throughout the life of the plant irrespective of the availability or otherwise of external resources.

328 (P256) As far as reasonably practicable, reactor components should be fabricated from materials which are free of elements susceptible to neutron activation and liable to contaminate the heat transport system.

329 (P257) Facilities for removing and storing the reactor coolant to allow inspection and repair work should be provided where appropriate and reasonably practicable.

330 (P258) Possible effects of changes in coolant

condition or composition on the nuclear reactivity of the reactor core should be identified and adequate provision should be made to limit the consequences of any adverse change of this kind either by the provision of appropriate protective systems or by the selection of appropriate reactor core design parameters.

331 (P259) Adequate provisions should be made in the design to minimise leakage of the reactor coolant and keep it within specified limits.

Reactor core

332 The principles described in this part apply to the reactor core as an assembly and to its main elements, the fuel and neutron absorbers, and breeder assemblies in fast reactors, individually when in that core. The principles relate to the requirements to control reactivity, heat generation and heat removal so that the fuel within the reactor can be kept within specified limits set to ensure safety during operation.

Principles

333 (P260) It should be shown that the reactor core design takes account of all operating modes including normal operation, refuelling, testing, shutdown and fault conditions.

334 (P261) The core should be stable in normal operation and should not undergo sudden changes of condition when operating parameters go outside the specified range. The stress and strain limits for the core structure and the fuel should ensure that their geometry will be adequately maintained.

335 (P262) The design of the core should take account of all identifiable environmental effects including irradiation, chemical and physical processes, and static and dynamic mechanical loads; and also of thermal distortion, thermally-induced stress, possible variations in manufacture and any other identified safety-related factor.

336 (P263) The core should be securely supported and positively located with respect to other components in the reactor. Gross unplanned movements of the structure of the core or adverse internal movements should be prevented by design.

337 (P264) The geometry of the core should be maintained within limits which enable passage of sufficient coolant to remove heat from all parts of the core. Where appropriate, means should be provided to reduce to a minimum the chance of any obstruction of the coolant flow which could lead to damage to the core as a result of overheating.

338 (P265) The design of the core should be such that reactor shutdown is not inhibited by mechanical failure, distortion, erosion, corrosion, etc of plant components or by the physical behaviour of the reactor coolant, under normal operation or fault conditions.

339 (P266) All components of the core should be mutually compatible and compatible with the remainder of the plant.

340 (P267) The incorrect location in the core of any safety-related components including fuel elements, breeder elements and absorbers should be physically inhibited as far as practicable.

341 (P268) The core should be so designed that all safety-related conditions can be monitored to an adequate degree of accuracy.

342 (P269) Fuel assemblies should be designed to permit adequate inspection of their structure and parts before loading into the core and provision should be made as appropriate for in-service monitoring and post-irradiation inspection to confirm fuel behaviour and performance.

343 (P270) The loss from, or addition to, the core of any component or any movement of any component within it which could cause a fault condition, as a result of an increase in nuclear reactivity or reduction in coolant flow, should be prevented by design.

344 (P271) The nuclear characteristics of the core should be such that temperature changes or coolant voiding, or changes in core geometry, which could occur in normal operation or fault conditions do not cause uncontrollably large or rapid increases in reactivity. There should be adequate design margins to ensure that any reactivity changes do not lead to unacceptable consequences.

345 (P272) No moveable fissile assembly or absorber when added to or removed from the core should increase the nuclear reactivity by an amount greater than the shutdown margin, with an appropriate allowance for uncertainty.

346 (P273) The design should be such that all fuel can be removed from the reactor, despite any environmentally induced damage such as bowing or from other damage occurring in normal operation and in design basis fault conditions.

347 (P274) The design should be such as to prevent overheated fuel causing failure of the primary

coolant circuit or the fuel geometry being so changed as to affect adversely the heat transport process. Safeguards should be available to maintain the plant in a safe condition if this is not practicable.

Shielding

348 (P275) The design of shielding should be such that the radiation dose rates do not exceed the levels of principle P14 and should take account of the likely build-up of radiation levels during the life of the plant.

349 (P276) Special precautions should be taken in the design of shielding and associated equipment to minimise:

(a) the incidence of localised high levels of radiation due to streaming;

(b) unplanned or uncontrolled movements of shielding;

(c) installation behind shielding of components requiring regular handling or to which regular access is required, except where such components are themselves sources of radiation requiring shielding;

(d) undue doses to extremities of workers during access to and manipulation of radioactive sources;

(e) unplanned or uncontrolled removal from behind shielding of any source which could cause a significant radiological effect when unshielded; and

(f) the presence of locations which could result in the accumulation of solids of safety significance. Where such locations cannot be avoided the design should include the provisions for detecting the presence of such materials and facilitating their safe removal and disposal.

350 (P277) Where liquid is used as a shielding material there should be design provisions for preventing loss of such liquid and suitable means should be provided for detecting changes in liquid level and initiating an alarm in the event of any potentially unsafe change.

Control of nuclear matter

351 This part deals with the general control of nuclear matter, which includes radioactive waste as well as nuclear fuel and absorbers, other than that which is in the core of a reactor. These principles should be used in carrying out an assessment except where the total amount of nuclear matter is so small or is in such a form that certain principles can be shown to be inapplicable. In interpreting and using this section, assessors should refer also to the section on ventilation and containment.

Note: Radioactive waste may not be disposed of or otherwise removed from a nuclear site unless an authorisation for that purpose is issued under the Radioactive Substances Act, 1960. Close cooperation, as laid down in the Holdgate-Rimington agreement[8], is necessary therefore between NII inspectors and the Authorising Departments (see note to paragraph 42) in assessments having a bearing on such disposals or removals.

General

352 (P278) Nuclear matter should not be generated on or brought onto a site unless suitable facilities and arrangements exist for its safe transport, handling, processing, storage and/or disposal. In particular:

(a) the arrangements should ensure that the type and form of the nuclear matter and the maximum inventories of that matter are within specified limits consistent with the safe operation of the plant, including where appropriate, plant sub-divisions or individual plant items;

(b) the facilities and associated arrangements should be sufficiently flexible to enable the handling and storage of abnormal items which might be produced on or arrive at the site (eg damaged or faulty fuel or containers, and material of non-standard physical or chemical composition).

353 (P279) A control regime should be established whereby all nuclear matter can be procured, handled, processed, transported, stored, inspected and where appropriate retrieved and disposed of safely.

354 (P280) The design of the plant and the control regime applied during its operation should:

(a) facilitate arrangements for controlling and keeping adequate records of the location, nature and quantities of all nuclear matter entering, leaving, stored and, where appropriate, moving within a plant and for preventing unauthorised access to and removal of nuclear matter;

(b) prevent unintended accumulation and unplanned or uncontrolled movement of nuclear matter and, where this is possible, make provision for inspection and detection, and for appropriate alarms to enable timely corrective action to be taken;

(c) ensure that the quantity of nuclear matter within the process is the minimum consistent with operational requirements.

355 (P281) There should be adequate provision to ensure that under normal and fault conditions nuclear matter is:

(a) cooled, monitored and controlled where the heat from radioactive decay or chemical reaction may be significant, and managed so that chemical reactions, precipitation, acidity etc are kept within the specified limits;

(b) segregated both from incompatible materials and according to physical and chemical form, flammability, specific radioactivity, half-life, fissile nature and type of radiation emitted where subsequent storage, processing, conditioning and disposal would otherwise be adversely affected.

356 (P282) Storage facilities for nuclear matter and the contents of the facilities should be adequately protected and maintained against any adverse environmental effects until such time as any waste is disposed of or the facility is decommissioned.

357 (P283) Nuclear matter which might contain, generate or release gases or liquids should be kept in containers with suitable ventilation, pressure relief or sump facilities.

Fissile materials

358 (P284) The potential for unplanned criticality during normal plant operation and fault conditions should be minimised. Representative cases should be analysed conservatively, taking into account all reasonably foreseeable circumstances and configurations. The analysis should fully take account of the variability of factors such as geometry, material composition, neutron moderation, reflection and absorption, fissile material quantity (adventitious accumulation etc), and interaction effects, and of deficiencies in accounting procedures, enrichment identification and burn-up credit etc. The safety factors and margins used should be justified.

359 (P285) Provisions for cleaning, inspection and measurement to facilitate the periodic establishment of the fissile material inventory, should be incorporated in plant in which fissile material is treated, processed or stored.

360 (P286) At all places where fissile material may be present, there should be a system of controls to prevent unplanned criticality. There should be adequate justification of these provisions, and where safety is based on configurations of materials or on circumstances other than the most reactive this should also be justified.

361 (P287) The design and operation of plant and equipment should be such as to facilitate the safe recovery from a criticality accident.

Process control

362 (P288) The plant design and flowsheet should be such as to minimise the need to move radioactive material on the site.

363 (P289) A sufficient quantity of buffer storage should be provided, where appropriate, between unit operations to adequately decouple any process perturbations which have safety implications.

364 (P290) Monitoring of key plant parameters should rely as far as is practicable on instrumentation which does not require nuclear matter to be diverted outside the main containment.

365 (P291) Sampling nuclear matter as a method of process control should be avoided. Where samples have to be removed from the containment, appropriate arrangements should be specified for their return to the process after use or for their treatment, storage or disposal as appropriate.

366 (P292) Provision should be made for the decontamination of vessels, pipework, plant equipment and containment structures prior to maintenance or modification and following final use.

367 (P293) Control limits should be defined and monitoring, recording and alarm systems provided to detect significant deviations from normal operating levels as an aid to maintaining plant control.

Radioactive wastes (general)

368 (P294) The nuclear plant design should be such that so far as reasonably practicable the quantity of radioactive waste (including secondary waste) and

scrap arising during commissioning, operation and decommissioning is minimised.

369 (P295) The generation of radioactive waste of a type or form incompatible with currently available storage or disposal technology should be avoided.

370 (P296) Radioactive waste stored on site should be in a form which minimises the hazard of storage and is compatible with retrieval and with any subsequent storage, transport or disposal route, and it should be appropriately monitored and inspected to ensure that it remains in such a form.

371(P297) The administrative and physical arrangements should be such that waste and scrap is at all times kept in a safe state and the radiological consequences of normal plant operations, recycling, salvage, decommissioning and storage operations are minimised.

372 (P298) Adequate provision should be made for:

(a) monitoring and maintaining in a safe state accumulations of stored radioactive waste and scrap;

(b) determining and recording appropriate details (eg quantity, type, origin and form) of the radioactive waste or scrap in a manner which is durable for the anticipated period prior to final disposal;

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

373 (P299) Waste streams arising from the decontamination of plant or equipment should be treated as radioactive waste and managed accordingly.

374 (P300) Appropriate and sufficient locations should be provided within the plant where process materials, plant items, construction materials and other items arising from plant breakdown, maintenance or refurbishment can be temporarily stored so that their level of contamination, chemical and physical properties, ease of decontamination and repair can be assessed.

375 (P301) Without prejudice to the requirements of the authorising departments, the means of control of discharges of liquid or gaseous wastes should be such that the radiological consequences on site are minimised.

376 (P302) Arrangements should be made which prevent:

(a) the inadvertent discharge of liquid waste, by means if necessary of buffer, hold-up or feedback facilities;

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

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

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

(e) the discharge of waste to the environment via routes not intended, designed or authorised for that purpose.

377 (P303) For the purposes of minimising the consequences of accidents and the on-site consequences of routine discharges, the position and design of discharge outlets should take into account the characteristics of the surrounding terrain, weather conditions and the proximity of buildings and stacks, both with regard to the aerodynamics of the discharge and the compatibility of discharges and operations in adjacent buildings.

378 (P304) The characteristics of the waste, in terms of total activity, concentration, and other physical and chemical properties with which any discharge treatment facility may have to deal during foreseeable fault conditions, should be taken into account in the design of the facility.

379 (P305) Radioactive waste should not be disposed of or otherwise removed from a nuclear site, except to an installation or place authorised for the purpose of receiving such waste.

380 (P306) Waste containment and transport provisions should be compatible with the storage and disposal facilities.

381 (P307) Where solid wastes are stored under water, the assessment principles relevant to the storage of liquid waste should be used as appropriate.

Radioactive scrap

382 (P308) A justification should be provided whenever nuclear matter is designated as scrap. Adequate records including, contamination levels and ultimate destination, should be maintained of all arisings of scrap.

Storage, handling and transport of nuclear matter (including nuclear fuel and absorbers)

383 (P309) Building and site layouts should be such that the movement of nuclear matter between buildings is minimised.

384 (P310) The operational limits to be applied during the storage, handling and transport of nuclear matter should be specified.

385 (P311) The plant and equipment and the systems of work for storage, handling and transporting nuclear matter on the site should be such that the risk of damage to the containment of such materials, to the materials themselves and to any adjacent plant, is minimised.

386 (P312) Where any machine or plant component is connected to, or physically associated with, the containment of nuclear matter in order to handle or move it, the design, construction, maintenance and operation should be such that the performance of the containment is not impaired.

387 (P313) The facilities for the storage of nuclear matter on site and the procedures used, should be adequate having regard to:

(a) the maximum duration of the storage of the nuclear matter, based on the lifetime of the plant which it serves and the availability of a final disposal route;

(b) the chemical and physical properties (including the possibility of criticality) of the nuclear matter and its containment taking into account any changes in the chemical or physical form which might occur during extended storage;

(c) the need for the nuclear matter to be readily recoverable by means which enable retrieval and relocation to take place on an appropriate timescale; and,

(d) the requirement to have adequate storage capacity and redundancy.

388 (P314) All containers or packages used for the transport or movement of nuclear matter on site or within the plant should be appropriately marked or labelled. The marking or labelling should ensure that their contents can be adequately controlled and their destinations indicated. Storage areas and facilities should be clearly identified and delineated.

LIFE-CYCLE REQUIREMENTS

Introduction

389 The safety case submitted by a licensee is aimed at demonstrating that a plant will be safe when it comes into operation. In order to achieve that safety, the construction of the plant, its commissioning, operation and ultimately its decommissioning must be consistent with the assumptions and commitments made in the safety case. The day-to-day activities during each of these phases will be regulated through conditions attached to site licences. The principles presented in this section deal with the forward look which the NII has to take towards those phases and the regulatory regime that will be in force. They address, therefore, the consistency between the safety case and actions necessary from the start of construction onwards.

390 Under the Nuclear Installations Act, the licensee has the ultimate responsibility for the safety of plant. It is necessary therefore for him to have an effective management system which will ensure that a high standard of safety will be maintained throughout the various phases of its life. An important aspect of an effective management system is the development of a safety culture which at all levels within the organisation emphasises safety, and which by the use of managerial, supervisory and individual practices and constraints sustains attention to safety through an awareness of the risks posed by the plant and of the potential consequences of incorrect actions.

391 Quality assurance is an essential part of an effective management system. It provides a disciplined approach which ensures that arrangements are in place covering all safety-related activities throughout the life of the plant. In order to give further confidence, it is important that the part of the organisation responsible for monitoring that the arrangements are fully implemented will have sufficient authority and be independent from commercial pressures.

392 The construction phase covers the civil engineering work on buildings and structures, the manufacture of plant items and the installation of those items on the site. In this phase the licensee needs to show that the site work is being carried out, and the plant and the individual items which go into it are being manufactured and constructed, to the required standards. Commissioning follows on after construction and is the process whereby the plant is put to work in a systematic manner in order to confirm that its performance meets the design intent and that the plant is capable of operating in accordance with the safety case.

393 Operational limits need to be set on the basis of the safety case analyses and other aspects of the operational life, such as maintenance requirements, are also linked to safety case commitments.

394 Decommissioning is the reverse of construction and commissioning: when the plant reaches the end of its working life the licensee must be able to take the plant out of service safely and reduce to an acceptable level and ultimately remove the risk from the plant. The licensee needs to be aware of this from the start and, in the pre-operational phase, he is expected to produce a preliminary decommissioning plan and a safety case in support of it.

395 Despite the high safety standards expected on a nuclear site, consideration has to be given to the possibility of an accident. Accident management is a topic which came into focus as a result of the accident at Three Mile Island and has received even more attention since the accident at Chernobyl. The nuclear site licence specifies the requirements for emergency arrangements to be produced and exercised at licensed nuclear installations in this country, but the preparations for this need to be made from the design stage onwards. Accident management may be described as the application of preplanned procedures or ad hoc actions to control the course of accidents in which the barriers to the release of radioactive materials are challenged or breached, in order to prevent or mitigate the consequences and to bring the plant to a safe stable state in the long term. To achieve this, two main areas will need to be addressed. The first is the training of personnel in the accident management procedures, and the second is the provision of instrumentation and other relevant equipment necessary to monitor and control the accident.

Management systems

396 (P315) A safety culture should be established which will enhance and support the safety actions and interactions of all managers, personnel and organisations involved in the safety activities relating to the nuclear plant. The commitment to this should be demonstrated by a written safety policy which is implemented appropriately at all levels and in which safety performance is monitored.

397 (P316) All functions which will have a bearing on the safe operation of the plant should be identified and the duties of personnel given responsibilities for those functions, including arrangements for any delegation of responsibilities, should be defined.

398 (P317) Quality assurance (QA) arrangements should be established and implemented which will eventually cover the whole of the life of the plant. The arrangements should be reviewed periodically. Persons and organisations responsible for verifying correct performance should have appropriate authority and independence.

399 (P318) Each phase in the life of a plant should be covered by a document which describes the commitment to the adoption of QA principles. The principles should be based on national or international standards or other defined documents.

400 (P319) The document for each phase should be available for implementation before commencement of that phase and should identify all activities that are necessary to achieve the required level of safety, the structure of the organisations responsible for the activities, and the authority, responsibility, and interfaces of specific parts of the organisations. Support documentation should provide more detailed information concerning management, organisation and responsibilities, along with the administrative and technical procedures and instructions.

401 (P320) There should be provision for identifying, updating and preserving documents and records relevant to plant safety. Particular attention should be paid to those which would assist management in the event of incidents, in making modifications and in decommissioning, or which would contribute to improvements in plant design.

402 (P321) Provisions should be made for training of staff who will have responsibility for the safety of the plant. These should include a management system for training on the site, analysis of jobs and tasks, development of training methods, assessment of trainees, revision training as required, and regular evaluation of training.

403 (P322) Arrangements should be made for obtaining and utilising information and experience from national and international sources relevant to the safe operation of the plant.

Construction

404 (P323) Construction should be carried out in accordance with approved procedures. No change which might affect safety should be made to the plant except in accordance with a procedure which will ensure that safety is not compromised. The procedure should also provide for amendments of the safety case as appropriate, such that the safety case and associated documents define the as-built plant and justify its safety.

Commissioning

405 (P324) The safety case should identify those

commissioning tests and inspections required to:

(a) confirm the plant's design safety assumptions and predicted performance, in particular that of the safety provisions;

(b) characterise the plant as a basis for evaluating its behaviour during its operating life.

The safety analysis should be reviewed in the light of the results of the commissioning programme and of any modifications made to design or intended operating procedures since the commencement of construction.

Operating limits

406 (P325) The plant parameters relevant to safe operation should be identified and operational limits on those parameters derived such that in the event of any design basis fault sequence:

(a) the integrity of the physical barriers to radioactive release is maintained and the fault consequences limited as required by P25; and

(b) no safety-related component (or structure or system) required to prevent or mitigate the fault sequence will be caused to operate outside the conditions for which it has been qualified.

407 (P326) Where a safety-related item is required to work only in the event of a fault, its safe operating limits should be appropriate to any reasonably foreseeable combination of plant conditions likely to arise during the fault.

408 (P327) The limits referred to in P325 should be set having regard to the expected extremes of plant conditions at any time. Account should be taken of all relevant combinations of parameter values which are expected. The possibility of both short and longer term or cumulative damage processes should be considered in defining and setting these limits.

409 (P328) The minimum staffing levels of suitably qualified and experienced people and the minimum level of operational equipment necessary to ensure safety in normal or fault conditions should be specified.

Maintenance, inspection and testing

410 (P329) The requirements for in-service testing, inspection or other maintenance procedures and frequencies for which specific claims have been made in the safety case should be identified and included in a maintenance schedule.

Decommissioning

411 (P330) The licensee should prepare an outline decommissioning plan which shows that the design of the plant will facilitate its safe decommissioning and dismantling. In particular the design should ensure that:

(a) the choice of materials and construction is such as to minimise eventual quantities of radioactive waste and to facilitate decontamination;

(b) any important access facilities required for decommissioning are provided;

(c) adequate facilities are provided for treating and storing radioactive waste generated during both operation and decommissioning.

Accident management

412 (P331) Accident management strategies should be developed to reduce the risk from severe accidents. The strategies should primarily aim to prevent the breach of barriers to release or, where this cannot be achieved, to mitigate the consequences. The ultimate objective should be to return the plant to a controlled state in which it can be maintained in a safe condition.

413 (P332) The strategies should identify any instrumentation needed to monitor the state of the plant and the level of severity of the accident, and any equipment to be used to control the accident or mitigate its consequences. Where additional hardware would facilitate accident management, this should be provided if reasonably practicable.

414 (P333) Provision should be made in the strategy for training plant personnel in accident management procedures and implementing the accident management strategies, utilising appropriate instrumentation and items of plant that are qualified for operation in severe accident environments.

APPENDIX I

Notes on the numerical principles for operations

Persons working with ionising radiations (P11)

1 The BSL value of 20 mSv for "persons working with ionising radiations", is in line with current ICRP thinking on dose limits, without the ICRP flexibility of "averaging over 5 years provided 50 mSv in any single year is not exceeded". We consider that this flexibility is a provision that should be retained for operational purposes and not used in design safety studies. Using the currently accepted risk/dose value of 4×10^{-2} per Sv for a working population, the BSL value equates to a risk of death slightly lower than 10^{-3} per year proposed in TOR as the limit of tolerability for the risk from all sources.

2 In setting a BSO level, however, we judged that 10^{-6} per year level proposed in TOR as the "broadly acceptable" risk to an individual of dying from a particular cause would result in a level (.025 mSv) which was below the reasonably practicable range. The BSO was set, therefore, at a level which would ensure that the licensee made a strenuous pursuit of the ALARP objective, but which on the other hand would not involve the assessors in pursuing every safety case into an ALARP justification.

Other workers on site (P11)

3 The BSL value of 5 mSv for other workers on site is intended to equate to the level above which workers would be expected to be treated as persons working with ionising radiation.

4 The BSO value for other workers on site is set at 0.5 mSv on the same grounds as those used in paragraph 2 of this appendix.

Group averages (P13)

5 The concept of an average dose is a particularly useful principle, since in many design safety cases dose budgets are used which provide information on collective doses and relate them to the number of workers. Clearly we cannot have a numerical collective dose principle which can be generally applied, since the number of workers is a variable factor.

6 The BSL and BSO values are set at half of the values in principle P11, a choice reflecting the need for group average values to be less than individual doses.

Members of the public (P14)

7. The BSL is set at 1 mSv the principal ICRP dose limit. This equates with a fatality risk of 5×10^{-5} per year which is lower than the fatality risk of 10^{-4} per year proposed in TOR as the limit of tolerability for members of the public.

8 The BSO of 0.02 mSv equates with the 10^{-6} per year level proposed in TOR as the "broadly acceptable" risk to an individual of dying from a particular cause. It is a demanding value but one which evidence to the Hinkley Point C public inquiry suggests is achievable for new plants on 'green-field' sites, though there may be more difficulty on multi-plant sites housing older plants.

APPENDIX 2

Notes on the numerical principles for accident conditions

Design basis accidents (P25)

1 The design basis analysis assumes (on the basis of the engineering analysis) that the safety systems will perform as intended and demonstrates that they will effectively prevent the fault condition escalating. The consequences will in most cases be negligible or only a small addition to the releases in normal operation, but some design basis fault sequences assume associated failures (eg of relief valves to reclose) which will leave open (temporarily) a pathway for the escape of activity and hence give a somewhat greater release. Principle P25, however, stipulates that the release should in no case give an offsite dose of more than 100 mSv, which, taking into account the conservatism in the analysis, should ensure that evacuation of people in the vicinity would not be necessary in the event of any accident included within the design basis.

Probabilistic safety analysis (P42 to P46)

2 The five accident frequency principles, P42 to P46, for which a PSA is required, have been chosen to address the risks discussed in TOR (individual risk of death to workers and the public, and the societal risk of major accidents) supplemented by consideration of the societal effects of lesser accidents, and also to emphasise defence-in-depth. A guiding aim has been to focus assessment on the design and operation of the plant and to minimise the extent to which judgements on the safety of the plant depend on the numbers of people who live and work in the vicinity of the site. This means that the risks of offsite consequences of accidents are not addressed directly, but rather via surrogate measures related to the plant. It further implies that a full risk analysis of the harmful offsite effects (usually referred to as a 'Level 3 PSA') is not required in order to address these principles.

3 The frequencies to be compared with the BSL/BSOs in the PSA principles are annual averages. Higher frequencies for shorter terms (eg for maintenance) may be acceptable, judged on a case by case basis and subject to ALARP. The frequencies are specified as 'total predicted'. 'Total' refers to all sources. 'Predicted' recognises that there is always some uncertainty in the calculation. This can be considerable for the lower figures sought, with the result that it is not possible to establish absolute values in a scientific sense. However, no allowance for these uncertainties in the predicted frequencies is required, provided that the NII is satisfied that they have been derived on a best estimate or non-optimistic basis and that appropriate sensitivity studies have been performed to identify the important elements in the analysis.

Doses to the public (P42)

4 This principle is based on the generally accepted premise that the larger the potential consequences of an accident, the smaller should be its frequency. The measure chosen to represent the severity of the accident is the effective dose which would be received by a person at, typically, 1 km downwind from the plant (see P36). This provides continuity with past practice for power reactors in the UK and with the design basis analysis, except that the person exposed is considered to be at a more realistic position, in keeping with the best-estimate approach of the PSA. A person at the site fence would, for many accidents, receive a greater dose, but his average occupancy there would generally be quite low. Someone living nearby would be likely to have a fairly high occupancy and be subject to a higher individual risk, averaged over a year.

5 The purpose of P42 is to constrain the risks of the whole range of offsite effects which an accident can lead to. These effects include individual risk of death (prompt and delayed) and of other health effects to local people, contamination of land, disruption of peoples' lives from the application of countermeasures such as evacuation, fear and alarm in the general public, economic loss etc. No attempt has been made to quantify each of these offsite effects, and clearly some of them are not amenable to quantification. Nevertheless, it is considered that the dose as described above, provides a generally adequate surrogate, and the BSL/BSO dose bands can be related in an approximate fashion to the offsite actions which would be expected, namely:

0.1 - 1 mSv	-	additional offsite radiation and contamination surveys;
		possibility of advice being given to restrict the use of foodstuffs produced close to the site;
1 - 10 mSv	-	increased offsite surveys;
		restrictions on the use of foodstuffs likely to be implemented;
		sheltering or issue of stable iodine may be considered in areas very close to the site;
10 - 100 mSv	-	restrictions on foodstuffs likely to be implemented up to several kilometres from the site;

sheltering or issue of stable iodine likely to be implemented;

evacuation may be considered in areas immediately adjacent to the site;

100 - 1000 mSv - restrictions on foodstuffs likely to be extensive;

sheltering or issue of stable iodine likely to be implemented to several kilometres from the site;

evacuation of nearby population likely to be implemented.

6 The frequencies in P42 should preferably be realistic estimates for the specified accidents occurring on the plant. To derive the risk to a person living nearby (paragraph 4 and see P36) we also need to take account of the probability that the person will receive the dose, given that the accident has occurred, allowing for the variability of wind and weather conditions. If these factors were included a plant which just met the BSLs would give a maximum individual risk of death to a person outside the site of about 10^{-5} per year, based on latest estimates of risk factors. This is consistent with the recommendations in the Barnes Report for Hinkley Point C[6]. A similar estimate can be made for a plant which just met the BSO frequencies, giving an individual risk of the order of 10^{-7} per year. Both of these frequencies are less than the values of 10^{-4} and 10^{-6} per year proposed in TOR for the generality of industrial hazards. Taking into account, however, the particular aversion which many people feel for nuclear risks, and the additional risk to the individual from normal operation, they may be said to be broadly consistent with TOR.

Risk to workers (P43)

7 The risk of death to workers on the plant from accidents does not involve consideration of offsite effects, and so a surrogate measure is not needed. The individual risk is used directly. The overall risk to workers is the sum of the contributions from normal operation and from accidents, and it is for this sum that TOR adopts a maximum tolerable value of 10^{-3} per year. For practical purposes, however, the two contributions are addressed separately: in P11 for normal operation and in P43 for accidents. It may be seen from Appendix 1, paragraph 1, that, to maintain consistency with ICRP, the major part of the tolerable level of risk is allocated to normal operation, and hence the BSL for accidents in P43 is set out at 10^{-4} per year. It is recognised that this level may be very demanding for some plants. In such cases, and in particular those in which the risk from normal operation is well below the BSL of P11, it would be acceptable for a trade-off of one against the other to be made in the safety case, where that can be justified.

8 The BSO value is chosen as 10^{-6} per year as being reasonably consistent with the broadly acceptable level of 10^{-6} per year in TOR, bearing in mind that, while the latter includes normal operation, it is directed principally at members of the public.

Large release (P44)

9 For a major accident, the dose to a person close to the plant may be into the range which would cause prompt death, so the particular level of dose is no longer an appropriate measure of its severity. In this situation the number of people affected and the land contamination become dominant concerns. A more appropriate surrogate for these effects, but one which is still related to the design and operation of the plant, is the quantity of radioactive material released in the accident.

10 The quantities and mix of the various harmful isotopes released (the source term) will depend on the particular accident sequence, and their effects will also depend on the weather conditions, the height of the release, etc, so it is not possible to draw a simple relationship between the source term and the effects. Nevertheless, one can specify the quantities of I_{131} (as representative of isotopes responsible for short-term health effects) and Cs_{137} (representing the longer term effects of contamination) which would be typical of a major accident (although certainly not the worst) which could occur in a large modern nuclear reactor. The quantity chosen for I_{131} is 10 000 TBq, this being the amount appearing in the source term from a reactor accident which might cause the eventual deaths from cancer of between one hundred and several hundred people, and possibly more under some weather conditions. The accident discussed in the revised TOR document is of this order of magnitude. The quantity chosen for Cs_{137} is 200 TBq, which is approximately 0.1% of the inventory of Sizewell 'B' and is in line with the trend in international thinking on large releases.

11 There could be major accidents, particularly at nuclear chemical reprocessing plants, where neither I_{131} nor Cs_{137} was representative of the source term. In such cases the 'large release' will need to be determined as one which is roughly equivalent, in terms of short-term health effects or longer term contamination, to the source term specified above.

12 The BSL frequency appropriate to exceeding such a large release is set at 10^{-5} per year. Given the difficulty of relating the source term precisely with the number of deaths, this is reasonably consistent with the

same value adopted for 100 cancer deaths in the Barnes report for Hinkley Point "C". The BSO is set at 10^{-7} per year as being a level which, it is judged, it might be reasonably practicable to achieve for a future design of nuclear plant, although present designs may have difficulty in achieving it and hence would require a demonstration of ALARP in the safety case.

Plant damage (P45)

13 This principle is included to reinforce the objective of defence-in-depth which looks for a series of physical barriers to a release of radioactive material. The safety of the plant should not rely predominantly on the integrity of the final barrier to the release: there should be sufficient reliability in each of the barriers to make a challenge to the final barrier very unlikely. At the international level, a principle has been proposed which refers to a degraded core in a nuclear reactor. It was considered, however, that in the SAPs the principle should be applied to any nuclear plants, including chemical reprocessing plants, which contain a large inventory of radioactive material. In these non-reactor cases it may not be straightforward to identify analogues to a degraded core but it should nevertheless be possible. The 'significant quantity' of radioactive material in P45 is left to be judged on a case-by-case basis, but as a general guideline is one which, if released, would constitute a large release in the sense of P44.

14 The BSL frequency is set at 10^{-4} per year on the basis of a judgement that a higher frequency would be intolerable in terms of the alarm, concern and loss of confidence that would be caused by such an accident, even without a release, and because it would indicate an intolerable weakness in the design of the plant or laxity in the control of its operation. It is also the frequency which is referred to in *Basic Safety Principles for Nuclear Power Plants*[7] as the target for existing nuclear power plants. The BSO frequency of 10^{-5} per year is that given in the same report as the goal for future plants.

Criticality incidents (P46)

15 This principle is included by analogy with P45 to address defence-in-depth for the protection of workers against radiation from accidental criticality incidents, which are an important concern on some non-reactor plants. Such an incident would represent a loss of control and might impose a challenge to the shielding and to the emergency arrangements for personnel protection. The potential consequences, however, are more limited than those of plant damage and so the BSL and BSO frequencies are set a factor of ten higher.

REFERENCES

1 HSE HM Nuclear Installations Inspectorate *Safety Assessment Principles for Nuclear Power Reactors* HMSO 1979 ISBN 0 11 883642 0

2 HSE HM Nuclear Installations Inspectorate *Safety Assessment Principles for Nuclear Chemical Plant* HMSO 1983 ISBN 07176 01536

3 HSE *The Tolerability of Risk from Nuclear Power Stations*
(a) HMSO 1988 ISBN 0 11 883982 9
(b) HMSO 1992 ISBN 0 11 886368 1

4 *The Ionising Radiations Regulations 1985* Statutory Instrument No 1333 HMSO 1985 ISBN 0 11 057333 1

5 ICRP (1991) *1990 Recommendations of the International Commission on Radiological Protection* ICRP Publication 60 Annals of the ICRP **21** (1-3) Pergamon Press, Oxford

6 *The Hinkley Point Public Inquiries* A Report by Michael Barnes QC HMSO 1990 ISBN 0 11 412955 X

7 IAEA *Basic Safety Principles for Nuclear Power Plants* A Report by the International Nuclear Safety Advisory Group Vienna 1988 (Safety series No 75-INSAG-3) 1988 ISBN 9201231881

8 Hinkley Points "C" Public Inquiry: Proof of Evidence of the Director General of the Health and Safety Executive (Annex 6) Rimington J D

9 HSE, Nuclear Installations Inspectorate *Safety Assessment Principles for Nuclear Power Reactors: Amendment Sheet 1* 1988

10 NRPB, Board statement on emergency reference levels, Documents of the NRPB vol 1, No 4 1990

GLOSSARY OF TERMS

Absorbed dose	The fundamental quantity in radiological protection. It is the energy absorbed per unit mass of material.
Accident management	A set of actions taken by plant personnel to control the course of an accident or mitigate its consequences and bring the plant to a safe, controlled state.
Adequate	The necessary and sufficient extent of any measure directed at achieving compliance with these principles.
Alarm	An automatic visual or audible indication to personnel of when a specific plant variable or condition has reached a pre-set limit or state.
Best estimate	When used to describe fault analysis, this refers to an analysis expected to provide the most accurate description of the fault and its consequences that could be achieved within the limitations of the analytical model employed without any deliberate bias being introduced. When used to describe the data used in the fault analysis, it refers to the most accurate value of the data item which can be derived from experiment, operating experience, judgement, etc as appropriate.
Bounding case	The case which represents the extreme, in respect of the condition of interest in a particular study, of a group of discrete cases.
Capability	The description in qualitative and quantitative terms of the complete function(s) provided by a component, sub-system or system, including information on: (a) the operating limits within which the function(s) can be sustained. and (b) the damage limits beyond which permanent degradation of functions must be assumed.
Civil structures	These include all types of masonary, reinforced concrete structures and structural steel work, together with the attachments for plant items and services such as drains and tunnels.
Class of accident	A group of fault sequences which follow paths that are sufficiently similar to justify analysis of the sequences together as a class.
Commissioning	The process by which a nuclear plant is put to work in a systematic manner in order to confirm that its performance meets the design intent, including safety.
Committed effective dose	The effective dose which will be received by an adult in the 50 years following an intake of radioactive material, or for children in the period from intake to age 70.
Common cause failure	Multiple failures of components from the same root cause.
Collective dose	A quantity which takes account of the number of people exposed by multiplying the average dose to the exposed group by the number of individuals in the group.
Conservative estimate	The use of models, data and assumptions which would be expected to lead to a result that bounds the best estimate on the safe side. This is used where reasonable doubt exists regarding the accuracy of models or data.

Containment	In power reactors, the containment is a structure other than a reactor coolant circuit boundary, which is or can be sealed for the purpose of containing radioactive releases under normal and fault conditions, together with the systems provided to maintain the adequacy of the containment function. Other than the power reactor containment defined above containment is usually a series of barriers (eg. gloveboxes, cells, building fabric) each with its own dedicated ventilation system maintaining a depression with respect to the next outside barrier.
Critical crack size	The critical size of a crack like defect in a structure is the predicted size which leads to unstable propagation of the defect under the predicted stress. In practice, appropriate safety factors would be used in this prediction.
Critical group	It is often convenient to class together individuals who form a homogenous group with respect to their exposure to a single source. When such a group is typical of those most highly exposed by that source, it is known as a critical group.
Criticality incident	The accidental occurrence of a self-sustaining fission chain reaction in fissile material which is not in a nuclear reactor core.
Design basis fault (sequence)	A fault (sequence) which the plant is designed to take or can be shown to withstand without unacceptable consequence, by virtue of the plant's inherent characteristics or the safety systems.
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	A general term for a measure of exposure to ionising radiation. If unqualified, it should be taken to mean the sum of the effective dose from external radiation and the committed effective dose from intakes of radionuclides.
Equivalent dose	The absorbed dose averaged over a tissue or organ and weighted by a factor depending on the type and energy of the radiation.
Effective dose	A quantity derived from equivalent dose to represent the combination of doses to different tissues in a way which is likely to correlate well with the total of the stochastic effects. It is the sum of the weighted equivalent doses in all tissues and organs of the body, where the weighting represents the relative contribution of the organ or tissue to the total detriment due to the stochastic effects resulting from uniform whole body irradiation.
Equipment qualification	A formal process to demonstrate that the equipment will meet the system performance requirements in normal operation and specified accident conditions.
Failure	A failure has occurred when an item (or items) of equipment ceases to function in the correct manner, does not function when called upon to do so or functions spuriously.
Failure modes	The ways in which a failure of an item of equipment can occur. For example, the failure modes of a relay include: contacts stuck open or closed, coil open circuit, low or high coil resistance.
Fault	Any unplanned departure from the specified mode of operation of a system or component due to a malfunction or defect within the system or component or due to external influences or personnel error.

Fault condition	When used without qualification, this means all design basis fault conditions and, where appropriate and as far as reasonably practicable, beyond design basis conditions also.
Fault sequence	A combination of events starting from an initiating fault and including any additional failures which may occur.
Hazard	An internal or external event with the potential to cause equipment damage or failure in the plant.
Individual risk	The risk to any individual of premature death from cancer or other radiation effects as a result of exposure to ionising radiation during any one year, whether the death occurs during the year of exposure or subsequently.
Initiating fault	The starting fault of a fault sequence. It may be a direct plant fault or a fault caused by an internal or external hazard or by human action.
Ionising radiations	Gamma rays, X-rays or corpuscular radiations which are capable of producing ions either directly or indirectly.
Normal operation	All activities performed to achieve the purpose for which the plant was constructed, including maintenance, inspection and other associated activities as well as starting up, running and shutting down the plant. Minor incidents arising from these activities which might give rise to operational problems or small unplanned doses to operators are also regarded as part of normal operation.
Nuclear matter	(a) Any fissile material in the form of uranium metal, alloy or chemical compound (including natural uranium), or of plutonium metal, alloy or chemical compound. (b) A substance possessing radioactivity which is wholly or partly attributable to nuclear fission or other processes of subjecting a substance to bombardment by neutrons or to ionising radiations. (c) Any substance which meets the definition of radioactive waste in the Radioactive Substances Act. (See also Secondary Waste)
Operating modes	All the states that the plant may be in during the course of normal operation (qv).
Physical barrier	Features of a plant which prevent or limit the release of radioactive material to the environment under normal and fault conditions. For a reactor, the physical barriers are typically the fuel matrix, the fuel cladding, the primary coolant circuit boundary and the containment building.
Plant	A plant is that part of a nuclear site identified as being a separate unit for the purposes of assessment. This may be a single reactor or a group of processing facilities as on a nuclear chemical site.
Pressure system	A system comprising one or more pressure vessels, any associated pipework and valves and protective devices such as bursting discs, pressure relief valves or pressure gauges.
Process flowsheet	A diagram or document setting out the sequence of relevant process steps, unit operations and basic engineering concepts, chemical and physical interactions, flowrates and concentrations of relevant reagents.

Protection system	The instrumentation within a safety system which measures (or monitors) plant parameters (or states) and generates safety actuation signals when these parameters (or states) move beyond pre-set limits.
Radioactive scrap	Obsolete, damaged or redundant material contaminated with nuclear matter, which may have recovery value and has not yet been consigned as radioactive waste.
Redundancy	Provision of alternative (identical or diverse) elements or systems, so that anyone can perform the required function regardless of the state of operation or failure of any other.
Reliability	The probability that a component, sub-system or system will perform in the manner required over the time period of interest and in the environment and operating conditions specified.
Risk	The likelihood of a specified undesired event occurring within a specified period (usually a year) or in specified circumstances.
Safety actuation system	The equipment within a safety system which physically accomplishes the required safety action(s) in response to actuation signal(s) from the protection system.
Safety culture	An organisational environment which at all levels emphasises safety and uses a variety of managerial, supervisory and individual practices and constraints to sustain attention to safety, through an awareness of the risks posed by the plant and of the potential consequences of incorrect actions.
Safety-related system	A plant system, other than a safety system, on which radiological safety may depend.
Safety system	A system which acts in response to a fault to prevent or mitigate a radiological consequence.
Safety system schedule	A schedule which identifies the minimum safety system requirements for each of the initiating faults and internal and external hazards listed in the fault schedule.
Safety system support features	That equipment which provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems.
Secondary waste	Waste that results from applying treatment, handling or storage technology to a waste or product stream of a process.
Segregation	The physical separation of components, systems, circuits, etc, to reduce the probability of common cause failures.
Severe accident	A fault sequence which leads either to a significant release of radioactive material to the environment or to a substantial unintended relocation of radioactive material within the plant. (Accidents of Level 5 and above on the International Nuclear Event Scale come into this category.)
Shielding	A structure or material placed around a source of radiation to reduce the radiation dose rate in the vicinity.
Sievert	The unit of equivalent dose and its derivatives, eg effective dose and committed effective dose.

Societal risk	A general term covering the likelihood of undesired events which affect society as a whole, such as specified numbers of deaths or injuries, numbers of people evacuated, land contamination, economic losses and general social disruption. The particular events must be specified for the term to acquire a specific meaning and to be quantified.
Task analysis	Systematic delineation and examination of the psychological and physical demands placed upon a human operator by specified task requirements. The output of a task analysis is essentially a human 'performance specification' for assessing interface design, procedures, training provisions, team organisation, workload, communications systems, etc.
Validation	The testing and evaluation of the whole system at the completion of its development to ensure compliance with the requirements specification. In fault analysis, to confirm that the analysis is correct by comparison of models with experiments or other available data.
Verification	Computer Software. The process of ensuring that the product of a phase in the *software development cycle* meets the requirements placed on it by the previous phase. QA. The act of reviewing, inspecting, testing, checking, auditing or otherwise *determining* and *documenting* whether or not items, processes, services or documents conform to specified requirements.
Veto	Inhibition of a safety system.
Whole body dose	The sum of the effective dose from external radiation and the committed effective dose from intakes of radioactive material.

ABBREVIATIONS

ALARP	As low as reasonably practicable
Bq	Becquerel. Unit of activity of a quantity of radioactive material. 1 Bq is equal to 1 disintegration per second
BSL	Basic safety limit
BSO	Basic safety objective
CID	Criticality incident detection
DBA	Design basis accident
DBE	Design basis earthquake
ERL	Emergency reference level (as recommended by the National Radiological Protection Board)
G	Giga or thousand million
PSA	Probabilistic safety analysis
QA	Quality assurance
SAP	Safety assessment principle(s)
SRI	Safety related instrumentation
Sv	Sievert(s)
T	Tera or million million
TOR	Tolerability of risk (from nuclear power stations)

Printed and published by the Health and Safety Executive
C2.5 11/98

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 6FS
Tel: 01787 881165
Fax: 01787 313995

RETAIL
HSE priced publications
are available from
good booksellers

HEALTH AND SAFETY ENQUIRIES
HSE InfoLine
Tel: 0541 545500
or write to:
HSE Information Centre
Broad Lane
Sheffield S3 7HQ

HSE home page on the World Wide Web:
http://www.open.gov.uk/hse/hsehome.htm

£10.00 net

ISBN 0-11-882043-5