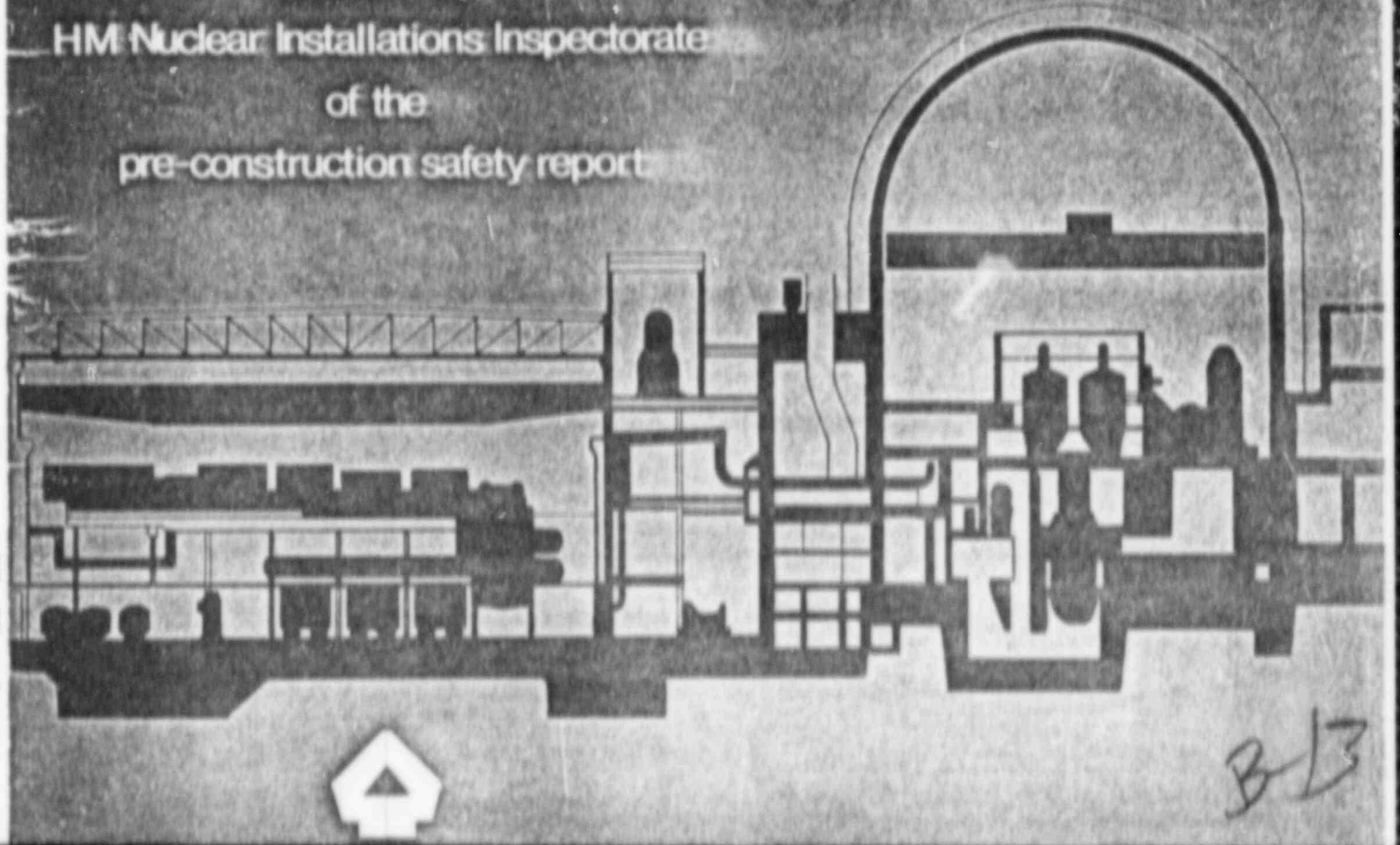
Sizewell B

a review by
HM Nuclear Installations Inspectorate
of the
pre-construction safety report



B-13

Health and Safety Executive

Sizewell B

A review by HM Nuclear Installations Inspectorate of the pre-construction safety report

London: Her Majesty's Stationery Office

First published 1982

Any enquiries regarding this publication should be addressed to the Health and Safety Executive at any Area Office or to the public enquiry point, Baynards House, 1 Chepstow Place, London W2 4TF, Tel 01 – 229 3456.

NII/8/37/82

ISBN 0 11 883652 8

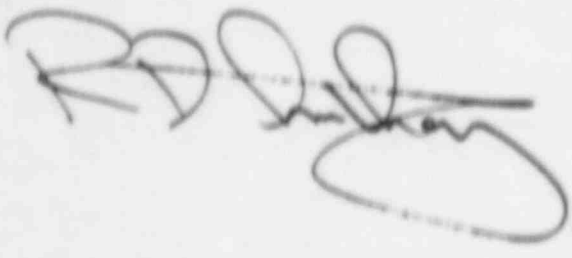
Foreword

Under the relevant legislation the Health and Safety Executive has the responsibility for deciding whether to issue a licence for the construction and operation of a nuclear power station. The Nuclear Installations Inspectorate of the Executive has been conducting an assessment of the Central Electricity Generating Board's pre-construction safety report for the proposed pressurised water reactor at Sizewell, with particular emphasis on those issues which need to be settled before the existing nuclear site licence can be varied to include the new station and consent given to start construction. The assessment is part of a continuing process which includes the generic review of 1974–78 and which, if the project was to be proceeded with, would continue through design, construction and operation of the station. This report presents a summary of the position reached in our work by April 1982. It has been prepared primarily to be of assistance to the public inquiry into the Sizewell B proposal.

In deciding whether to recommend the issue of a licence for a nuclear installation the Inspectorate's aim is to be satisfied that the installation's siting, design, construction and operation will meet the health and safety standards which we have set. These standards are stringent both for the protection of persons on the plant and for those outside who may be affected by an incident on the site. We are not concerned with the need for additional electricity generating capacity or how this is to be provided.

Following the generic review we concluded that, based on the information provided, there was no fundamental reason for regarding safety as an obstacle to the selection of a pressurised water reactor for commercial electricity generation in the United Kingdom. Though assessment of the specific design for Sizewell B as set out in the pre-construction safety report is at an early stage, the work which has been done so far and is reported here confirms the earlier conclusion. This means that no difficulty has so far been identified which needs be regarded as insuperable. However, there are a number of safety issues remaining where more work needs to be done or more information needs to be provided to satisfy the Inspectorate that an acceptable design and safety case has been put forward and licensing and construction can be allowed to proceed. These issues are discussed in the text of the review and the main ones are brought together and summarised in the conclusions. They consist mainly of a number of matters on which we require further information and analysis but where we believe that this will show that the necessary standards can be achieved. There are also matters for which we believe some modification to the original proposed design intent may be needed before we can be satisfied and, finally, there are a few issues where the most appropriate solution has yet to be found.

The Inspectorate's general conclusion is that a satisfactory design is achievable and can be developed so as to meet the safety objectives. Only when this has been achieved, and our concerns have been met, will our recommendation be made with regard to licensing. This conclusion has been endorsed by the Executive.



R D ANTHONY
HM Chief Inspector of Nuclear Installations

Contents

1 Introduction

1.1 In the United Kingdom, if a generating board wishes to install and operate a power station it must first obtain planning consent from the appropriate Minister under the Electric Lighting Act of 1909. If the proposed station is to be a nuclear power station the board must then obtain a licence from the Health and Safety Executive (HSE) under the Health and Safety at Work etc. Act 1974 and the associated relevant statutory provisions of the Nuclear Installations Act 1965. HM Nuclear Installations Inspectorate (NII) is that part of the HSE which carries out its nuclear site licensing and regulatory function under the relevant Acts.

1.2 Following the Government's agreement in December 1979 (ref. 1) to allow the Central Electricity Generating Board (CEGB) to proceed with a pressurised water reactor (PWR) as the next nuclear power station order, the CEGB opened discussions with the Inspectorate with a view to providing a design and safety case and starting on the necessary processes which it hoped would eventually lead to licensing and consent to start construction. In addition, the Government announced that an inquiry would be held before planning consent under Section 2 of the Electric Lighting Act of 1909 could be granted.

1.3 In January 1981 the CEGB wrote to the Secretary of State for Energy requesting consent under Section 2 of the Act for construction of an additional generating station utilising a 1200 MWe pressurised water reactor to be known as Sizewell B. It also wrote to the Health and Safety Executive requesting an appropriate revision to the existing nuclear licence for their Sizewell site to cover this further nuclear installation. Since the proposed station is to be on an existing licensed site a new licence is not required but licensing of the PWR station will involve a variation to the existing licence once it has been through the licensing process which includes the provision of a satisfactory safety case.

1.4 The Inspectorate's requirements before licensing a new PWR power station could be considered included receipt of the following information:

(a) the safety principles and criteria to be used in the design;

(b) a statement of the design in outline (the reference design), to be supplemented later by more detailed information;

(c) a preliminary safety report (PSR) outlining the principles and the basis on which the safety case is to be made, together with information showing how the reference design meets the safety criteria. It provides a preliminary safety analysis of the critical fault conditions and preliminary assessment of the proposed protection equipment;

(d) statements of the proposed research and development work in support of the safety case;

(e) proposals for quality assurance;

(f) details of the contract design, i.e. the design intended for construction; and

(g) a pre-construction safety report (PCSR) containing a more comprehensive statement than the PSR of the safety case and design description including more detailed safety analysis and assessment of the performance and standard of the proposed protection equipment.

It was expected that the information would be provided chronologically in approximately the order shown and that the process of review and assessment by the Inspectorate would cover a period of about two years, taking into account the work already carried out in the earlier generic review (ref. 2).

1.5 In this report are described briefly the history of the project, the safety issues identified at various stages and the principles and criteria used as a basis for judgement. However the main purpose is to summarise and review the present position of the Inspectorate's assessment of the safety case for Sizewell B following receipt of the CEGB's Reference Design Report (ref. 3) in September 1981, receipt of an advanced draft of the PCSR (ref. 4) towards the end of December 1981 and discussion with the CEGB leading up to publication of the final drafts of the PCSR (ref. 5) and Reference Design Report (ref. 6) in May 1982. The report has been written at this early stage so that the views of the Inspectorate on the safety aspects of the Sizewell B proposals may be made public in good time before the start of the public inquiry. Hence, while the review covers all those aspects of the design which might affect safety, in the time available since receipt of the PCSR the assessment work has had to be concentrated mainly on those matters of safety principle or of design intent which would be likely to have a significant effect on the main features of plant provision or layout. It represents the stage that was reached at the end of March 1982, though of course assessment of the safety of the proposed design, discussions with the CEGB and modifications to the proposed design or safety case, where considered to be necessary, have continued from that time and will continue until the Inspectorate is satisfied with the case made.

1.6 The report is not a general review of the safety of the proposed PWR station. Rather it has been the aim to discuss any shortcomings of the safety case presented in the PCSR and to present the Inspectorate's views on the position with regard to the safety issues and the progress being made in dealing with them at this stage in the licensing process. It should be

read with the PCSR and the sequence of the sections of the report follows closely that of the topics covered by the chapters of the PCSR. In the interest of brevity, the descriptive material in the text is kept to a minimum since it is to be found in the PCSR and the associated Reference Design Report.

1.7 From the conclusions of the report it is clear that there is no reason for a change of the view, following the generic review, that there is no fundamental reason for regarding safety as an obstacle to the use of a PWR for a commercial nuclear power station. However, before the specific design for Sizewell B can be accepted for licensing there are a number of safety issues still to be resolved. These are discussed in the various chapters of the report and brought together for convenience in Section 19. An indication of the further work that will be necessary and the further information to be provided before the Inspectorate can be satisfied is also given.

2 History of the project

Generic review

2.1 Following a proposal by the CEGB in 1973 to adopt a PWR, later confirmed as a Westinghouse design, for the next stage of its nuclear power programme the Inspectorate increased the resources allocated to light water reactors and embarked upon a generic review of PWR safety in preparation for a formal safety review leading to a decision on licensing.

2.2 For the purpose of the review, an account of which was published in 1979 (ref. 2), the generic aspects of the PWR were taken to be those safety issues which could be regarded as specific to and inherent in the concept and those features which, while common to other reactor systems, had novel significance in the PWR. The generic issues selected for detailed consideration were:

(a) potential plant faults and their analysis;

(b) loss-of-coolant accidents;

(c) primary coolant circuit integrity including the reactor pressure vessel, primary loop pipework and steam generators;

(d) fuel element behaviour;

(e) reactor protection system;

(f) containment;

(g) radiological risk in normal operation;

(h) radioactive waste arising on the reactor site.

2.3 The objective of the generic study was to arrive at a view on the safety of the PWR concept and in particular to determine the technical conditions which would need to be satisfied for a PWR to be accepted as a commercial nuclear power plant in the United Kingdom. Whilst a particular plant, the Westinghouse 4-loop, 1150 MWe plant at Trojan, Oregon, USA, was selected as a reference design, because the CEGB identified it as the nearest complete plant to its requirements for which a full safety report was available, the review was not specific to this plant. Indeed, to supplement this study the Kraftwerk Union PWR of similar size was also considered and discussions held with this design company. Discussions were also held with regulatory bodies in France, Germany and the USA and use was made of information provided in studies such as the Rasmussen Report (ref. 7) and the UKAEA's investigation into pressure vessel integrity carried out under the chairmanship of Dr Walter Marshall (ref. 8).

2.4 A summary document setting out the scope and main conclusions of this study was presented to the Secretary of State for Energy in July 1977 (ref. 9). This was followed by a more extensive report giving the main conclusions and essential supporting technical arguments which was published early in 1979 (ref. 2). The main conclusion of this generic review was that there was no fundamental reason for regarding safety as an obstacle to the selection of a PWR for commercial electricity generation in the UK. However, a number of safety questions were not settled to the Inspectorate's satisfaction, because more information was required or the design or state of the art needed improvement, and a number of detailed recommendations were recorded where an increase in confidence was desirable or where reasonably practicable improvements appeared possible.

Pre-licensing review

2.5 The Secretary of State for Energy announced in a statement in Parliament in January 1978 (ref. 10) that the CEGB and the SSEB would be authorised to begin work at once with a view to ordering one advanced gas-cooled reactor (AGR) station each. In addition he said the Government endorsed the CEGB's wish to establish the PWR as a valid option which should be developed in the early 1980s, subject to the necessary consents and safety clearances being obtained. In December 1979 the present Government again endorsed this intention. In June of 1980 the Inspectorate presented to the CEGB its requirements for a programme of safety submissions leading to licensing. The programme was similar to that which had been agreed for the new AGRs but with increased emphasis on design description and fault analysis for what would be the first commercial PWR station in this country. It was subsequently agreed that the main elements of the programme would provide:

(a) a Westinghouse SNUPPS (Standardised Nuclear Unit Power Plant) FSAR (Final Safety Analysis Report) and a commentary on it to be submitted in mid-July 1980;

(b) a preliminary safety report (PSR) submission for the proposed UK design to be submitted at the end of September 1980;

(c) the major part of the safety case and a full set of representative fault studies to be submitted with the draft pre-construction safety report (PCSR) in mid-February 1981; and

(d) completion of the PCSR in draft form by mid-November 1981 and publication of the final draft in mid-February 1982.

The Inspectorate would start to prepare the draft report in mid-February 1982 for publication in May of that year.

2.6 It was accepted by the Inspectorate that whilst this programme did not give quite the two years it was expected such a review might take, given that the information provided was satisfactory the Inspectorate should be able to indicate its views on the acceptability of this specific design for licensing by the time of its report, and hence in time for a public inquiry in the second half of 1982.

2.7 In the event, whilst the SNUPPS FSAR and the PSR were submitted on time, they proved to be disappointing in that they advanced the Inspectorate's knowledge following the generic review to only a limited extent. More importantly, a series of design reviews took place within the industry which led to a number of changes to the design during the latter part of 1980 and the first half of 1981. The position with regard to the proposed design and its safety case remained uncertain, with little firm information coming forward, until the setting up of a joint industry task force under the chairmanship of Dr Walter Marshall in July 1981. This task force was established to ensure that firm design proposals for the Sizewell B PWR, consistent with UK safety requirements, would be developed as quickly as possible so that a satisfactory safety case could be prepared for submission to the Inspectorate by the CEGB.

2.8 The Inspectorate agreed to liaise with the task force through its Safety Liaison Group and meetings were held to prepare a revised programme of safety submissions and new publishing dates for an inquiry to be held early in 1983. A revised reference design report was to be presented in September 1981 and the first issue of the PCSR in draft form just before Christmas. This would be followed by a short period of assessment by the Inspectorate and discussions with the CEGB but this would have to be completed by the end of March so that the PCSR could be published by May 1982. The Inspectorate's review was to be published by July 1982.

2.9 Though the Inspectorate had already received a certain amount of technical information in support of the CEGB's safety case, and would receive advanced information in the form of draft chapters and supporting documents of the PCSR the revised programme meant that the assessment work would be by no means complete by the time the Inspectorate's own review came to be written. However, it was anticipated that it would be possible to comment on the more important issues of significance to safety, to indicate where there were reservations and to give a view on what still required to be done.

Main topics identified as requiring further information

2.10 Consideration of the status of the Inspectorate's assessment of the design safety case, and of information available from the CEGB and the task force regarding the proposed new reference design and safety case, led to the following views on the main safety issues, as the NII saw them, being put to the CEGB in September 1981:

(a) Whilst accepting the CEGB's safety criteria as a suitable basis for a safe design, the Inspectorate needed to be satisfied that all that it was reasonably practicable to do had been done in areas where there had been changes to the reference design;

(b) A comprehensive definition was required of the external hazard levels to which the station would be designed. Agreement was needed on the criteria to be adopted for the design of the plant against hazards including plant layout and means of segregation.

(c) The Inspectorate was concerned that sufficient attention should be paid in the design and safety case to the effect of human error and the role of the operator;

(d) There appeared to be significant deficiencies in the approach to fuel behaviour in both normal and fault conditions. In particular, on the evidence available, a satisfactory case had not been made on the clad ballooning issue;

(e) There were a number of uncertainties about the design of the containment, for example its ability to withstand steam line break accidents with consequential steam generator tube failures. Also the criteria for protection against external hazards had not yet been set out. Containment performance in degraded core situations was a further area of uncertainty;

(f) Whilst the Inspectorate had been assured that the reactor pressure vessel would be fabricated from ring-forgings and that steps would be taken to ensure satisfactory material composition and properties, there was nevertheless still concern about the likelihood of failure of the vessel as a result of certain fault transients. Also the CEGB's proposals for inspection of the vessel during fabrication as well as in service were not sufficiently formulated;

(g) There were questions outstanding about the analytical approach to be used to justify the integrity of the reactor internals during and following a loss-of-coolant accident (LOCA);

(h) The Inspectorate wished to see more attention given to steam generator issues, for example the level of in-service inspection of the shell and the assurance of tube integrity;

(i) The proposed use of the Westinghouse Integrated Protection System (IPS) was a novel feature and would require detailed examination. In addition, a secondary, diverse guardline system would have to be provided to overcome common mode failure problems and provide a sufficient level of protection against frequent faults;

(j) There were a number of outstanding questions regarding lack of redundancy or diversity in other parts of the protection system such as the refuelling water storage system and the component cooling water system;

(k) It was not possible to judge whether or not a case could be made for faults involving failure of the shut down system (ATWT) without the provision of an emergency boration system;

(l) In the case of radiological protection and waste management, the main concern was that appropriate provisions should be made to minimise build up of radioactivity in the primary circuit and to reduce doses to personnel especially during maintenance and refuelling, as far as was reasonably practicable;

(m) The fault studies and fault and event tree analyses of a number of intact circuit (other than ATWT) faults, such as vessel overcooling accidents, steam generator tube failures, steam line break and main steam isolation valve failure, were not sufficiently developed;

(n) The capability of the emergency core cooling system (ECCS) to deal with breaches of a certain size occurring below the core level was questioned, as was the validation of the computer codes used in the safety case for loss-of-coolant accidents;

(o) The study of the effects of faults leading to major core damage was at an early stage and subject to a number of uncertainties in arriving at the related source terms and their probabilities;

2.11 In addition, a number of more detailed safety issues were identified as requiring attention. These included items from the generic review, from the US Nuclear Regulatory Commission's (USNRC) unresolved safety issues (ref. 11) and from the Inspectorate's work on the specific design proposals and safety case received up to that time.

2.12 Finally the Inspectorate wished to be satisfied about the management structure of the industry, in particular that of the CEGB, so as to be able to identify the lines of responsibility for safety in design and subsequent operation, for advisory work and policy decisions at HQ and elsewhere and for internal auditing, for example by the CEGB's Health and Safety Department, of these responsibilities. The CEGB's policy and arrangements for quality assurance would form a part of this review.

2.13 The CEGB responded to these points by agreeing to deal with them in the PCSR or its supporting documentation, unless it could show that they were not significant in terms of the design and plant layout and could be left until a later date, or alternatively that they could be answered satisfactorily by technical discussion or by correspondence.

Objectives of the review

2.14 The review reported here should be seen in the context of the overall safety assessment of a nuclear power station carried out by the Inspectorate. As has been described, this assessment starts with an appraisal of preliminary information about the likely design of the plant and generic information about similar plants. There follows the present more formal stage which involves examination of the safety report and supporting documents relating to the specific proposal for licensing. Assuming that a licence is granted, this examination continues throughout the detailed design and construction stages and the Inspectorate needs to be satisfied at each stage before consents required by the licence conditions are given to proceed further, including consents to load fuel into the reactor and to the various stages of commissioning. Details of operating and maintenance procedures are also examined during this period, prior to a decision on whether consent should be given to full commercial operation of the plant. Finally there is review throughout the life of the plant of operating and maintenance procedures and of any plant modifications. Thus assessment is a continuous process from design inception, through detailed design, construction, commissioning, operation and, ultimately, decommissioning.

2.15 The Inspectorate's objectives at this stage of the pre-licensing process involve the following:

(a) confirmation that the CEGB's intentions are consistent with NII's safety assessment principles (ref. 12);

(b) identification and resolution of those safety issues which are of importance; and

(c) acceptance that the design intent and safety principles proposed, and the detailed design of plant which is of special concern to safety, will result in a plant which would be acceptable in all the important aspects so far as safety is concerned.

By 'important' is meant major matters of safety principle or matters which are likely to have a significant effect on the main features of plant design or layout.

2.16 In addition the Inspectorate needs to be satisfied that the main questions arising from its generic review and from subsequent assessment have been answered or are capable of being answered at the appropriate time.

2.17 The process starts with a period of review of the PCSR and its supporting documentation, questions are asked and technical discussions follow with the licence applicant, in this case the CEGB, and with its main contractors for the design including the National Nuclear Corporation (NNC), British Nuclear Fuels Limited (BNFL), Westinghouse and Bechtel, as appropriate. This would be expected to result in further information being provided either in support of the safety case or in clarification of it, and design changes may be made to meet the Inspectorate's concerns. Finally, when a decision is made on licensing, the Inspectorate should be in a position to accept the design as meeting the required standard of safety such that there is small chance of significant modifications subsequently being required for safety reasons.

2.18 It will be seen that the present review is written at a comparatively early stage of the process, the Inspectorate's normal assessment work and interaction with the licence applicant having been suspended for the time being in order to prepare the review and publish it for the public inquiry. Hence, as would be expected, there are reservations and concerns in many areas. These will require more information to be provided and more assessment work to be done before they can be resolved and the objectives of the pre-licensing process achieved.

3 Safety criteria

General

3.1 The PWR is a reactor system which has been licensed in many countries against requirements largely based upon those drawn up in the USA. However, the proposed Sizewell B plant, like other nuclear installations in the UK, must satisfy the Inspectorate that it meets the required standards to obtain a licence in this country. In carrying out its review of the safety case for the proposed plant, the preliminary conclusions of which are reported here, the Inspectorate uses a set of safety assessment principles (ref. 12) which provide a framework and guidance against which judgements on acceptability are made. The Health and Safety at Work etc. Act requires that the risk to plant staff and other persons (including the general public) should be as low as is reasonably practicable and that the best practicable means should be used against the release of noxious substances. The Inspectorate's principles embody these requirements so far as nuclear safety is concerned, conventional hazards being excluded except where they affect nuclear safety.

3.2 The safety assessment principles were drawn up in the light of experience gained in licensing nuclear reactors in the UK, but they were made sufficiently general to be applicable to any proposed reactor system. They comprise a set of objectives which should be met as far as reasonably practicable, but in some cases there is what amounts to a definite requirement that they be met, for example the need to be able to shut down the reactor and maintain it safely shut down, and the principle that dose equivalent limits should not be exceeded.

3.3 A number of the principles are expressed in quantitative terms. These 'assessment levels' are intended to give guidance to the assessor of the level to aim for. Satisfaction of these assessment levels should, in general, be sufficient for acceptability but, if reasonably practicable, it would be expected that suitable provisions be made to make the plant safer. On the other hand, it may not be reasonably practicable to satisfy an assessment level. This might, nevertheless, be deemed acceptable, provided that a suitably strong case is made.

3.4 Neither the assessment levels nor the principles themselves are mandatory and it is not intended that they should be imposed upon the designers, since this would remove the flexibility which they must have to design the plant. American criteria, or criteria from other countries, may be used as the design basis, provided that adequate justification for their choice together with appropriate supporting information is given, and in some parts of the PCSR this has been done. The overriding requirement is that the designers satisfy the twofold duty placed upon them of ensuring that the plant is within the required limits and is then as safe as is reasonably practicable.

3.5 The CEGB has its own safety criteria and guidelines (refs. 13, 14) which have been the subject of discussion with the Inspectorate over the period since their inception. While in a number of respects the CEGB's requirements differ from the NII's principles, if only because they are aimed at designers rather than assessors, it is accepted that their correct application should lead to a nuclear plant design which is likely to prove acceptable to the Inspectorate. A final judgement on this can only be made, however, on the basis of the design and safety case put forward for the specific plant.

3.6 The Inspectorate does not set out to review all parts of the safety case in depth. Different aspects are examined at different levels of detail, the purpose being to ensure that the CEGB and its contractors perform the duty placed upon them, rather than to check that the safety case and the data and the calculations on which it is based, are entirely free from error. Nor does the Inspectorate aim specifically to check that the design satisfies the CEGB's own safety criteria. The Inspectorate may, however, come across instances where it appears not to do so. In such cases the Inspectorate asks for justification of the apparent shortcomings. There can be instances where a plant design is submitted which is lacking safety provisions provided on earlier plants, in apparent violation of the 'as safe as reasonably practicable' requirement. There may be sound reasons for this, because of the differences between plants, but the CEGB would be asked to justify such cases.

NII safety assessment principles

3.7 The Inspectorate's safety assessment principles are divided into three categories. The first category comprises a set of fundamental requirements which include the radiological protection limitations on dose and the 'as safe as reasonably practicable' requirement to be applied to the assessment of radiological consequences. The second category comprises basic principles which develop the fundamental requirements and are concerned with the limitation of radiological consequences for normal operation and for fault conditions. The third category is mainly concerned with engineering features.

3.8 The procedure applied in the evaluation of potential faults and the protective provisions for controlling them is described in the basic principles. The

aim is that all potential fault sequences should be subject to analysis in the safety case, though it is recognised that methods of selecting bounding cases may need to be applied to reduce the effort involved. Faults beyond the design basis need to be studied to enable their contribution to the overall risk of the plant to be assessed and, together with sensitivity studies, to give assurance that no situations exist where a sudden change in consequence occurs which might not otherwise be considered. (Steps should be taken to avoid such situations where reasonably practicable.)

3.9 In assessing the fault sequences the Inspectorate looks for 'effective barriers' against the potential outcome of each sequence. For the less serious sequences the plant is required to be protected by at least one effective barrier. For more serious sequences better protection is required. Moreover, there are limits imposed by the possibility of common mode failure to the reliability achievable by a barrier; simply increasing the degree of redundancy provided is judged to be insufficient to achieve the higher standard. The principles require, therefore, the provision, where reasonably practicable, of two or more independent and diverse effective barriers against the less infrequent of the more serious faults, the expectation being that the common mode failure problem will be overcome by the provision of barriers relying on different parameters for initiation, different principles of operation, etc. Further discussion on barriers is given in Section 16.

3.10 In any safety case, claims are likely to be made that certain events are of such low probability of occurrence as to be 'incredible'. Where the events are clearly recognised as being sufficiently remote, such claims would be accepted. However, the claims frequently relate to the integrity of major components for which the demonstration of effective barriers is not practicable. In these cases a special procedure is followed in which all the relevant scientific and technical factors are taken into consideration by the Inspectorate in making a judgement on the issue.

3.11 While fault analysis and barrier assessments are important aspects of the Inspectorate's review process, the systems provided on the plant are only as good as the engineering which goes into them. The major part of the NII's principles document is devoted, therefore, to engineering principles and the practical application of the more basic requirements discussed above. General engineering principles are presented followed by principles specific to the different parts of the plant. Aspects such as basic plant characteristics, design, testing, inspection and maintenance, and quality assurance are all considered.

3.12 It is important for engineering assessments to be based on a good understanding of the plant, on the loads to which it will be subjected during its life, and on the ways in which it might be affected by plant operation and maloperation. Much of the equipment will be required to operate in fault conditions and it must be shown to be reliable and effective in such situations. Plant not involved in that way must be shown to be proof against the conditions which might arise, at least to the extent that further failures do not occur and add to the severity of the problem. In some situations, relevant reliability data may not be available, and assessments on the effectiveness of plant and parts of barriers will need to be on the basis of engineering judgement. The principles give the bases on which those judgements should be made.

4 Topics of general application

Introduction

4.1 In many components, systems and structures throughout the station there are aspects in common; in this section those topics which are of such general application are reviewed in order to avoid needless repetition. The majority of these topics are discussed in Chapter 3 of the PCSR.

Design criteria for components, systems and structures

General

4.2 As a basis for acceptable safety performance, the Inspectorate needs to be satisfied that plant and equipment serving a safety-related function are capable of operating throughout the range of regimes which they may be expected to experience, that is, to demonstrate the effectiveness of the 'barriers'. One way of dealing systematically with such matters is to establish appropriate criteria for the design, manufacture, inspection and testing of components, systems and structures (usually abbreviated to 'design criteria'). The CEGB's basic intent in this area is generally acceptable but there remain several issues to be resolved. These are discussed below.

Safety classification of components, systems and structures

4.3 The basis of the safety classification adopted in the PCSR is that of ANSI:N18.2 (ref.15). The safety classification given to a component determines, *inter alia*, the standards to which the component is designed, manufactured, inspected and tested, as well as determining the quality level assigned in the quality assurance system.

4.4 The Inspectorate has expressed reservations as to its acceptance of the ANSI:N18.2 approach since this relies only on a consideration of the consequences of failure of the component being classified. In the Inspectorate's view, the safety classification should be based on more comprehensive analysis of the role of the component in mitigating the consequences of other faults and the extent to which those consequences may be worsened by non-availability or non-operability of the component.

Codes and standards

4.5 The Inspectorate has noted a tendency for the CEGB to propose the ASME Boiler and Pressure Vessel Code as the basis for the safety case whilst indicating a clear intention to deviate from that code in a number of areas. The Inspectorate has indicated that it would expect compliance with the ASME Code, and especially with its N-stamp and approvals procedures, as a minimum. The Inspectorate would wish to review additional requirements (beyond those imposed by the code) on a case-by-case basis and would not contemplate any blanket authorisation for deviations.

Protection against the dynamic effects of pipe rupture

4.6 During the generic review, shortcomings were identified in the system of scheduling adopted by Westinghouse for the components, systems and structures which needed to be preserved in the event of a postulated pipe rupture. Consequently the Inspectorate sought a commitment from the CEGB that it would undertake detailed and comprehensive scheduling. This has not been given and therefore the Inspectorate is not in a position to judge the adequacy of the CEGB's provisions in this respect. A commitment to undertake detailed scheduling, or some suitable alternative, should be provided prior to a decision on licensing.

Plant-generated missiles

4.7 The Inspectorate wishes to see a more comprehensive treatment of plant-generated missiles than is given in the PCSR. For example, in terms of the definition of pressure components which may give rise to missiles, the physical separation assumed to be effective and the consideration of secondary missiles that might be released by jet impingement, e.g. on instrument racks or removable flooring.

4.8 In terms of missiles which might be released from failure of turbo-generators, the Inspectorate wishes to be assured that an 'effective barrier' capable of controlling fission product release exists under impact from high trajectory ('lob-shot') missiles.

Valve and pump operability

4.9 In the past, licensing in the USA has depended on the assurance of redundancy provided in response to the 'single active failure' criterion of 10 CFR 50 Appendix A (ref. 16). The Inspectorate does not accept this as sufficient because reliability should also be considered, especially during and after accident conditions, as the Three Mile Island incident (ref. 17) showed. For example, fluid forces or excitation from external hazards may so distort a valve or a pump that its operating clearances could be lost and the valve fail to close or the pump seize. The position of the CEGB as set out in the PCSR is not yet acceptable to the Inspectorate since the intention appears to be to provide a lesser demonstration of operability than is currently offered as good practice by US manufacturers.

Design against external hazards

General

4.10 The appropriateness of the design input or 'forcing functions' for external hazards is discussed in Section 5, since this is a site-related topic. Here the Inspectorate deals mainly with earthquake design criteria since earthquakes are likely to be the most limiting of the external hazards identified in the design bases discussed in Chapter 3 of the PCSR.

Earthquakes beyond safe shutdown earthquake (SSE) level

4.11 In Section 5 the basis for selection of the level of excitation assigned to the safe shutdown earthquake is discussed. While the problems of extrapolating the meagre statistics which exist to events of lower probability than 10^{-4} events/year are recognised, the Inspectorate needs to be satisfied, as far as is reasonably practicable, that there is no sudden detrimental change in the risk/damage relationship for such events. The CEGB has undertaken to conduct sensitivity studies to explore this question. Sufficient assurance from such studies as to confirm the acceptability of the design basis proposed by the CEGB is required, prior to a decision on licensing.

Permissible stresses in the SSE

4.12 Although not explicitly discussed in the PCSR, the CEGB has given an undertaking that stresses under the action of the SSE will be shown to be within ASME Service Level B limits for active components required to function during or after an earthquake, and within Service Level D limits for all other Seismic Category 1 components and structures.

4.13 This is generally acceptable but the Inspectorate has two reservations on the details of these proposals as it understands them. The first is that all active components (as defined, for example, in the US Code of Federal Regulations) should be covered by the Service Level B limits. This would include, for example, the supports of the reactor pressure vessel, of the steam generators and of the reactor coolant pumps. The CEGB's intentions, are not clear with regard to these components. The second is that the Inspectorate is not yet satisfied that the Service Level D limits on stresses are adequate for assuring the integrity of the structures unless these stress limits are applied to the combined SSE and loss-of-coolant accident (LOCA), or SSE and steam line break (SLB), load cases as discussed in para 4.14 below.

Load combinations

4.14 US regulatory practice requires that all Seismic Category 1 components be analysed for combined SSE and LOCA loads, not only because it is thought that the SSE might be one of the more credible triggers for LOCA, but also to ensure that under the action of SSE and LOCA forces, propagation to other loops cannot cause the LOCA to exceed the design basis for the containment or ECCS. The CEGB has elected to dispense with this load combination and with it its logical extension to a SSE and SLB case, and have not provided adequate justification for the alternative proposed. The Inspectorate will need evidence from the CEGB to show that that the design bases for the containment and for the ECCS in particular are unlikely to be exceeded in earthquakes, or other external hazards, prior to a decision on licensing.

Operating basis earthquake (OBE)

4.15 A requirement of the NII's principles, which is also a regulatory requirement in the USA, is that an earthquake at a lower level of excitation than the SSE, called the operating basis earthquake, should be assigned. The International Atomic Energy Agency's Safety Guide also advises such an approach (ref. 18).

4.16 In the Inspectorate's view it would be advantageous to have multiple OBE events factored into the fatigue analysis, since otherwise it might be necessary to shut-down and re-validate the plant after any earthquake. The CEGB has not discussed this matter in the PCSR, though it is one on which the Inspectorate would wish to be satisfied prior to licensing.

External hazards trip

4.17 The Inspectorate would wish to see consideration given to a trip, controlled by excitation from external hazards, to provide automatic shut-down of the reactor in the event that the external hazard exceeds that level against which the plant is pre-qualified (for example, the OBE level). Following tripping because of an external hazard it would then be necessary for the CEGB to revalidate the plant for further service before plant start-up would be permitted. The CEGB has not yet offered such provision nor proposed any alternative philosophy of recovery from external hazards events.

Human factors

Introduction

4.18 Human factors (or ergonomics) is concerned with the efficiency of humans in their working environment. Efficiency in any particular task will be influenced by psychological factors, the environment, and the design of the man/machine interface. The safety of a nuclear power station will be affected by the efficiency of its staff in the following general areas:

(a) the management of the station;

(b) operations, particularly in the control room;

(c) the maintenance and testing of essential equipment.

4.19 A proper consideration of human factors requires that it is given detailed consideration at all stages and in all aspects of the station design and operation. The Inspectorate would expect the CEGB to have at its disposal suitable expertise to assist the design and operation departments.

4.20 The Inspectorate set up a Working Group in 1980, including two industrial psychology consultants, to give advice on human factors aspects of nuclear safety. Their report (ref. 19) suggests a number of areas that may require examination and it has been made available to the CEGB.

Human factors assessment

4.21 In the PCSR there is only brief mention of the role of the operator in testing and maintenance, operating procedures, operator training, the control room, and operator response to faults. The various sections give little indication of intent to design and operate to good ergonomic principles. However, the CEGB has said that such principles will be applied and, for example, has issued supporting reports to the PCSR dealing with changes and recommendations following the TMI-2 accident. The Inspectorate will expect to see evidence of this, together with the provision of a formal human factors assessment, prior to operation.

4.22 As would be expected at this stage, few details of the control room design are given. However, it is likely that previous CEGB experience, coupled with the application of contemporary ergonomics expertise, will produce an acceptable situation which the Inspectorate will be able to assess at a later stage.

4.23 The Inspectorate is particularly concerned with the following issues:

(a) The staffing intended for the station. A review should be carried out to look into the proposed management structure and procedures, including training, to confirm that they are suitable for a PWR station in the light of current knowledge.

(b) The fault studies in the PCSR appear to take no account of operator error. For example, whilst all protection actions for 30 minutes following a fault are to be automatic, if an operator intervenes during this period his reliability is likely to be much lower than that of automatic systems. Also, some actions by the operator are necessary after this initial period.

(c) Operator training. A highly realistic simulator should be provided to give suitable operator training in preventing and dealing with fault situations. It is understood that the CEGB is now committed to doing this.

Conclusions

4.24 Although human factors are not adequately considered in the PCSR, the CEGB has given a commitment to apply ergonomic principles to the design and operation of the station. Provided they show evidence of utilising sufficient expertise and resource this should lead to an acceptable position.

Quality assurance

Introduction

4.25 Quality assurance (QA) is a management system which is essential to provide adequate confidence in the control of the design, manufacture, construction, operation and decommissioning of a nuclear plant. A section on QA is included in the NII's principles and the Inspectorate has also written a guide (ref. 20) on this subject for use by its own staff and by licensees and suppliers. There are many examples, worldwide, where a failure in control of quality has led to a significant reduction in the safety of the plant and expensive modifications to correct the situation.

Assessment of PCSR and supporting documents

4.26 At this stage of the pre-licensing process the Inspectorate would expect the licence applicant to have prepared quality assurance proposals including a QA programme and management structure, and to have available the QA and quality control (QC) schemes from their main contractor for the main safety-related items of the plant. This should include sufficient information about the CEGB's management organisation to enable the lines of responsibility for safety in design and subsequent construction and operation, for policy decisions in regard to nuclear safety and for internal auditing of these responsibilities, to be identified.

4.27 The general statement of intent and approach to QA outlined in Chapter 3.9 of the PCSR is acceptable. It specifies, in sufficient detail at this stage, the main participating organisations and, with one exception, their respective responsibilities and interfaces. The exception is the lack of clarity of the respective roles of the CEGB's Engineering Services Department and the proposed Authorised Inspection Agency and this will need to be resolved before licensing. However, whilst the main QA documents to be prepared by the CEGB are specified in the PCSR, none of these is yet available for submission. The CEGB should be in a more advanced state of preparation than appears to be the case, especially in view of the considerable importance of a high level of QA and QC in ensuring satisfactory control of fabrication and enhanced margins of safety in the case of the reactor pressure vessel, reactor internals and other such items where steps have to be taken to prepare for ordering well in advance of licensing. This is also of concern in that it

appears to reflect a lack of commitment to QA by management without which there can be no guarantee of its acceptable implementation.

4.28 As the Inspectorate has not yet received the CEGB's QA programme for Sizewell B, it does not have all the details it would wish to have of the management organisation for the project. However, it has been supplied with the CEGB's Health and Safety Department (HSD) management structure and objectives and in March 1982 carried out an audit of the implementation of the procedures used in the preparation of the PCSR at the CEGB's HSD and Generation Design and Construction Department (GDCD) and at the National Nuclear Corporation (NNC). In general the performance was found to be satisfactory.

Conclusions

4.29 From the Inspectorate's examination to date, it is concluded that the CEGB's broad approach to quality assurance as outlined in the PCSR is acceptable but that, in the absence of a written programme and procedures for the main safety items, the Inspectorate has been unable to assess the detailed proposals. These are very important to safety and should be made available as a matter of urgency, especially in relation to the early order items.

Fire considerations

Introduction

4.30 One of the internal hazards which must be examined in assessing the safety of a nuclear power station is fire. It is not an infrequent occurrence and is one of those hazards where neither redundancy nor diversity of systems will ensure safety unless there is adequate protection. In this assessment the Inspectorate has judged the proposed strategy for dealing with the risk of fire and examined the consequences of fire upon safety.

4.31 The overall strategy adopted should have as its aims:

(a) to prevent fires from starting;

(b) to extinguish those which do start;

(c) to prevent the spread of those which have not been extinguished.

4.32 The major sources of combustible material are likely to be cables and lubricating oil. Significant reduction in the quantity of either of these is not practicable and the possibility of replacing them by non-combustible equivalents is limited.

4.33 The provision of fire protection equipment is dependent upon the fire hazard in each area and the CEGB's strategy is that of providing detection, extinguishing and suppression equipment appropriate to the risk. It is thus necessary to identify the risk in each area where fire might lead to a radiological hazard. In general, this has been done for the containment and auxiliary buildings. In the PCSR, areas of non-safety-related plant where high fire load exists, such as parts of the turbine building, are also considered. However, not all areas where a potential fire risk exists and where the radiological consequences of such a fire could be serious are identified, for example, the areas used for resin encapsulation of solid radioactive waste, and waste gas processing and storage.

4.34 The important aspect of personnel safety has not been adequately dealt with in the PCSR. Conventional fire protection practice has shown that unless such matters are considered as an integral part of the design process then the protection afforded can be markedly reduced.

4.35 Three principal areas have been identified which relate to parts of the strategy proposed for protection against the fire hazard which on the information available at present the Inspectorate would find difficult to accept without the need for design changes. These are discussed below.

Segregation

4.36 It is the intent of the CEGB as set out in Chapter 3.3.1.2 of the PCSR that a fire starting in one zone and destroying everything within that zone will still not prevent achievement of hot shutdown. (A zone is an area of the plant in which, should a fire occur, the hazard will not spread beyond the zone boundary. This is usually achieved either by enclosure in a fire-resisting structure or by separation.) To satisfy this aim, trains of protection equipment will be segregated by one of three means: a three-hour, fire-rated physical barrier, a one-hour, fire-rated physical barrier plus automatic fire detection and suppression, or spatial separation of at least six metres plus automatic fire detection and suppression. The Inspectorate has questioned the application of the last two of these methods and has informed the CEGB of its concern that active fire protection equipment is to be used in place of adequate segregation (by barriers or spatially). This appears to offer a lesser degree of assurance than is provided by best practice adopted in nuclear stations elsewhere. The Inspectorate will need to give further consideration to the proposed implementation of the physical barrier requirements and to the reliability of the active fire protection equipment to be provided, but at present there are reservations in these areas.

4.37 As the consequences of fire breaching a single three-hour rated barrier could be serious the Inspectorate would expect to see a high standard of fire segregation where this means of protection is proposed. It should be an imperforate fire-resisting structure so far as is reasonably practicable. Whilst it

is accepted that some breaching of the structure will be necessary, for example doors are required for access, penetrations are needed for fluids, etc., it is considered that these should be justified on an individual basis.

Cable routing

4.38 In the PCSR it is stated that cables will be routed via corridors and plant rooms. A basic fire prevention rule is to separate fire risk from fire load, i.e. to reduce the risk of ignition as far as is reasonably practicable. Plant rooms and corridors can possess a high risk of ignition due to the presence of switch gear, transient combustibles, etc., and should therefore contain only those cables required to service the areas concerned. It is not clear from the PCSR that this is to be done.

4.39 In addition to a reduction in the standard of nuclear safety, the Inspectorate considers that using corridors as cable routes is questionable as it could reduce the standard of personnel safety that might reasonably be expected for operators. The CEGB's strategy should be improved in this respect.

Fire at a reactor coolant pump

4.40 Fire protection for the reactor coolant pumps (RCP) is provided by a shroud surrounding the oil system for each motor which drains any leakage from the area to collecting tank. Fire at a RCP is said not to be possible because of this system. However, there is a need to demonstrate:

(a) the effectiveness of such a collection system, particularly since it has only recently been introduced in the USA;

(b) that fires starting elsewhere within the compartment, e.g. at the motor terminal box, will not spread to affect the oil system.

The consequence of fire in the RCP compartments could be fire exposure of unprotected steel work supporting the RCPs or steam generators.

Conclusions

4.41 The CEGB's approach to the internal hazard of fire is to apply a defence in depth strategy by examination of fire prevention, fire protection and fire segregation. While the Inspectorate agrees with this basic strategy, it has reservations about the way the strategy is apparently to be implemented in relation to the segregation of protection equipment, the routing of cables and the fire protection of the reactor coolant pumps. The Inspectorate also questions whether all the significant sources of fire risk in the site have been identified in the PCSR.

Introduction

5.1 This section is concerned with the case made about the impact of the siting of the station, its environment and potential hazard situations both external and internal, on the nuclear safety of the plant.

5.2 The demographical aspects of the site are discussed in relation to its geographical location to ensure that the site location is in conformity with policy on siting for the first of a new type of power reactor system in the UK. Then the geological and hydrological stability of the site and its consequences for plant stability throughout its projected life are considered. Finally an assessment is made of the safety impact of certain external and internal hazards, both natural and man-made, which may present a risk to the plant and thus to people.

5.3 In this context it is considered appropriate to take into account layout of both the site and the plant within it, and the consequent potential for adverse interaction between separate systems.

Siting

Introduction

5.4 In a densely populated area like the United Kingdom the contribution to safety to be gained from siting is limited, the main safeguard to the public from any risks arising from nuclear power plants has been and will continue to be the achievement of high standards of design, construction and operation of those plants. Nevertheless it is prudent to take advantage of the contribution which may be derived from the choice of site.

5.5 The Government adopted a cautious approach in its siting policy at the start of the first nuclear programme in the 1950s, in that heavily built-up areas were avoided and the sites chosen for the first (Magnox) stations were situated in comparatively remote, or rural, areas (ref. 21). Also the population close to the site was limited with the additional benefit that emergency countermeasures such as evacuation of people from the area could be readily carried out.

5.6 In 1968, after a safety review, the Government announced a relaxation of the earlier policy in the case of certain designs of reactors, specifically advanced gas-cooled reactors in pre-stressed concrete pressure vessels, which could be sited nearer to urban developments.

Siting of the PWR

5.7 For reactor systems new to commercial use in the UK, like the PWR, it is policy to utilise remote location until appropriate experience has been gained (ref. 22).

5.8 The site at Sizewell is located such that it is suitable for any reactor system which can be licensed for commercial use in the UK.

The site

5.9 The Sizewell site is situated on the Suffolk coast about 20 miles south of Lowestoft (population approximately 52 000) and 22 miles north east of Ipswich (population approximately 125 000), the nearest large towns in the area. With regard to population distribution, the most sensitive sector lies west by south of the site and includes 14 small villages and the town of Leiston (population approximately 5000) which is situated one and a quarter to two and a quarter miles from the site.

5.10 Arrangements exist for consultation with the local authorities on any proposed residential and industrial developments in the vicinity of the site with the objective of maintaining the site characteristics.

Summary and conclusion

5.11 A site having been accepted for a nuclear station, arrangements are made with the local authorities to ensure that residential and industrial developments are controlled so that the general characteristics of the site are preserved. In the case of Sizewell, the site was accepted for the existing station as one which fell within the policy and characteristics for more remote sites, and it remains within that class of sites which would be acceptable for any reactor system licensed for commercial operation in the UK.

Geology and hydrology

5.12 The geological structure, seismology and hydrology of the site have been examined to ensure that it would be satisfactory for the construction of a further nuclear installation. The information reviewed, which is based on a comprehensive investigation (ref. 23) of the site carried out on behalf of the CEGB between early 1968 and the end of 1980, indicates that all of the site which could affect the security of the nuclear power station is uniform, compact and capable of taking all constructional loads. No unusual civil engineering techniques will be needed for building the plant. Monitoring techniques to be used in assessing the settlement of the reactor buildings are referred to in the PCSR. These proposals are satisfactory as settlement is not likely to be great.

Site layout

Introduction

5.13 In assessing the safety implications of site layout the sections of the PCSR in Chapters 1, 3, 5, 6, 9, 10 and 15 dealing with building and plant layout on site, buildings and systems classification, system function and performance, and system inter-connections and interfaces were considered. The main objective was to assess the adequacy of the site and plant layout arrangements for minimising the adverse effects of both internal and external hazards, particularly in regard to the protection system.

Assessment

5.14 The general strategy of site and plant layout follows closely that developed for the SNUPPS plant combined as far as possible with UK practice. This is broadly acceptable. However, in its detailed application the safety aspects of the proposed layout of the various buildings, and juxtaposition of buildings and systems throughout the plant are not yet satisfactorily dealt with. Also, as might be expected, the present stage of the design as described in the PCSR and the Reference Design Report excludes many detailed aspects of the plant layout and contains only minimal information on such matters as layout of cabling, auxiliary pipework routes and protection and control systems. Further information in support of the safety case in this area will be required at a later date.

5.15 Physical separation and segregation of redundant and diverse systems are claimed as contributing towards meeting the design safety guidelines for protection against internal and external hazards. However further information needs to be provided to demonstrate this. Firstly, the sensitivity of layout arrangements to hazards which are within the design basis needs further consideration. Secondly, the behaviour of buildings and plant following events of lower probability than the design basis should be explored to show that there is no sudden change to an unacceptable failure mode. Particular examples are:

(a) the susceptibility to damage from missiles, and possibly from aircraft crash or fire, of vulnerable parts of the plant;

(b) the possible adverse interaction arising from the location of the single refuelling water storage tank near non-seismically qualified structures;

(c) the effect of layout on the requirement for separate entrance and exit to areas of potential fire hazard.

Conclusions

5.16 The impact of the site and plant layouts on safety is not treated as a separate topic in the safety case but is claimed to be covered implicitly in the overall safety assessment in the PCSR by due consideration in each section. However, especially in the absence of specific CEGB design guidelines on layout, the treatment provided needs to be improved in a number of areas before it can be regarded as satisfactory.

5.17 In the absence of firm acceptance of the range of design basis external hazards proposed in the PCSR, only qualified acceptance of the proposed layout can be given. This therefore will need to be re-examined when the range of hazards to be considered is finally agreed.

External hazards

Introduction

5.18 A consideration in siting a nuclear power station is the possibility of hazards arising from sources external to the site. Both the NII's principles and the CEGB's criteria require that the possibility of such hazards should be examined and either the chance that they might affect the station shown to be acceptably low or the station shown to be protected against them such that the consequences in terms of release of radioactivity are acceptable. These hazards include natural hazards, such as floods, earthquakes and high winds, and man-made hazards, such as missiles and explosive or toxic gas clouds from industrial or transport sources in the vicinity of the site, aircraft crashes and sabotage. A feature many of these hazards have in common is that the whole plant can be threatened so that, for example, neither redundancy nor diversity of protection systems will ensure safety unless the systems are suitably qualified and designed against the hazard. This means that such hazards may potentially present a more significant threat to the safety of the plant than internal faults or failures.

5.19 It may be possible to show that the probability of an initiating event is so low that no further consideration is necessary. However, if this cannot be satisfactorily demonstrated, other ameliorating factors, such as plant layout, diversity and segregation of protective features (adopted perhaps for other reasons) will need to be taken into account in order to demonstrate that the potential for a release of radioactivity of unacceptable proportions is sufficiently small. Such an evaluation could include an examination of the effects of the event on the plant itself. The external hazards of significance are discussed below.

Aircraft crash

5.20 It is the CEGB's claim that the probability of an aircraft crash on the proposed power station in such a manner as to prejudice nuclear safety is sufficiently low that additional design measures need not be provided specifically for this hazard, and that this will remain the case in the foreseeable future. In the

Inspectorate's view the case made in the PCSR is insufficient to support this contention and it has asked for further review by the CEGB of the statistical analysis of the probability of significant aircraft crash with particular reference to the Sizewell area. The CEGB does not expect to be able to complete this work until later in 1982 but anticipates that the work now in hand will be capable of producing the required case. If not, then for those aircraft with an unacceptably high probability of impact, it will need to be shown to the extent necessary that the combination of impact probability and consequences in terms of effect on the plant is such that they will not cause unacceptable releases.

Gas cloud explosion

5.21 Should a cloud of gas, for example from an accident to a tanker containing liquefied petroleum or liquefied natural gas, drift over the site and be ignited it would present a significant loading on the containment and other structures and could lead to a serious accident. It is claimed in the PCSR that the probability of a gas cloud explosion affecting the site from the transport and use of such materials in the vicinity of the site is so low that no special measures are deemed necessary. This statement is acceptable for land-based traffic and fixed installations but the potential hazard arising from shipping needs further examination by the CEGB before licensing.

Industrial sources

5.22 In the case of Sizewell, industrial hazards are adequately controlled by the local authorities, acting on the advice of the Inspectorate where necessary.

Safe shutdown earthquake

5.23 The Inspectorate has accepted that the zero period acceleration of 0.25*g* assigned to the safe shutdown earthquake (SSE), corresponds approximately to the expected excitation at the 10^{-4} events/year level, based on mean UK seismicity. However, it is noted that the largest UK earthquakes in the past century have occurred in the East Anglia region (Colchester and Dogger Bank) and both appeared to have offshore epicentres. The Inspectorate has asked for assurance that no offshore tectonic features (faults) exist, which might render inappropriate the assumption of mean seismicity.

Flooding

5.24 The Inspectorate has reviewed the CEGB assessment of flooding risk which identifies the sandhills to the seaward side of the station as the major defence against flooding. Generally, the arguments are acceptable, but the Inspectorate has indicated a wish to see a more rigorous assessment of the risk of waves over-topping the sandhills so that the possibility of generalised flooding of the station, which could impair the functioning of protective systems, is seen to be sufficiently remote.

6 Nuclear design

Introduction

6.1 This section of the report is concerned with the nuclear characteristics of the fuel and the reactivity control systems and their effect on the safety of the plant. The nuclear design affects the behaviour of the plant during normal operation and also during fault conditions and is, therefore, of central importance to the safety case. It is discussed mainly in Chapter 4 of the PCSR.

6.2 There are a number of specific aspects of this part of the safety case which require consideration. Firstly, the prediction of power distribution is an important input to a determination of fuel behaviour and to the behaviour of plant in normal operation and fault conditions. Similarly, temperature coefficients of reactivity and the effect of soluble boron in the moderator play an important part in plant behaviour. The shutdown margin is also a feature which is of importance in relation to potential faults, in particular, failure of the shutdown system (ATWT) and main steam line break. While not seen as of major importance, core stability has to be considered and, finally, the radiation doses received by structures and the pressure vessel need to be assessed.

6.3 At the more general level, there are other points to be considered. The requirements for validation of codes used in the safety case are particularly important here, where confidence in some of the key parameters mentioned above is dependent upon the validity of codes used in their derivation.

6.4 Plant operating procedures can have implications in relation to the nuclear design; control rod patterns, arrangements of rods in control and shut-off banks, and refuelling procedures are some examples. The Inspectorate has done little assessment in this area but, following the work done at the time of the generic review, it does not anticipate any problems which cannot be overcome by suitably defined modes of operation.

Power distribution

6.5 The method of restricting the power shape in the core is by operator control within set limits of axial offset, power and departure from nucleate boiling ratio (DNBR) for the peak-rated fuel. These limits have to cover the large number of flux shapes expected during normal operation throughout the life of the core and also arising from control rod malfunction and operator error. Even though it is claimed in the PCSR that assurance on this approach has been obtained by measurement of over 1000 such flux distributions, situations could arise where these limits are exceeded. Such cases are likely to be associated with a large axial offset which causes an alarm to occur. This alarm is followed by a trip if the power or DNBR limits are exceeded.

6.6 The information provided in the safety case on power distribution control is difficult to follow and in some areas is inadequate or not strictly relevant to the Sizewell design. In particular, there is no discussion of the basis of the uncertainties associated with the components of the peak rating. There is also insufficient information to provide verification of the correlation between the measured axial offset and the actual offset in the core.

Reactivity coefficient

6.7 There are a number of reactivity coefficients related to changes in fuel and coolant temperature, coolant pressure, density, voidage and boron concentration, which play an important role in both reactor control and fault transients. Some of these coefficients are positive, others negative, and their effects can be stabilising or destabilising, depending upon whether the relevant reactor parameter increases or decreases during the course of the fault.

6.8 On the whole the approach adopted in the PCSR for the calculation of these reactivity coefficients is adequate, although further information needs to be provided. For example, it is necessary for the CEGB to provide details of the core behaviour and reactivity coefficients which span the entire life of the plant instead of just the first cycle, and they have agreed to do this. Again, full details of the determination of the Doppler coefficient are not provided. Finally, the reactivity effect of the large void in the core coolant expected during LOCAs is not included in the information in the PCSR. These deficiencies will need to be made good before a decision on licensing is made.

Shutdown margin

6.9 On insertion of the control rods at power, there are reactivity contributions arising from the Doppler effect, the variation of the average moderator temperature, the effect of flux redistribution and the reduction in coolant and void content. These reactivity effects have been estimated conservatively, and the reactivity worth of the control rods is sized to compensate for the reactivity changes leaving an appropriate allowance for shutdown margin.

6.10 However, there are two reservations arising from the Inspectorate's assessment of the determination of the minimum shutdown margin. Firstly, the size of the shutdown margin has been reduced, compared with some earlier plants, on the basis of the less onerous requirements applied to the Sizewell plant for the main steam line break accident (the requirements to prevent DNB occurring for the highest rated fuel channel and to prevent hot leg boiling). Even though the size of the shutdown margin appears to be adequate for operating states of the Sizewell PWR, justification is required for reducing it from 1.69 Niles for previous Westinghouse plants to 1.3 Niles for Sizewell. In the justification the Inspectorate would expect, on reliability grounds, two control rods to be assumed stuck out of the core when determining the shutdown margin; no discussion is given in the PCSR of the reasons for assuming only one stuck rod.

Stability

6.11 Calculations in the PCSR show that the core is stable against xenon oscillations although the axial stability decreases with burn-up, the stability index becoming zero at 12 000 MWd/te. Hence demand on the control system and the operator are likely to increase with burn-up. The Inspectorate expects to see, therefore, a discussion in the safety case of the effect of operator and control system error on maintaining stability at the end of the life of the core. This should be provided before licensing.

6.12 Only a limited number of measurements of stability have been made for cores of similar size to that of the Sizewell PWR and additional measurements would help to give confidence in the analysis.

Pressure vessel and reactor component irradiation

6.13 Standard transport theory methods are used to calculate the neutron doses in the pressure vessel walls and other structural components, but there appears to be no comparison of the results of calculations with measured neutron doses or fluxes. Such comparison is required in support of the calculations.

Analytical methods

6.14 The analytical methods used to calculate the neutronic performance of the reactor core are generally adequate, although further information will need to be supplied. In particular a detailed description of the method of calculation of the Doppler coefficient is required. Validation of the codes used in the analysis should also be provided.

Conclusion

6.15 For the most part the Inspectorate is satisfied with the information on the nuclear design and sees no reason why its concerns, which require additional information or further justification, cannot be met by the time a decision on licensing is required.

7 Fuel element behaviour and core thermal hydraulic design

Introduction

7.1 Fuel element behaviour is of importance to the safety of a nuclear plant primarily because the fuel contains the major part of the radioactive products in the plant. Its performance as a heat source is crucial to safety because the release of its fission products is the likely consequence of some failure to transfer its heat to the coolant. In addition, it has an influence upon the core reactivity, and therefore upon the heat generation rate, because of the feedback effect of the fuel reactivity coefficient.

7.2 The adequacy of the fuel element design and safety case as set out in Chapters 4 and 15 of the PCSR is assessed in relation to the NII's safety assessment principles. For normal operation (and this includes ANSI Condition I operational transients) this means that all reasonable steps should be taken to minimise the failure of the fuel rod cladding and thus minimise the release of radioactive fission products into the coolant. For fault conditions, the definition of satisfactory performance depends upon the frequency with which the fault is expected to occur, as discussed later.

7.3 In order to demonstrate compliance with the relevant requirements of the principles, the Inspectorate expects the safety arguments in the PCSR first, to define and justify the limits within which the fuel can operate safely during both normal and fault conditions and, second, to demonstrate that none of the limiting criteria is exceeded when the fuel is subjected to the full range of operational and fault conditions. For fault calculations it is necessary to describe the initial fuel conditions from which the fault is assumed to occur and to demonstrate that they are appropriate to any history and mode of operation which the fuel might undergo during the life of the plant.

Thermal and hydraulic design

7.4 The overall objective of the thermal and hydraulic design given in the PCSR, i.e. to provide adequate heat transfer compatible with the heat generation distribution in the core such that the safety design bases are met, represents an acceptable statement of intent.

7.5 The safety arguments are made in relation to specific design bases and design evaluations. The Inspectorate's assessment has shown that the PCSR does not provide sufficient detail to demonstrate that the safety assessment principles are met, but further information is given in supporting reports which have not yet been assessed. More information may be required to resolve outstanding points, but the Inspectorate does not regard this as a serious problem. It should be recognised, however, that resolution of some of the problems could result in a reduction of the margins available to accommodate fault transients and therefore, in the extreme, it is possible that core power restrictions may be necessary to restore these margins to acceptable levels.

Fuel limiting criteria

7.6 Fuel rod performance criteria are used to demonstrate that the fuel design is capable of meeting the requirements laid down in the safety case. There are three main types of criteria, relating to design, clad rupture and secondary limits.

Design criteria

7.7 Current and past operational experience of PWRs appears to demonstrate that the proposed fuel assembly design is capable of meeting the design criteria as described in the PCSR. However, whilst this evidence in support of the safety case is accepted, there are a number of detailed claims made in the PCSR which will require further information and assessment. This is not expected to reveal problems which would require changes in fuel assembly design, but it is nevertheless important to confirm that the assembly will operate with adequate safety margins. The CEGB has promised to produce the required information to demonstrate that the safety margins are acceptable before a decision on licensing is required.

Clad rupture criteria

7.8 These criteria are used to show that no additional fuel failures occur in frequent faults covered by the ANSI Condition II events. In the case of the more severe Condition III and IV events, the criteria are used to determine the total number of failed rods and hence the radiological release associated with the fault. (The design basis faults of Chapter 15, in principle, cover these three ANSI conditions.)

7.9 Assessment of the five rupture criteria has shown that not all have been adequately justified and, therefore, further information to verify the claims made in the PCSR will be required. The main areas of concern are associated with:

(a) the use of the departure from nucleate boiling ratio (DNBR) failure criterion (DNBR less than or equal to 1.3),

(b) the applicability of the criterion, peak clad stress < yield stress, and

(c) the adequacy of the radial average peak fuel enthalpy criterion when applied to slower transients.

DNBR criterion

7.10 The concern here is related to two applications of the criterion. In the first, it is used to demonstrate that, for transients of a frequent nature where the plant protection systems are designed to limit the minimum DNBR in the core to > 1.3, no additional failures will occur. Whilst the existence of film boiling on a fuel rod does not necessarily cause clad failure, DNB is conservatively interpreted in the PCSR as a failure of the cladding. The onset of film boiling is statistical in nature and a value of 1.3 for the DNBR means that, at the 95% confidence level, there is a 95% probability that the fuel rod will not be in film boiling. Conversely, however, this implies a 5% probability that the rod will be under film boiling conditions and, on the basis of the PCSR interpretation, must be assumed to fail.

7.11 The number of failed fuel rods in the core during normal operation is used to define the radiological source term in accident conditions, and it is assumed in the PCSR that the source term results from the equivalent of between two and three failed rods, i.e. 0.005% of all the rods in the core. However, application of the above statistical argument to the current Westinghouse reactors suggests that as many as 20 fuel rods could be failed for a fault where the protection system limits the minimum DNBR to > 1.3. In the Inspectorate's view derivation of the initial source term should take account of this higher number of failures, unless convincing arguments are produced in favour of the assumed source term, and this should be in the safety case.

7.12 The second concern is related to the use of the DNBR criterion in determining the total number of failed rods in the core following the more severe accidents. The method given in the PCSR assumes that, if the DNBR is less than or equal to 1.3, the rod fails; if it is greater than 1.3 then no failure is assumed. A clear demonstration that this approach is conservative should be provided before a decision is made on licensing.

7.13 The CEGB has given a commitment to provide further information on both the above points in order to satisfy the Inspectorate's concerns.

Peak clad stress and pellet/clad interaction

7.14 While accepting that in most circumstances DNBR will be the limiting criterion, the Inspectorate considers it necessary for faults to be evaluated against all the relevant rupture criteria in order to confirm that the failure prediction is not an underestimate. Demonstration of adequate performance in some faults is related to peak clad stress being less than the yield stress. This criterion has been shown to be less restrictive than the pellet/clad interaction (PCI) criterion and hence the current analysis, which claims to show no additional clad failures, could be non-conservative. Resolution of this issue is not regarded as a serious problem, but it will require the use by the CEGB of accident analysis codes which are not currently used by Westinghouse.

Fuel enthalpy criterion

7.15 The Inspectorate has also questioned the use of the radial average peak fuel enthalpy criterion for reactivity initiated accidents. Here the main concern relates to the application of the criterion to transients slower than those used experimentally to derive the limits. For fast transients the experimentally derived values will be used; for slow transients, i.e. those taking longer than ten seconds, the PCI criterion will be used. However, in the case of intermediate transients, an acceptable failure criterion has not been identified in the PCSR. This point will need to be covered in future submissions.

Secondary limits

7.16 The secondary limits define the conditions beyond which the fuel is assumed to suffer loss of geometry leading to a possible loss of coolability and severe fuel damage. The assessment of these criteria has revealed a number of shortcomings. This is not necessarily a criticism of the limits themselves, which may be perfectly acceptable but, without an adequate supporting case in the PCSR, a judgement on the matter cannot be made.

7.17 For reactivity initiated accidents (RIAs), the Inspectorate has reservations about the proposed limit for radial average peak fuel enthalpy deposition for pre-failed or defective rods. There is insufficient justification in the PCSR for the 90 cal/g limit and, unless it can be shown that failure propagation resulting from the energetic disruption of defective fuel does not occur, the proposed limit could be too high.

Fuel behaviour in normal operation

Operational experience

7.18 The safety arguments given in the PCSR to justify the Sizewell B fuel design for normal operation can be divided into two main types: those related to the design bases and those concerned with evidence from PWR operational history.

7.19 The design bases are requirements for fuel rod, fuel assembly and RCCA design to ensure that the components can perform their duty during normal operation and frequent faults. There is insufficient information to demonstrate that, under the worst expected operating conditions for Sizewell B, these design bases are met.

7.20 The arguments based on operational history are important and there is a great deal of evidence to show that current Westinghouse fuel can perform satisfactorily under normal operating conditions. The Sizewell B design will, however, use BNFL CONPOR fuel pellets. These are used in French PWRs, though actual evidence from this source has not been made available in the PCSR. Despite the difference, the Inspectorate regards the current Westinghouse experience as being relevant. The high standard of reliability shown by PWR fuel gives confidence that the proposed fuel design will be satisfactory in normal operation.

Fault initial conditions

7.21 Whilst operating experience is satisfactory, this is not a complete demonstration of a satisfactory fuel design since it is the loadings which result from fault conditions which are limiting. To determine fully the adequacy of the fuel design, it is necessary, therefore, to study its behaviour in faults. However, the outcome of a fault depends upon the starting conditions of the fuel, which result from its previous history and the reactor conditions immediately prior to the fault. To derive these initial conditions it is necessary to calculate changes in the important fuel parameters during the life of the reactor.

7.22 The approach described in the PCSR is to define a single set of initial conditions which characterise the worst possible conditions in the core prior to any transient. The use of this method is accepted in principle, but the CEGB is required to demonstrate that the initial characterisation of the fuel for transient analysis is not exceeded by the worst possible operation of the Sizewell B core. Additional information to that given in the PCSR is required to demonstrate this.

7.23 The Inspectorate has been unable to check, therefore, that the initial fuel conditions used in the fault transient analysis are pessimistic. As a result, there is some uncertainty about the size of the margins that are available to accommodate fault transients. In view of this, the case for the behaviour of fuel under normal operation is considered to be incomplete and further information on the bounding limits and their justification will be required before a decision is taken on licensing. This problem is regarded as a shortcoming of the PCSR, rather than a fundamental problem of the fuel design or operating conditions.

Fuel behaviour in fault conditions

7.24 The fuel is most at risk under fault conditions and its behaviour then has direct implications on the subsequent release of radioactive material. The safety case needs to show, therefore, that the chosen limits appropriate to each fault are not exceeded during the course of the fault transient, thus ensuring that the damage done to the fuel rods does not prevent safe shut-down and subsequent removal of fuel from the core. For all faults a coolable geometry should be maintained, so that damage propagation leading to conditions outside the design basis is prevented.

Frequent faults

7.25 In the case of frequent faults (ANSI Condition II) the Inspectorate would wish to see no additional fuel rod failures as a result of the transient. A sufficient description of fuel behaviour in frequent faults is not given in the PCSR. In particular, the appropriate limiting criterion associated with each fault is not specified or justified. The only failure criterion used is DNBR less than or equal to 1.3, since peak linear heat rating is always below the specified limit. The problem of clad stress induced by pellet/clad interaction (PCI) has not been covered adequately in the PCSR and further information will be required. It is understood that the CEGB has initiated work to provide this.

7.26 Calculations have been presented to determine clad stress in what is claimed to be the most limiting fault, the rod cluster control assembly (RCCA) bank withdrawal and, whilst the peak clad stress is below the yield stress criterion, it is in excess of the PCI failure criterion. A more satisfactory argument is required on this point since otherwise limitations would need to be applied in relation to the proposed mode of operation or fuel operating conditions.

Infrequent faults

7.27 For infrequent faults (ANSI Condition III) some degree of fuel failure is acceptable because of the lower probability of the fault occurring. Acceptance of the safety case depends upon a clear demonstration that the amount of fuel rod failure is as low as reasonably practicable, and that the resultant radiological consequences are within limits appropriate to the expected frequency of the fault.

7.28 For the single RCCA withdrawal fault, the treatment of fuel is unsatisfactory. In particular, details of the core-wide fuel rod failure analysis are not presented and so the adequacy of the 5% failure fraction cannot be assessed. Additional information is also required on the fuel and clad temperature variations during the transient, since it is possible that the 30-minute period before operator intervention would, in principle, allow film boiling on some fuel rods for that period of time. This is likely to give rise to enhanced fission gas release from the fuel pellets and thence, via the failed cladding, to the coolant. In addition it could allow excessive clad oxidation going beyond the 17% secondary limits which, on the subsequent quench, could bring about brittle failure of the cladding of the affected fuel. This is a pessimistic interpretation of the course of events. At the present time, however, the Inspectorate has no means of judging a more favourable outcome.

7.29 The treatment of fuel failure in this fault assumes DNBR to be the limiting criterion but PCI could be a contributory failure mechanism. PCI has not been considered and it will be necessary, therefore, for the CEGB to show that DNBR adequately bounds PCI failures.

7.30 In the case of the incorrectly loaded fuel assembly fault, no information on fuel behaviour is provided in the PCSR. It is claimed that operating procedures will identify any abnormal power distribution before power raising commences, and hence there will be no challenge to the fuel. Since administrative procedures are relied upon, a study of fuel behaviour in this fault is judged to be necessary to show that the consequences are acceptable.

Limiting faults

7.31 For all limiting faults, the Inspectorate would expect the radiological release to be within acceptable limits consistent with the frequency of the fault (which is low) and coolable geometry to be maintained. Additionally any damage done to the rods should not prevent safe shutdown and subsequent removal of the fuel from the core.

7.32 The Inspectorate has several reservations about the adequacy of the case made in the PCSR to satisfy these requirements. Two general comments can be made. Firstly, very little information is given in the PCSR about the initial fuel conditions used in the transient analysis and, hence, it has not been possible to check that the most pessimistic initial conditions have been assumed. Secondly, there is a lack of detail regarding the whole core failure analysis and it has not been possible to check the core-wide fuel rod failure fractions which are assumed. In addition, there are concerns related to the large break, loss-of-coolant accidents (LOCA) and RCCA ejection faults.

Large break LOCA

7.33 The current method of demonstrating compliance with the fuel secondary limits which has been developed in the USA, and subsequently used in the PCSR, is to use an 'evaluation model' to predict theoretically the consequences of the accident transient. The Inspectorate has reservations about the models which describe fuel behaviour, in particular the treatment of fuel rod clad swelling and rupture, blockage heat transfer and cladding oxidation in ruptured rods. These models will need to be reassessed when the CEGB makes the revised 1981 Westinghouse Evaluation Model available to the Inspectorate.

7.34 The evaluation model approach aims to provide a pessimistic calculation of peak fuel rod temperature based on the use of conservative modelling of the plant response during the accident. At the time of the generic review, the Inspectorate was concerned that this approach, which concentrated on the response of the hottest fuel rod in the core, could possibly be non-conservative because it ignored the response of lower rated, i.e. cooler, rods which exhibited temperatures where the cladding would distend. It was felt that this ballooning of the cladding could cause a flow blockage within the core which would interfere with the ability of the emergency core cooling system (ECCS) to cool the core. This could lead to an unacceptable situation with a loss of coolable geometry and hence severe fuel damage. The clad ballooning safety case is not presented in the PCSR because, despite the intense international research programmes to study this phenomenon, the information necessary to make the case apparently could not be assembled on the PCSR timescale. However, the overall strategy proposed by CEGB is regarded as an acceptable framework for presenting the safety arguments. If the safety case can support the objectives of the strategy, it should prove sufficient to satisfy us. We must, however, withhold judgement until the submission, expected later this year, has been assessed.

7.35 In the event that the safety arguments for clad ballooning are judged to be inadequate, options are available to overcome the problem, but these would have implications on either the fuel design or its operation, or both. Alternative fuel designs which have been discussed with the CEGB look promising, but the detailed safety arguments have not so far been made. If it became necessary to resort to an alternative design, certain aspects of the safety case for other faults would need to be reconsidered. Finally, if the safety case were still unacceptable after all of this, then reactor power would need to be limited to a level where the potentially damaging transients were avoided.

RCCA ejection

7.36 In the treatment of this fault, the Inspectorate wishes to see more detail regarding fuel failure calculations, since they may need revision for the Sizewell B design. No analysis of the response of previously defective fuel is presented in the PCSR, which is a shortcoming given that the PCSR defines the secondary limit at 90 cal/g whereas the calculated radial average peak fuel enthalpy for this fault is given as 176 cal/g. The effect of defective fuel rods suffering disruptive failure and affecting adjacent rods during the course of the fault has not been considered. For this fault to be acceptable it will be necessary to show that failure propagation cannot occur and that ejection of fuel particles into the coolant is insignificant in terms of the consequences of release of radioactive materials.

Anticipated transients without trip (ATWT)

7.37 Further information should be given in the PCSR on the treatment of fuel behaviour in this category of faults. For the faults which are dealt with, the case made in the PCSR suffers from the same

deficiencies as for the other fault categories previously discussed.

7.38 In addition to fuel rod failure, ATWT faults often test the pressure circuit; the pressure transient generated by the fault is influenced by the fuel behaviour, especially the fuel-to-clad gap heat conductance. There is not sufficient information in the PCSR to assess adequately the interaction between fuel behaviour and the core response. Hence, the Inspectorate will require a clear demonstration that fuel behaviour is adequately accounted for in reactor transient analysis associated with ATWTs.

Conclusions

7.39 The treatment of fuel behaviour and its implications on reactor safety constitute an important part of any proposed safety case. This was recognised by the Inspectorate in the generic review and a number of safety issues relating to fuel behaviour were identified. the current assessment of the Sizewell B PCSR has shown that most of the main fuel issues raised then have been taken into account. The Inspectorate is satisfied that experience to date with PWRs demonstrates satisfactory fuel performance in normal operation. However, it is concerned about the adequacy of the case set out in the PCSR to demonstrate acceptable fuel performance in the design basis accidents and further information will be required before a decision is made on licensing.

7.40 The majority of these concerns relate to the lack of evidence to support the chosen fuel limiting criteria and to show how the fuel behaves in relation to these criteria. This involves insufficient detail on both the assumed fuel state and the computer codes which calculate fuel response. It is recognised that these inadequacies result, in the main, from the different licensing requirements in the UK and the USA and, therefore, the Inspectorate believes that, given time, a suitable case can be made which will remove the majority of reservations. However, at this stage it cannot be said that resolution of the Inspectorate's concerns will be achieved simply by improving the calculational techniques used to make the safety case.

7.41 If the application of the current DNBR limit is found to be non-conservative some changes may need to be made. These could include the use of more restrictive trip settings in the protection system, or a different mode of plant operation, or some combination of the two.

7.42 The safety case has not yet been presented on clad ballooning, which was raised in the generic review as an important issue, and so a judgement cannot yet be made on this topic. However, a number of alternative positions are available, though further justification would be required for the CEGB's preferred options.

7.43 The demonstration, in the PCSR, of the adequacy of the thermal and hydraulic design is incomplete. Despite this, the Inspectorate does not regard the deficiencies as a major problem and believes that, given time, its concerns can be satisfactorily resolved. Failing this, it should be possible to overcome any residual problems by suitable changes to the mode of operation of the plant.

7.44 In view of the Inspectorate's concern about the treatment of fuel in the PCSR, more information will be required before a decision can be made on licensing.

8 Civil works and structures

Introduction

8.1 The civil works and structures throughout the plant play a safety role in supporting equipment and providing protection for equipment and operators against a potentially hostile environment. For example, in terms of fire protection, emphasis is placed on the durability of structural members (i.e. the length of time they can be expected to resist penetration by a major fire) which segregate one train of protection equipment from another.

8.2 Probably the most important of all the civil engineering works is the containment which, together with its supporting systems, represents the last line of defence against uncontrolled release of fission products, in events involving ruptures of the primary circuit.

8.3 It is somewhat paradoxical that the most exacting duty imposed on many of the more important structures (particularly considering external hazards loading) is to resist collapsing on to the equipment.

General

8.4 A brief but comprehensive review of the CEGB's proposals in respect of civil engineering works for the Sizewell B project has been conducted. This embraces parts of Chapter 3 and all of Chapter 14 of the PCSR, together with the supporting reports referenced in Chapter 14.

8.5 Reservations have been raised concerning the classification of structures, design criteria (particularly in terms of load combinations) and quality assurance (which are discussed in Section 4 of this report), and on the treatment of external hazards (discussed in Section 5). The Inspectorate has also raised some issues on foundation design, soil fluidisation and containment structural design which are discussed in the remainder of this section.

Foundations

8.6 The Inspectorate has generally accepted, on the basis of advice to the CEGB from Professor Bolton Seed (ref. 24), that a large margin of safety exists against the risk of soil fluidisation up to the level of earthquake presently specified at the safe shutdown earthquake level. Since, however, the Inspectorate has expressed some concerns on seismic design in earlier sections of this report (notably to query what offshore tectonic features might exist that could invalidate the CEGB's assumption that mean UK seismicity is appropriate to the site), it is pertinent to note that certain of these concerns could require a reassessment of this conclusion about the stability of the soil.

8.7 The Inspectorate has recently been advised by the CEGB that the foundation design of the main buildings incorporates single-pipe containment of radioactive drainage as on the SNUPPS plant. Such a proposal would be a departure from the standards normally adopted by the CEGB. It is clear from the proposals that redesign of the foundation slabs would be necessary to incorporate pipe-within-trench confinement of radioactive drains. Nonetheless, these proposals (not explicitly described in Section 9.3 of the PCSR) are not satisfactory as they stand. It is understood that further information is to be provided.

Containment

8.8 The basic approach to structural design of the containment proposed in the PCSR and supporting reports is to adopt the philosophy of ASME III Division 2, but to 'anglicise' the ASME Code to incorporate Système International (SI) units in place of the Imperial units used in ASME, to adjust the cylinder strengths used as control in the USA to the cube strengths used in the UK and to make other adjustments to adopt the codes to UK design and construction practice. The Inspectorate has had detailed discussions on the successive drafts with CEGB, and is satisfied that this presents no obstacle to licensing. It should be noted, however, that several of the issues raised in Sections 4, 5, and 16 could have significant impact on containment design.

8.9 The Inspectorate has recently been advised that it is intended to extend the secondary containment, provided by the auxiliary building, to enclose all of the primary containment. Worldwide experience of concrete steel-lined containments supports the view that leak rates of the order of 0.1 %/day are achievable at design conditions, the greater part of the leakage occurring at penetrations. Nevertheless, the provision earlier described in the PCSR was of a secondary containment which did not enclose the equipment access hatch (the largest penetration in the containment). The safety case for the secondary containment should be established prior to licensing.

8.10 The downward adjustment of the design pressure from the SNUPPS design, has been explained in terms of the larger contained volume of Sizewell B. The Inspectorate has been informed that the same margins on mass and energy release and on calculated design pressure as are applied to satisfy USNRC

requirements have been applied on Sizewell B and this would be acceptable. However, concern is expressed in Section 16 on the determination of the peak pressure reached in the limiting design basis transients and this concern will need to be resolved.

8.11 The Inspectorate's emphasis on protection against man-made external hazards in discussion with the CEGB stems from studies which indicate that containment response to earthquake, for example, is predominantly beam-mode response (which occurs at frequencies generally lower than the first natural frequency of major equipment) whereas gas cloud explosion or aircraft crash excite shell modes in the containment, and these straddle the equipment frequency range. It follows that analysis of earthquake response contributes little toward assurance against aircraft crash or gas cloud explosion, or vice versa. Hence, even if significant damage to the containment can be ruled out by inspection for small aircraft or modest explosions, analysis of the detailed equipment response is required to provide assurance against LOCA or steam line break beyond the containment design basis.

Conclusion

8.12 There are a number of specific concerns and qualifications which will need to be cleared, but apart from these reservations and qualifications, the Inspectorate is generally satisfied that the proposals made in the PCSR for the containment and other civil works and structures provide an acceptable basis for licensing.

General

9.1 The reactor pressure vessel (RPV) is one of those components, identified in Section 2.5.1.4 of the PCSR, whose failure is held to be 'incredible', that is to say, the probability of failure is deemed to be so low that no protection against that failure is required. At an early stage in the Inspectorate's negotiations with the CEGB it became clear that no numerical (i.e. probabilistic) case would be provided, so that, since the consequences of RPV failure could be serious, the 'special case procedure' of NII Safety Principle 27 (ref. 12) would need to be followed.

9.2 Concern for failure of the vessel arises not only from the fact that rupture of the vessel may produce a loss-of-coolant accident (LOCA) in excess of the design basis for the emergency core cooling system (ECCS) but may simultaneously give rise to missiles which could damage other protection or safeguarding systems, including the containment. The safety case for the RPV is contained in part in Chapter 3 but mainly in Chapter 5 of the PCSR.

9.3 The special case procedure requires detailed examination of all the scientific and technical factors which are relevant. As input to this process, and in addition to the PCSR and its supporting reports, the Inspectorate has reviewed the first (ref. 8) and second (ref. 25) reports of the study group chaired by Dr Walter Marshall (LWRSG). In this connection, it is worth noting that the CEGB has undertaken to implement the recommendations of the second report. In addition, the Inspectorate has sought advice on specific questions relevant to RPV integrity from the Task Force on Fracture, from Roentgen Technische Dienst and from R L Cloud Associates. Discussions on topics of mutual interest have been held with many bodies overseas, including material suppliers, RPV fabricators, research organisations and regulatory bodies.

Design

Vessel style

9.4 Direct comparison between the Trojan RPV which the Inspectorate examined in the generic review and the style of RPV incorporated in the Sizewell B proposals shows many differences, most to the advantage of the Sizewell B RPV.

9.5 Whereas the Trojan RPV was made mainly from plate, with forgings being used only for the vessel and head flanges and the inlet and outlet nozzles, the Sizewell B style of vessel is composed of ring forgings throughout, with the possible exception of the 'dutchmen' to form the top and bottom heads which may be forged from plate. This ensures that no welds (which are generally accepted to be the most likely source of defects) will be oriented to carry hoop stress. Since the membrane stress from pressure in the hoop direction is approximately twice its value in the longitudinal direction, the increase in integrity is clear. Moreover, the elimination of longitudinal welds has reduced the main seam weld length by some 40%, further enhancing integrity.

9.6 Furthermore, by selection of the forging for the central strake at the limits of length commercially available, the closing welds are well removed from the region of highest irradiation damage. It is estimated that the welds will be exposed to an integrated dose one order of magnitude lower than that of the 'belt-line' material adjacent to the reactor core. This goes some way to offset some of the concerns expressed below in terms of materials specifications.

9.7 In considering the layout of the biological shield around the RPV, it is clear that a large gap would permit the possibility of access for in-service inspection from the outside of the vessel. However, the penalty of a wide cavity in terms of increased dose rate from radiation streaming was argued by the CEGB in support of its decision to adopt a narrow cavity. Thus it arises that inspection from outside of the cylindrical part of the vessel will be extremely difficult. The Inspectorate has accepted this feature of the design, but has counselled the provision of access to permit supplementary examination from the outside of the nozzle-to-shell welds should it be necessary.

9.8 In the generic review, considerable support was expressed for the large forging concept and for set-on nozzle welds. Whilst the Inspectorate's views on the benefits of such concepts have not changed, it has accepted the CEGB argument that for this first UK PWR the absence of general fabrication experience with such a concept for a Westinghouse 4-loop PWR might have unacceptably narrowed the choice of fabricator. Hence, it has, in general, accepted the Sizewell B proposal.

Codes and standards

9.9 The ASME Boiler and Pressure Vessel Code is one of the major planks on which the platform of PWR vessel technology is built. Reliance upon the provision of Section III (Nuclear vessels) and Section XI (In-service inspection) constitutes a major part of the safety case presented in the PCSR. The strengths of the ASME Code are quite widely understood, and include:

(a) Design by analysis;

(b) Fatigue assessment;

(c) Brittle-fracture-safe operation assured by conservatively-set heat-up and cooldown rates (Appendix G);

(d) Comprehensive QA procedures required to ensure code compliance, supported by audits by code committee representatives on first authorisation and re-authorisation to use N-stamp;

(e) In-service inspection (including volumetric examination of weld zones) imposed as mandatory;

(f) Frequent revisions (Summer and Winter Addenda) and periodic re-writes to keep the code in contact with developments in the technology;

(g) Code development supported by a large body of knowledgeable engineers and scientists.

The weaknesses of the code are less well understood, but stem mainly from the fact that it represents a consensus of the industry, and accordingly may not even represent the best that is reasonably practicable far less the best that is achievable.

9.10 In the Inspectorate's review, it has been concluded that Section III of the ASME Code provides an acceptable minimum standard upon which it expects to see the CEGB impose additional requirements in specific areas. The most important of these includes the provision of fracture analysis (and supporting detailed stress analysis) of all important sections of the RPV.

Stress analysis

9.11 In the generic review, concern was expressed for shortcomings evident in the stress report for the Trojan RPV. In the interim there has been a great deal of development, notably in the area of finite element methods. Nowadays the difficulties of modelling the thin clad layer, referred to in the generic review, can now be overcome using sub-structuring or 'super-elements' as they are sometimes called.

9.12 The analysis presented in the several supporting reports to the PCSR provide a substantial improvement on some parts of the Trojan stress report. However, the Inspectorate has expressed reservations about the use of two-dimensional axisymmetric representations which may underpredict stress intensities in situations where substantial geometrical or thermal asymmetry or discontinuity is present. We shall be seeking further resolution of this question since it can significantly affect the 'margin of safety' between the critical and detectable defect sizes.

9.13 In discussion with the CEGB, the Inspectorate has made it clear that comprehensive validation of all computer programs used in support of the safety case will be required. For many of the Westinghouse proprietary programs examined in the generic review, NII is satisfied at this stage with the extent of the validation provided. However, the CEGB has indicated that it proposes to use other programs, some in the open literature, some proprietary, and these should also be validated if their use is envisaged in support of the licence application.

9.14 In Section 4 of the second LWRSG Report the recommendation is made that stress reports should be subject to independent checking. The Inspectorate considers that, since this in no way conflicts with the third-party review requirements of ASME III, it is a useful way of enhancing confidence. It is extremely important however, that any checks should be carried out using validated computer programs and qualified, experienced personnel.

Manufacture

Materials

9.15 There is little doubt that the past decade has seen considerable development in the grades of steel used for LWR pressure vessels, namely SA533B plate and SA508 Class 3 forgings. Realisation of the important role played by many of the impurities and 'tramp' elements in enhancing irradiation damage has accelerated the development of extremely 'clean' steels, low in copper, sulphur, phosphorus, tin, antimony and arsenic. Realisation of the importance of other elements, such as carbon, chromium, manganese and molybdenum, in controlling the tendency of welds or heat-affected zones (HAZ) to crack, has led to further controls on these elements being imposed. Recent irradiation experience indicates a synergistic effect of copper and nickel which may require additional controls on nickel, especially in welds.

9.16 In various supplementary documents to the PCSR the CEGB has undertaken to impose tighter limits on many elements than are imposed in the ASME/ASTM specifications. The Inspectorate considers that still tighter limits than those proposed are desirable and reasonably practicable, and will be pursuing this.

9.17 The Materials Property Council Survey (ref. 26) showed that 22 out of the 25 vessels in the survey had their integrity limited by the toughness of weld metal, and not by parent material. This clearly indicates the need to improve the controls imposed by ASME on start-of-life mechanical properties of weld metal by improving compositional control.

9.18 The choices of steelmaking, forging and heat treatment processes as well as of inspection techniques can each be crucial to the quality of the product. As yet, the Inspectorate has no clear indication of what is intended and this makes it difficult to conduct any assessment of the integrity of the vessel in these areas.

Fabrication

9.19 One of the essential characteristics of the SA533B and SA508 Class 3 materials is that strength and high toughness are achieved at the expense of weldability. It is well known that, in thick sections, these carbon-manganese low-alloy steels require a high degree of pre-heat and post-weld heat treatment to accompany all welding operations, including deposition of clad, if hydrogen cracking is to be avoided.

9.20 Since the text of the PCSR contains only general statements relating to intentions to select an experienced fabricator, the Inspectorate is unable to express a view about the acceptability of what the CEGB may propose. It has certainly made it plain that it would regard possession of a current ASME N-stamp as the minimum reasonable qualification for the fabricator and material supplier.

9.21 Moreover, although the CEGB has recently provided some preliminary information on the role of the Authorised Inspection Agency, this information is not sufficiently detailed as to permit an understanding of the respective roles of the various departments of CEGB, of units within NNC or of the fabricator in relation to the Authorised Inspection Agency. Such relationships are crucial to the achievement of properly cognisant control of the selection and qualification of materials, processes and personnel, and the necessary information will be required well in advance of arrangements for the Authorised Inspection Agency being made.

9.22 Again, at the component level the Inspectorate has at present no information on what quality assurance procedures will be applied. Such uncertainty means that it cannot yet be satisfied that the required degree of excellence will be achieved in practice.

Fracture analysis

9.23 In the generic review, the Inspectorate indicated that, in addition to compliance with the ASME III Code in terms of demonstrating freedom from rupture, collapse or gross distortion, the safety case should include fracture analysis of the vessel. This view is supported by the LWRSG's First and Second Reports.

9.24 In order that the Inspectorate should have access to informed and independent advice on the subject of fracture, a Task Force on Fracture was set up. This task force is led by Professor C E Turner of Imperial College, University of London, and includes a number of specialists from the universities and the Welding Institute. It is supported by a full-time research assistant.

9.25 One of the first issues considered by the Task Force on Fracture was the evidence given by W E Cooper of Teledyne Materials Research and J F Enrietto of Westinghouse to the Select Committee on Energy (ref. 27), in support of a 'leak-before-break' case (that is, that leakage would prevent fast fracture because any defect would penetrate through the wall before it achieved critical size). The task force concluded that no reliable case for 'leak-before-break' could be made either at the beltline or in the nozzle region. The Inspectorate is satisfied, therefore, that the CEGB has not put forward 'leak-before-break' arguments in the PCSR.

9.26 In terms of the material toughness assumed in the supporting reports to the PCSR, it is noted that the CEGB has assumed a high upper-self toughness, low nil-ductility transition (NDT) temperature, and a modest NDT shift with no reduction of upper shelf at end-of-life. It is difficult to reconcile these assumptions with the uncertainties expressed in terms of materials specifications, outlined in para 9.15 *et seq*. The Inspectorate considers that it would be prudent to assume a shift in NDT of, say, 50 °C to allow for the combined lifetime effects of irradiation embrittlement, ageing and strain ageing. It also considers the CEGB assumption of no loss in upper-shelf toughness to be unreasonable in the absence of any surveillance data for the materials under consideration.

9.27 In terms of toughness measurements the Inspectorate notes and supports the CEGB specification that toughness measurements should be made over the whole temperature range of interest rather than that this property should be inferred from other (Charpy) measurements. This policy should be extended to the area of surveillance specimens. The Inspectorate has considerable concern that many of the measurements included in the reference data set (ref. 28) are derived from small specimens which may, in terms of both size and geometry effects, overpredict toughness. The clear understanding from the Inspectorate's and others' research programmes (for example, ref. 29) is that there is a marked effect of specimen size and geometry both in terms of initiation toughness and the slope of the resistance curve, with very large specimens tending to illustrate lower-bound initiation toughness and relatively flatter R-curves.

9.28 It is also clear from several programmes of work that the behaviour of model vessels can only be satisfactorily described if lower-bound toughness data are used. Thus the proposal from the CEGB to use mean toughness data for assessment of Conditions III and IV events is regarded as a possible departure from the realistic behaviour exhibited by large-scale tests, not as the removal of unnecessary conservatism, which is how it is regarded by CEGB.

9.29 Whilst the CEGB proposal to adopt the methodology now generally known as the R6 methodology addresses the generic review concern that in certain instances evaluation based on linear-elastic fracture mechanics (LEFM) may not be conservative due to the

possibility of plastic collapse of the ligament ahead of a crack which is subcritical in LEFM terms, the Inspectorate has a number of reservations about the methodology. Of these the most important relate to inadequacies in validation (particularly in terms of the treatment of residual and thermal stresses) and the use of net section stresses to assess limit loading.

9.30 In addition to the reservation described above, the Inspectorate has reservations about the use of resistance-curve (R-curve) methodology for Condition III and IV events without corresponding assessment of limit load. In principle, the R-curve concept, in which some small amount of stable crack growth produces an increase in toughness but a corresponding increase in net section stress, seems implicitly to necessitate limit load assessment to ensure against collapse of the ligament ahead of the (stable) crack.

9.31 The Inspectorate shares the reservations of the LWRSG (ref. 25) about the value of proof pressure testing. Some claims for benefits from over-pressure tests have been advanced in LEFM terms in the past, but the Inspectorate currently sees little merit in such arguments and will wish to review with close attention the eventual proposals in this regard.

9.32 The Inspectorate supports the recommendation of the LWRSG that consideration should be given to increasing the cladding thickness beyond the minimum currently specified to provide further insulation against the more severe thermal transients and hence increase the size of defect which could become critical.

Inspection

9.33 It is accepted that production of a totally defect-free RPV is impracticable. It is therefore essential that inspection processes be applied which will provide adequate knowledge of the extent, location and size of all defects present, that are or could become significant in terms of RPV integrity, to allow adjudication on their acceptability. The processes available for volumetric examination for buried defects are restricted in practice to radiography and ultrasonics. Of these only ultrasonics has adequate capability for characterisation of crack-like defects in terms of size and location.

9.34 The PISC trials (ref. 30) confirmed many of the reservations which the Inspectorate expressed in the generic review about the adequacy of techniques which complied with ASME XI, but demonstrated that other techniques, including some modified from ASME XI procedures, could achieve enhanced results.

9.35 In order to have access to informed but independent advice in the general area of inspection, especially with reference to ultrasonic inspection, the Inspectorate has retained the services of Roentgen Technische Dienst as consultants. This firm has been deeply involved both in underlying research and in the application of ultrasonics to LWR vessel inspections in Holland, Belgium and the German Federal Republic.

9.36 It is clear that there is no single technique which is capable of detecting and sizing all defects equally, regardless of size, location and orientation. Given this it is particularly encouraging to have the CEGB's commitment that in-process inspections will be carried out in such a way as to provide redundancy and diversity in terms of operator and technique.

9.37 The Defect Detection Trials (DDT) organised by the UKAEA, Risley, are currently in progress. Preliminary results from inspection of the first two plates indicate very impressive performance from three UK teams each using a different technique. Whilst the Inspectorate has reservations concerning the differences between the DDT specimens and a real vessel, it considered that these results support its views on the benefits to be derived from multiple examinations by diverse techniques.

9.38 The Inspectorate also sees substantial benefit from the commitment now offered by the CEGB that all inspection techniques, equipment and personnel will be validated in a Validation Centre which is independent of the CEGB, the NNC, the Authorised Inspection Agency, the fabricator and the material supplier.

9.39 The Inspectorate sees an urgent need to establish acceptance standards for inspection, and considers that more stringent standards than those summarised in Figure 3.3 – 3 of the PCSR are appropriate for in-process inspections, whereas some fitness-for-purpose criteria are probably more appropriate to in-service inspection.

9.40 Although not offered by the CEGB in the PCSR, there is substantial merit in machining or grinding the clad to a plane (though not necessarily fine) finish. Both visual examination for surface cracks and ultrasonic examination will be enhanced thereby, especially examination by 70 ° longitudinal probes for underclad cracks. Such provision of ground or machined clad should be considered in conjunction with the LWRSG recommendation to consider increasing the clad thickness to insulate against the more severe thermal transients, since this would only appear practicable if multi-layer cladding were adopted.

9.41 The Inspectorate is in general agreement with the sense of the CEGB case that in-process inspection (where access is available from both inside and outside of the vessel, where seam welds can be inspected prior to clad overlay and where multiple, diverse inspections are reasonably practicable) contributes more to vessel integrity than in-service inspection.

9.42 In the generic review the Inspectorate expressed concern about the possibility that cracks, emanating from the partial penetration welds attaching the in-core instrumentation nozzles to the bottom head,

might give rise to a rupture in the bottom head of the vessel, and indicated its requirement that the ECCS be designed to cope with such a breach. The CEGB has responded to the concern that radial cracks might link up across the ligaments of three adjacent penetrations to form a triangular 'flap', by investigating the feasibility of ultrasonic inspection of the ligaments in-service and undertaking that such inspection will be provided should it be necessary. Once such inspection is offered the doubts then reduce to breach sizes which, on present analysis, appear well within the capability of the existing ECCS.

Operation

Overcooling accidents

9.43 Considerable attention has been focused on a class of events known as 'overcooling accidents' in which rapid cooldown of the vessel produces high thermal stress and may be followed by repressurisation by the ECCS whilst the vessel is at low temperature. The most obvious example is rupture of a steam line.

9.44 Whilst the fracture analyses presented in the PCSR demonstrate apparently satisfactory response on the vessel to steam line break and LOCA, the reservations noted earlier in this section may reduce the calculated margins.

9.45 There are a number of options which may be exercised to give further confidence in RPV integrity. Some of these relate to improving the inherent resistance of the vessel to thermal transients and others relate to reducing the frequency and mitigating the effects on the RPV of such events. Neither option has yet been discussed by the CEGB, although the Inspectorate would expect some response in the course of its implementing the LWRSG recommendations.

9.46 There is particular promise in the suggestion that the integrated protection system (IPS) could be arranged to hold the vessel in a 'fracture-safe' envelope, to prevent re-pressurisation at any temperature below the onset of 'upper shelf' behaviour. As yet, however, the CEGB has not put forward any formal proposals for this.

Transient specification

9.47 One of the important issues which has relevance throughout the safety case for the RPV is the frequency of transients and faults, and the consequent pressure-temperature relationship in the coolant circuit. In terms of the frequency of occurrence the Inspectorate would expect differences in operating practices between the USA and the UK to have impact, and some differences can be seen between US and UK equipment specifications in this respect. In terms of pressure-temperature time-histories, differences in operating practices, in regulatory assumptions (for example, the 30-minute rule) and in system design can also be expected to have considerable impact.

9.48 The Inspectorate would expect the CEGB to carry out a comprehensive and systematic review of the frequency and course of transients affecting the vessel to augment the limited review so far presented which examines some of the 'limiting' conditions only. This review should be carried out before a decision is made on licensing.

Conclusions

9.49 In considering the integrity of the reactor pressure vessel, it is clear that much valuable progress has been made since the generic review. However, the Inspectorate is not yet satisfied with the case as put forward in the PCSR, and has identified a number of shortcomings which should be rectified and more information which should be provided before it could offer a favourable judgement on the CEGB claim that failure of the RPV is 'incredible'.

9.50 The Inspectorate would wish to see improvements in the specification for the RPV so as to impose sufficient controls on materials and processes to give assurance regarding the properties postulated in the fracture analysis.

9.51 An improved stress analysis has been presented and this is generally acceptable, though there is a concern that the two-dimensional axisymmetric representations generally used may underpredict stress intensification due to geometric and thermal asymmetry or discontinuity.

9.52 Again, whilst an extensive fracture analysis is presented in the supporting reports, the Inspectorate has a number of reservations both about the fracture methodology adopted and about the postulated material properties.

9.53 Whilst the preliminary results of the inspections of the first two plates in the Defect Detection Trials (DDT) organised by UKAEA, Risley, and the commitments by the CEGB to multiple diverse in-process inspections and to independent validation of all ultrasonic techniques, equipment and personnel, give enhanced confidence, the Inspectorate wishes to see the margin claimed between critical and detectable defects better justified.

9.54 The Inspectorate wishes to be satisfied that all reasonably practicable steps have been taken in the design of the integrated protection system (IPS) to control and mitigate the effects of events leading to overcooling or to pressurisation when cold. It considers that the vessel should be maintained 'on the upper shelf' toughness regime during the highly stressed parts of any transient.

9.55 Finally, more information is required on the QA procedures relevant to the RPV to give assurance

that the level of integrity sought will be achieved in practice.

9.56 Whilst these shortcomings inhibit the Inspectorate's acceptance of the safety case as presented in the PCSR, it believes nevertheless that there are no reservations which cannot be overcome and that an acceptable safety case can be made, based on existing technology. The Inspectorate expects to be satisfied about all relevant items before the CEGB is committed in regard to the RPV, and requires an acceptable case to be provided before a decision on licensing is made.

10 General pressure circuit integrity

Introduction

10.1 In this section the safety case submitted by the CEGB for the more important pressure-bearing components (excluding, of course, the reactor pressure vessel, covered in the previous section) is examined. The choice of components for inclusion in the section is determined either by the CEGB submitting an 'incredibility-of-failure' argument, or by the existence of concerns not satisfactorily dealt with in the PCSR.

Reactor coolant loop piping

10.2 The licensing requirements imposed on PWR in the USA, and the design basis adopted by the CEGB, necessitate protection against the consequences of ruptures in the reactor coolant loop and connected reactor coolant system pipework of up to and including double-ended guillotine break of the largest coolant loop pipe. Since this constitutes the design basis for loss-of-coolant accidents (LOCA) there is, perhaps, less concern for the integrity of coolant loop piping, in that there is not the same need to show that the probability of failure is so very remote, as is the case for those pressurised components whose failure is deemed by the CEGB to be 'incredible'. Nonetheless, since LOCAs represent a potential radiological risk to the public and operating staff, the Inspectorate expects to be satisfied that all reasonably practicable steps have been taken to ensure that the incidence of ruptures in coolant loop piping is minimised and that the likelihood of systems propagating to the extent that the design basis is exceeded is as small as is reasonably practicable. The safety case for reactor coolant loop piping is presented in part in Chapter 3 but mainly in Chapter 5 of the PCSR.

10.3 One of the major bases for coolant loop integrity advanced in the PCSR is design, manufacture, test and inspection to the requirements of ASME III and ASME XI. This was accepted, subject to a number of reservations, in the generic review and this remains the Inspectorate's view.

10.4 The austenitic stainless steel employed for the construction of the coolant loop is a material of such high toughness combined with high workhardening capacity that the concepts of linear-elastic fracture mechanics are inappropriate. Thus the Inspectorate generally supports the views developing in the USA that assessment of limit loading and of tearing instability is a more appropriate methodology for assessment of coolant loop piping. It does, however, have a reservation in terms of the relatively low initiation toughness and relatively flat resistance curve occasionally measured in weld material, and will require proof that high toughness is available in the welds.

10.5 A further concern related to welds is the tendency of unstabilised stainless steels to become sensitised to stress corrosion by the heat cycle during welding. The main response in the PCSR is to control the carbon and, subject to the Inspectorate being provided with adequate evidence, this should be an acceptable approach.

10.6 A wide range of alternative source materials for the construction of the coolant loop piping is put forward in the PCSR. Of these, the Inspectorate has reservations on the acceptability of centrifugally cast pipe since the coarse-grained dendritic structure of this material can seriously impair ultrasonic examination. From this point of view use of fine-grained, close-die forged pipe is to be preferred. However, no specific proposals from the CEGB have, as yet, been received.

10.7 The Inspectorate examined the analytical methods employed for stress analysis (including dynamic analysis) of the reactor coolant system in the generic review and found the methodology generally acceptable. In discussion it was understood that the NNC will perform the overall system analysis for Sizewell B on behalf of the CEGB and that it will extend the usual Westinghouse system model to represent shell mode behaviour of the reactor vessel. This approach appears acceptable as a basis for licensing.

10.8 The Inspectorate has been unable to consider much pertinent matter because of the lack of details so far presented in respect of material, fabrication process and inspection technique. The Inspectorate does, however, accept and will wish to see implemented, the CEGB's general commitment to install some form of permanent guide rails at each loop weld to permit remote automatic scanning of welds and thereby reduce the radiation exposure received by operators during ultrasonic in-service inspection.

10.9 Although the case for reactor coolant loop integrity provided by the CEGB responds to many of the reservations raised in the generic review, the Inspectorate will need further information beyond that contained in the PCSR to allow it to judge that the risk of LOCA has been minimised to the extent of reasonable practicability. The safety case should provide at least a specification, reasonably firm information relating to quality assurance, and proposals for in-process and in-service inspection.

Reactor coolant pumps

10.10 The pump bowl (that is, the pressure-retaining component) of the reactor coolant pump (RCP) is one of those components, identified in Section 2.5.1.4 of the PCSR, whose failure is deemed to be 'incredible'. Moreover, no numerical (probabilistic) case has been advanced so that it is necessary to apply the special case procedure of NII Safety Principle 27. This requires a special examination of all the relevant technical and scientific factors.

10.11 As in the case of other pressure-retaining components in the reactor coolant system, heavy reliance is placed on the provisions of the ASME III and ASME XI Codes to ensure high integrity. As indicated in the Inspectorate's generic review, which examined the Model 93A1 pump (which is very similar to the design of the Model 100D proposed for Sizewell B service), such proposals are generally satisfactory. However, the Inspectorate wishes to see in-process inspection by ultrasonics in addition to the code inspection by radiography, and hence expects emphasis to be placed on achieving a grain-refined condition prior to inspection for acceptance. It is not yet clear that the CEGB's proposals will satisfy this requirement.

10.12 The Inspectorate has little concern for failure of the pump bowl either by low-energy fracture or by ductile crack extension; rather it believes that plastic collapse of the ligament ahead of a growing crack is probably limiting. This, of course, assumes that corresponding toughness is achieved in welds as is achieved in the parent material. Such an assumption could easily be invalidated, for example if electro-slag welding were adopted.

10.13 Further information is required on materials, fabrication, in-process and in-service inspection, before the Inspectorate can be satisfied that an adequate safety case to justify the CEGB assumption that coolant pump bowl failure is 'incredible' has been made. Given that this information is provided, it is the Inspectorate's view that a satisfactory safety case can be made based on current technology. The case should be made prior to a decision on licensing.

10.14 In its generic review the Inspectorate assessed the safety case for the pump flywheel, and accepted the stress and fracture analysis presented. However, these analyses and that supporting the PCSR depend on assurance that the pump remains energised for the first 20 seconds after a LOCA (to prevent overspeeding by regenerative braking of the motor, and hence to avoid bursting of the flywheel). The Inspectorate has identified a weakness in this case (in that it depends on timing circuits in the generator energiser controls which are not of protection grade) and it will expect a different case to be made prior to a decision on licensing.

Pressuriser

10.15 The pressuriser is one of those components, identified in Section 2.5.1.4 of the PCSR, whose failure is deemed to be 'incredible'. Since the consequences of failure may be serious, and in the absence of any numerical case, the special case procedure of Safety Principle 27 is applied.

10.16 The case presented in Chapters 3 and 5 of the PCSR relies almost entirely on the well-proven nature of the Westinghouse pressuriser, designed, manufactured, inspected and tested to ASME III and ASME XI Codes. Whilst this gives assurance of integrity beyond that of the generality of pressure vessels, the Inspectorate has indicated to the CEGB that substantiation of the 'incredibility'-of-failure case will require supporting stress and fracture analysis of the same order, and comprehensive specification in terms of materials and processes of the same order of detail and refinement, as for the reactor pressure vessel. The CEGB has given a commitment to provide this information and the Inspectorate expects the case to be provided to its satisfaction prior to a decision on licensing.

Steam generators

General

10.17 The safety case for the steam generators is contained partly in Chapter 3, but mainly in Chapter 5 of the PCSR. The steam generators may be regarded as three components:

the channel head

the tubes

the shell and internals

Channel head

10.18 The channel head, including the tube plate, is part of the primary circuit boundary, and is one of those components identified in Section 2.5.1.4 of the PCSR, whose failure is deemed 'incredible'.

10.19 From the stress and fatigue analyses assessed in the generic review the Inspectorate is satisfied that an acceptable safety case can be made for the channel head although such a case has not yet been put forward for the Model F steam generator. In making that case the CEGB will need to examine the feasibility of in-service inspection of the welds attaching the divider plate to the channel head and tube-plate to address the concern expressed in the generic review.

10.20 The eventual safety case for Sizewell B should include a comprehensive specification, stress and fracture analysis, and proposals for in-process and in-service inspection. In general, this should be of the

same order of detail and refinement as the case for the RPV and the Inspectorate would expect to see such a case, in sufficient detail as to allow it to determine that it will be acceptable, prior to a decision on licensing.

Tubes

10.21 The steam generator tubes constitute part of the primary circuit boundary; they also constitute part of the primary containment, since the main steam lines penetrate the primary containment without facilities for isolation at the containment boundary (because the safety valves are located outside the containment).

10.22 There has been a long history of steam generator tube problems with PWRs (refs. 31, 32, 33, 34). Whilst the present design basis adopted in the USA is double-ended rupture of a single steam generator tube, and the policy of steam generator tube inspections and plugging (refs. 35, 36) has been defined, it is clear from four incidents in which the leak rate exceeded the specified limits that this design basis is in question. Three of these incidents are reported in NRC's review (ref. 37), the other is the recent incident at the R E Ginna plant.

10.23 In considering the features of the secondary circuit for Sizewell and of the Westinghouse Model F steam generator intended to respond to the denting, stress corrosion and sludge pile problems which have occurred in the past, the Inspectorate is inclined to believe, from the substantial experimental and analytical evidence offered, though lacking actual operating experience, that the measures proposed in the PCSR are likely to ameliorate these problems substantially, if they do not eliminate them entirely.

10.24 The Inspectorate has one area of concern, however, for which it has not yet been provided with the measure of assurance it seeks. This relates to the possibility of circumferentially orientated defects arising in the crevice at the top of the tube-plate. One of the design features of the Model F steam generator intended to respond to previous crevice corrosion problems is the adoption of 'fully' hydraulically-expanded tubes. This process leaves a crevice of average depth around 6 mm at the top of the tube-plate. None of the experimental evidence presented by the CEGB relates to long-term tests of model boilers containing a crevice with an adjacent zone of cold work. The lesson has been learned from previous reactor systems that short-term corrosion data do not give adequate assurance where a safety issue is involved. The Inspectorate is therefore concerned for the possibility of inter-granular attack (IGA) in the crevice at the top of the tube-plate.

10.25 The experience of two independent inspections of the San Onofre and Ginna steam generators (refs. 38, 39), suggests that the most modern multi-frequency eddy current testing (ECT) techniques are not capable of identifying IGA in the crevice even when it has penetrated 70% of the wall. One explanation offered (ref. 39) is that the IGA in the specimens removed from Ginna is tightly-facetted and not accompanied by the 'fingers' of stress corrosion characteristic of laboratory-corroded specimens.

10.26 If IGA occurs in the crevice at the top of the tube-plate and cannot be detected and accurately sized using multi-frequency ECT, then it is difficult to see how the criteria of Regulatory Guides 1.83 and 1.121, which form an integral part of the PCSR case, can be met. In such circumstances, the Inspectorate is concerned that there is a potential for multiple tube ruptures even in modest over-pressure transients (such as load rejection or turbine trip).

10.27 That such multiple failures of steam generator tubes can occur is demonstrated by the experiences of Point Beach, 1975, Surry, 1976, Prairie Island, 1979 and Ginna, 1982. Such events present the risk of a small-to-medium LOCA into a breached containment, and even if only a fraction of the activation products in the primary coolant is discharged, it is difficult to see how releases above an emergency reference level (ERL) could be avoided.

10.28 The Inspectorate has made its concerns known to the CEGB and has indicated that it needs to be satisfied either that IGA can be shown, e.g. by long-term test data in model boilers, not to be a problem, or that an inspection technique exists capable of reliably detecting IGA, prior to licensing. Until such information is provided, the Inspectorate can only conclude that a satisfactory safety case has not been made.

Shell and internals

10.29 The steam generator shell is one of those items, identified in Section 2.5.1.4 of the PCSR, whose failure is deemed to be 'incredible'. As in other such cases where the consequences of failure (particularly in terms of the potential to release a damaging missile) may be serious and no numerical case is offered to support this claim, the special case procedure is applied.

10.30 At an early stage in the discussions, the CEGB confirmed that the steam generator shell would be manufactured from SA508 Class 3 forgings, with the attendant advantages discussed under the reactor pressure vessel in Section 9 of this report. The CEGB has also confirmed that, although the steam generator shell is assigned Safety Class 2 under the rules of ASNI: N18.2, the design, manufacture, test and inspection of the shell will be carried out to ASME III Class 1 and in-service inspection will be carried out to ASME XI Class 1 rules.

10.31 Although the margin on critical versus detectable defect size appears small in the fracture analysis of the shell presented in the supporting reports, the Inspectorate is inclined to the view that this arises from a quite unnecessarily large degree of pessimism in the analysis and that this margin can be improved.

10.32 The Inspectorate has also been assured that means will be provided to inspect visually the corner at the inside of the shell/tube-plate to ensure that crud deposition is not occurring, under which conditions rapid corrosion could occur.

10.33 The response which the Inspectorate has so far received from the CEGB in answer to the generic review concern for the loads and stresses on the moisture separators and driers under steam line break accident loads is not acceptable, but the problem is amenable to solution and not urgent.

Primary component supports and restraints

10.34 The method of supporting the components of the primary circuit and the loop piping outlined in Chapter 5 of the PCSR is in all essentials identical to that of the Trojan plant examined in the generic review, hence the concerns expressed in the generic review are regarded as potentially valid for Sizewell B.

10.35 All primary component supports are included in the list of components identified in Section 2.5.1.4 of the PCSR, whose failure is deemed 'incredible'. Since failure of these components could lead directly to failure of other components whose failure is elsewhere deemed 'incredible', and in the absence of any numerical case, the special case procedure is again applied.

10.36 In the context of the reactor pressure vessel supports, the Inspectorate expressed concern about the lack of facility to inspect or replace the sliding surfaces, given that evidence had not been presented on the stability of the carbon steel cermet then proposed, under moderately high irradiation dose. In support of the Sizewell B design, the CEGB has indicated its intention to revert back to 'Graphair' material which comprises rods of graphite in a steel carrier. Data have been presented on irradiation stability, and if satisfactory long-term friction data are now presented it should be possible to withdraw any requirement for inspection or replacement facilities.

10.37 In the context of the hinge pins of the steam generator and reactor coolant pump support columns, the CEGB has not yet provided experimental evidence on the long-term capability of these components to perform their role as active components, nor has any capability to measure pin friction or check component deflections or inspect pin surface conditions been advanced in the PCSR or supporting reports. Since failure of these components could lead directly to a LOCA beyond the containment and ECCS design bases the Inspectorate considers this to be a serious concern.

10.38 In the context of the steam generator snubbers, the Inspectorate has not yet seen any response to its generic review concerns indicating the desirability of providing for rapid checking of reservoir oil levels, and for checking the slow spring rate.

10.39 The Inspectorate wishes to see provisions made to meet the above concerns before being able to agree that an acceptable safety case has been made.

10.40 In terms of pipe whip restraints on the primary loop piping the Inspectorate is generally satisfied with the provisions described.

Accumulators

10.41 The ECCS accumulators are included amongst those components identified in Section 2.5.1.4 of the PCSR, whose failure is deemed to be 'incredible'. As in other such cases, the special case procedure is applied.

10.42 A safety case for these components should contain specifications, stress and fracture analysis, and specific proposals for in-process and in-service inspection and QA. These are not at present included in either Chapter 3 or Chapter 5 of the PCSR.

10.43 The Inspectorate has advised the CEGB that it requires such a safety case, at an equivalent level of treatment to that supporting the reactor pressure vessel. Provided this information is forthcoming there seems no reason why a satisfactory case should not be made prior to a decision on licensing.

Main steam line 'no-break' zone

10.44 The length of main steam piping from the containment building to the restraint downstream of the main steam isolation valve (MSIV) is among those components, identified in Section 2.5.1.4 of the PCSR, whose failure is deemed to be 'incredible'. Such a position obviates the need for protection against the dynamic effects of pipe rupture (so that, for example, no jet impingement shields are provided between steam lines). Again, the special case procedure is applied.

10.45 In Chapters 3 and 10 of the PCSR it is proposed that this section of pipe will be designed, manufactured, inspected and tested to the provision of ASME III Class 2 and ASME XI Class 2. In addition the CEGB has offered in-service inspection of all welds in the no-break zone. The Inspectorate also requires assurance of the integrity of the MSIV body, and of the highly discontinuous safety valve header and its supports, since these are as important as the welds in the pipe.

10.46 The Inspectorate has informed the CEGB that it requires a specification, stress and fracture analysis and proposals for in-service inspection to standards comparable to ASME III Class 1 and ASME XI Class

1. This information should be received and a satisfactory case made prior to a decision on licensing.

Reactor internals and core

10.47 In Section 2.5.1.4 of the PCSR gross failure of the reactor internals is claimed to be 'incredible'. This is more precisely defined in Section 5.4, where it is claimed that gross failure of the internals, in a manner which would result in loss of coolable geometry in the core or such as to prevent insertion of control rod assemblies when necessary, is deemed 'incredible'. In the absence of any numerical case, the special case procedure is applied.

10.48 In the Inspectorate's generic review a number of concerns about the technique of modelling the internals and core response to fluid forces during LOCA were raised, and it was concluded then that the case for preservation of coolable geometry in the core in a LOCA had not been made. In supporting reports to the PCSR and in discussions with the CEGB, the main concerns have now been addressed. By and large the Inspectorate is satisfied, generally via generic analysis not necessarily fully representative of Sizewell B, that either the analysis for Sizewell B will satisfy its concern (e.g. representation of the internals shell mode behaviour) or else the issue has been shown to have only a trivial effect (e.g. use of uni-axial springs in the model).

10.49 In a component manufactured in stainless steel, low-energy fracture is unlikely to occur so fracture analysis is of little concern. The Inspectorate has already, through the generic review and the PCSR supporting reports, conducted a fairly extensive review of generic stress reports, which are reasonably representative of Sizewell B, and found them to be broadly satisfactory. Its remaining concerns, therefore, are for the specification and QA to be applied. In discussion, the CEGB has given the commitment that the specification and QA will be at least as rigorous as that imposed in the past by Westinghouse Pressurised Water Reactor Systems Division on their Pensacola Division. This may be acceptable, but the Inspectorate can only judge this when the relevant information is supplied.

10.50 The Inspectorate's conclusion in respect of 'incredibility' of internals failure is that a comprehensive safety case has not yet been made, and more information is required.

Valves

General

10.51 From extensive experience it is evident (refs. 40, 41) that a very small fraction of the total number of valves in a PWR contribute the preponderance of valve failures leading to reactor outage.

10.52 Valve failure is important to nuclear safety on two grounds. The first is that such failures can lead directly to loss of integrity in safety-related systems. The second is that maintenance of failed valves in many cases enhances radiation doses to exposed workers.

10.53 The inherent weaknesses in terms of design, specification, procurement, inspection, maintenance and testing of valves have been identified (ref. 40) as:

(a) Failure to treat the valve as an entity, i.e. the valve/powered operator/the duty/the environment, as a complex whole.

(b) Poor valve selection and procurement practice especially for key applications.

(c) Installed valve systems are often designed and supplied to one standard, but tested and evaluated to much stricter standards (occasionally to the point of exceeding state-of-the-art).

(d) Case-by-case utility response to problems provides little feed-back to architects, engineers, reactor vendors or valve suppliers.

10.54 Neither in Chapter 3 of the PCSR nor in the supporting reports has the Inspectorate yet been given an assurance that these problems will be avoided on the Sizewell B project. It wishes to be satisfied that an acceptable philosophy, at least, has been developed prior to a decision on licensing.

Main steam isolating valves (MSIV)

10.55 The MSIVs are an exception to the concerns expressed above, in that a strategy of valve qualification for them has been developed by the CEGB. These valves play a major role in steam line breaks (SLB) in reducing the degree of cooldown experienced by the RPV (discussed in Section 9). Since the flow in a steam line break (SLB) rises to several times the normal flow, the valves are required to close rapidly against this enhanced flow of high-density fluid (low steam quality due to overloading of the separators in the steam generator). The MSIV also constitutes a part of the 'no-break' zone discussed in paras 10.44 *et seq.*, which enhances concern for integrity of the valve body under SLB conditions.

10.56 It is considered impracticable to test the full-size valve under SLB conditions; the CEGB have therefore responded by undertaking that it will test similar valves at a number of scales to derive the fluid forces which will then be used in analysis of the full-size valve. Whilst the Inspectorate has not yet been provided with the detail, the proposal is judged acceptable in principle.

Conclusions

10.57 Although the case for the integrity of reactor coolant loop piping responds to many of the concerns raised in the generic review, the PCSR does not contain sufficient information to allow the Inspectorate to judge that the risk of LOCA has been minimised to a reasonably practicable extent. In particular it requires assurance that high toughness will be achieved and that an acceptably stringent specification will be imposed to achieve the necessary control of materials, fabrication and erection procedures. Such a case, in sufficient detail to allow the Inspectorate to judge its acceptability, should be made prior to a decision on licensing.

10.58 In regard to the integrity of other pressure circuit components (excluding the pressure vessel) the Inspectorate is not yet satisfied with the case made to support the claim of 'incredibility' of failure for a number of these, including the pump bowl, pressuriser, steam generator shell and head, ECCS accumulators and main steam line 'no-break' zone. There are also reservations about the case made for steam generator tube integrity. Apart from this latter, the concerns are related to the supply of information rather than to the technology available.

10.59 In regard to the integrity of primary component supports and restraints, the Inspectorate has noted a number of concerns which will need to be resolved before it can conclude that an adequate case to demonstrate 'incredibility' of failure has been made. Such a case is required to be made prior to licensing.

10.60 In regard to the integrity of the reactor internals and core, most of the issues raised in the generic review have been satisfactorily resolved. However, further information over and above that submitted in the PCSR and supporting reports will be required to demonstrate 'incredibility' of failure which might lead to loss of coolable geometry because of omissions, such as a specification and proposals for inspection and QA. The Inspectorate requires a suitable case, in sufficient detail to allow a judgement that it will be acceptable, prior to a decision on licensing.

10.61 In regard to the integrity of valves in general, the Inspectorate has indicated a number of shortcomings which have been identified from US PWR experience. Only in the case of main steam isolation valves have the principles of an acceptable strategy been presented. A similar comprehensive approach in relation to the other valves in the system will also be required.

11 Protection system and safety-related instrumentation

Introduction

11.1 The protection system, as defined in the NII's Safety Assessment Principles, consists of all equipment or systems which act directly in the event of faults to prevent damage that could lead to the escape of radioactivity. These systems perform a wide range of actions including shutdown and cooling of the reactor and services to ensure the integrity of the containment.

11.2 It should be noted that the terminology used in this report is that defined in the NII's principles and differs from that used in the PCSR. For example, in the PCSR 'protection system' has the narrower meaning of the equipment which initiates protective actions and excludes the associated plant items such as are required for reactor shutdown, cooling, etc.

11.3 Because of this vital duty in ensuring safety these systems should be specified, designed, constructed and operated to very high standards. The object of the assessment has been to determine whether the CEGB's intention as set out in the PCSR is acceptable. Some of the systems considered perform operational as well as protection functions. While the Inspectorate has assessed their function in the protection role the impact of their failure in normal operation has also been examined.

Protection system description

11.4 The protection system is described in Chapters 6, 7, 8, 9 and 10 of the PCSR and also in the safety analysis of Chapter 15. It consists of the following main elements:

(a) Fault detection and logic. This comprises a primary system consisting mainly but not entirely of the 'integrated protection system' and a secondary system of conventional design to give diversity against frequent fault situations.

(b) Plant systems, i.e. engineered safeguards, actuated by signals from the above system to give the protective actions required.

(c) Services for the above systems consisting of electrical power, compressed air supplies and cooling services.

11.5 The more significant changes made from the design reviewed in the Inspectorate's generic review are:

(a) the introduction of the integrated protection system (IPS) which potentially overcomes several of the previous objections. These include better redundancy, complete automation of the safety injection sequence and inclusion of control rod positions in trip functions;

(b) a general increase in redundancy from two trains to four trains. Notable exceptions to this are the low head safety injection and containment spray systems;

(c) additional features for protection of the RCS against over-pressure particularly when below full power temperature;

(d) a higher degree of diversity in most areas of the protection system to reduce susceptibility to common mode failure against frequent faults;

(e) the fast boron injection system to provide additional shutdown for steam break faults has been deleted and a different system to deal with ATWT situations added.

General protection system strategy

11.6 The general design basis for the protection system is not yet satisfactorily presented in the PCSR and the Inspectorate is unclear in a number of areas as to exactly what is intended. Many statements of intent are made with reservations such as 'as far as possible' or 'adequate' (defined in the PCSR as acceptable to the CEGB).

11.7 Although it is clear that there is a general intent to provide diversity for frequent initiating faults, and this is welcome, there is insufficient analysis to show that the systems described meet this intent. This is especially so in the case of fault detection, reactor tripping and services. In some cases it is clear that the intent has not been met, e.g. ATWT and the wide use of steam generator level measurement.

11.8 The fault analysis in the PCSR does not address many aspects of the protection initiation system and services on the grounds that they can easily be modified at a later stage. The Inspectorate is not able to accept this view without justification. Further, the analysis should include spurious actuation of individual protective actions and logical combinations of these to determine the consequences.

11.9 In many instances the fault studies described refer to the SNUPPS plant which does not have the integrated protection system fitted. Whilst the Inspectorate accepts that the IPS is likely to improve the protection, this situation results in an inadequate discussion of the specification for the IPS and omission of consideration of control rod banks being out of line.

11.10 Many issues of a fundamental nature were raised in the Inspectorate's generic review. These have been reviewed and several of them are found to be still outstanding in that they have not yet been dealt with in the safety case.

General design basis

11.11 A safety report should clearly identify and provide a comprehensive specification for systems which form part of the protection system since they are one of the prime factors in ensuring safety. Proper identification allows attention to be given to segregation, qualification, manufacture, operation and future modification. These systems are not sufficiently well identified in the PCSR and a schedule of all such systems has been requested.

11.12 The component safety classification adopted in the PCSR is insufficient as it stands since it would require the protection system and all safety-related instrumentation to be classified as Class 1E; the alternative being that it is classified as non-safety. A definition of what requirements are placed on Class 1E equipment by the CEGB should be provided.

11.13 To demonstrate that a minimum acceptable degree of redundancy is provided, all parts of a protection system providing a safety action should meet the single failure criterion, i.e. any single active or passive failure, unless acceptable alternative arguments are advanced. It is apparent that a number of systems or sub-systems do not meet this criterion, e.g. the refuelling water storage tank of the emergency core cooling system, and parts of the emergency charging and boron injection systems. The Inspectorate does not consider the single failure criterion proposed in the PCSR to be acceptable in that it does not adequately address passive failures. A systematic analysis is required to show that each system meets the single failure criterion and justification and agreement are required for exceptions.

11.14 The systems should be designed to perform the necessary safety functions following hazards such as seismic events, extremes of temperature, humidity and high winds with sufficient reliability. A prerequisite is that the structures containing the protection system must also withstand these hazards. To be consistent with the CEGB's design target risk for the station the required systems or sub-systems should be designed and qualified to remain operational following hazard events of magnitude corresponding to a very low probability (about 10^{-6}/year) event. The design intent indicated in the PCSR should go further than is presently proposed.

11.15 The redundant trains of the protection system and particularly their cabling should be so segregated that events such as fires and violent plant failures do not cause a loss of necessary functions. The cabling segregation arrangements described in the PCSR differ markedly from previous UK practice in that cabling is run in equipment rooms and that segregation in some areas relies on the operation of fire-fighting systems. The large number of systems and cables involved and the means for segregation proposed make this a very complex problem which the Inspectorate has not yet had time to examine properly. Following the Inspectorate's earlier comments on this topic CEGB issued a report (ref. 42) which there has not been time to examine in detail. Whilst the report indicates that the design proposed may be more acceptable in some respects than had been understood from the PCSR it also appears to confirm the Inspectorate's view on the complexity of the problem and the time that may be required to reach a conclusion. Hence the Inspectorate retains some reservations about the capacity of the present layout to accommodate the CEGB's strategy in some areas.

11.16 Technical specifications are the rules which are applied to operating the station and form part of a requirement placed on the licensee under the licence conditions. They should detail the action to be taken when protection system components are out of service and the limitations on the time of such outages. These are required at the PCSR stage for the major protection system components in order to assess the acceptability of protection systems and the segregation against hazards. They are not yet provided in the Sizewell B PCSR although an average allowance is made for maintenance and repair activities in reliability calculations.

11.17 The pressure differential transmitters employed widely as sensors in the protection system are of a type not previously employed for this duty in the UK. Most of them are located in the containment and are not therefore readily accessible for testing except during the annual shut down. Whilst the Inspectorate believes these sensors to be proven and adequately reliable it is not yet satisfied as to their possible failure modes. The Inspectorate has established that many of these sensors share common tappings and this it finds unacceptable, since any sensors claimed to be independent should have separate pressure tapping points on the plant. A further concern is that these sensors are not fully testable, i.e. for accuracy and response time, with the plant in operation. So far as reasonably practicable arrangements should be provided for fully testing sensors on a regular basis.

11.18 The Inspectorate will require evidence before licensing that the CEGB has established a satisfactory policy for the selection of valves to give adequate reliability and low maintenance.

11.19 In conclusion, before a decision on licensing the Inspectorate requires an improvement in the safety case in the following areas: classification of protection systems, application of the single failure criterion,

hazard design levels, segregation against fires and technical specifications for main plant items.

Fault situations

11.20 A fault table showing the situations to be protected against and the protective actions claimed is an essential part of the specification for protection systems. Such a table is given in the PCSR. The Inspectorate has not had time to analyse this table in sufficient depth but has noted a number of omissions relating to the protection system, including:

(a) No fault studies are presented for reactor operation with less than four coolant loops. In the absence of such studies, it may be necessary to prohibit operation with less than four loops operational.

(b) Failures of control and instrument supplies including the instrument air system are not included.

(c) The analysis of common mode failure of sensors ignores the possibility of stuck or out of tolerance transmitters.

(d) In the case of reactor coolant pump (RCP) flow faults, the RCP speed trip should not be claimed for one, two or three RCP failures. An alternative line of protection should be claimed.

(e) The analysis should include spurious actuation of each protective action and logical combinations including those caused by fires.

(f) The analysis does not take account of essential control room indicators required by an operator to meet technical specifications or deal with fault situations.

Protection initiating system

11.21 Two separate systems are provided to sense fault conditions and initiate the necessary parts of the protection system. These are called the primary, which acts for all faults, and the secondary, which provides diversity and acts only for frequent faults. The primary system consists mainly but not entirely of the 'integrated protection system'. In principle this aspect of the design meets the Inspectorate's requirements and is acceptable. However, there are a number of specific concerns which are brought out in the discussion which follows.

Integrated protection system (IPS)

11. 22 The IPS is a design of protection initiation system developed by Westinghouse in the USA using micro-processors to perform essentially the same functions as the old system reviewed in the generic review. Such a system has never been licensed for nuclear protection duties (but comparable systems are used in other critical applications such as aircraft control) and therefore merits very detailed investigation. An initial investigation was completed by the Inspectorate during 1981 and included a visit to the Westinghouse plant at Pittsburgh for discussions and viewing of a prototype. Also during this period the Inspectorate sent a representative, as an observer, to the meetings of a working group (ref. 43) consisting of CEGB and NNC personnel charged with the task of examining the system.

11.23 The acceptability of this system can be considered under three main headings:

(a) Is the technology of micro-processors acceptable for the duty of reactor protection?

The Inspectorate is able to give a clear affirmative to this question provided the technology is implemented in an acceptable manner. It is noted that protection against frequent faults is additionally provided by conventional means.

(b) Is the implementation of micro-processor technology in the Westinghouse IPS acceptable?

With the limited time and effort available the Inspectorate is not at present in a position to answer the question, nor is the information provided by the CEGB such as to demonstrate this. The development procedures at Westinghouse on both hardware and software appear to be what would be expected for such a system, although the prototype qualification tests and reliability calculations are not completed. Some functional modifications have been requested by the CEGB to meet the requirements for Sizewell B. The Inspectorate has identified to the CEGB some matters of concern which should be resolved before licensing. These include the need to specify the reliability of the IPS and the need for a thorough check of the software provided.

(c) Are the functions performed by the system acceptable?

Generally the IPS is required to perform similar functions to those of the system it supersedes. The adequacy of specific functions is covered later in this section. It is clear that many of the functions performed by the IPS offer better protection than the previous systems notably:

(i) the system has four redundant trains and generally operates on a two-out-of-four basis;

(ii) the departure from nucleate boiling (DNB) and linear power density trip functions now employ improved measurements of reactor power and axial neutron flux core distortions;

(iii) the RCP speed trip is a better indication of coolant flow than the RCP voltage trip it supersedes;

(iv) automatic control of the safety injection change-over to recirculation is provided.

11.24 The Inspectorate does however have some concerns about the functional aspects of the system, for example:

(a) The use of by-passes to cover sensor failures taken together with the two-zone segregation provided for the station does not give adequately reliable protection following a fire.

(b) The Inspectorate assumes that application of the by-passes will be compulsory following any sensor failure to preserve the intended logic. It wishes to know what limitations will be placed on the use of the by-pass system.

(c) There are reservations about the 'P Blocks' by-pass functions derived within the system which are used to by-pass functions not required by the operational state. An analysis of this system should be provided to show that common mode effects do not degrade the reliability of the protection provided.

(d) The Inspectorate remains to be convinced that the boron injection signal derived from control rod positions will be adequately reliable and diverse from possible causes of control rod failure. This concern on reliability arises from the fact that the signal is derived from information within the IPS which is not designed or intended to indicate individual control rod positions.

Other primary protection initiation

11.25 Several primary system initiation actions are not performed by the IPS and no details are given as to how or where they will be provided or what specification they will meet. These include power-operated relief valve (PORV) and block valve control, high and low frequency electrical supplies, containment purge closure on high radiation levels, and auxiliary feedwater flow controls.

Secondary protection initiation

11.26 Few details are given of this system beyond the variables monitored and the outputs required. It appears to be the intent not to apply by-passes to this system following failures of sensors in operation. Since the sensors in question can fail to danger the Inspectorate requires a clarification of the intention.

Conclusions

11.27 Whilst the systems in this sub-section are not specified in the detail expected in a PCSR, an acceptable safety case should be possible along the lines indicated.

11.28 The integrated protection system is a new system which has not previously been licensed for nuclear protection duties. Whilst the Inspectorate has no objection in principle to the technology employed, further work will be necessary to convince it on the concerns expressed.

Control and protection

11.29 In the generic review, the Inspectorate expressed concern at the use of common sensors for control and protection. It was concluded that sensors may be used for both functions provided the protection claimed against any particular control faults employed different sensors, i.e. another line of protection. It is noted that the fault table in the PCSR makes protection claims from common sensors although an analysis is provided on the effects of common mode failure of all such sensors. The latter analysis should be improved in that it does not include many sensor failure modes. The Inspectorate reiterates its previous conclusion that claims in the fault table for protective actions against control faults should not employ the same sensors. Further information is required on the means to be provided for signal selection to the various control loops and on the intended cabling routes and power supplies for these control loops.

11.30 There appears to be the potential for fires and power supply failures to give multiple control faults which are beyond the design basis of the protection system. These cases are not listed in the fault table nor are they analysed. The control rod control system can potentially give rise to faults which are not included in the fault listing, namely all rod run-out faults, multiple rod run-out faults, and faults with rod speeds greater than the specified control rate. The Inspectorate has requested further information to cover these points.

Interlocks

11.31 Interlocks are provided in various parts of the plant to prevent unprotected situations arising. These should form part of the protection system and should meet the necessary requirements.

11.32 The description of interlocks in the PCSR is not yet satisfactory and the Inspectorate requires a schedule of all interlocks which carry out a protective action to be provided, together with a specification and necessary justification including diversity, etc. The Inspectorate has identified to the CEGB the specific interlocks which it considers should be included and awaits its proposals.

Reactor trip system

11.33 It is necessary to trip the reactor for all fault situations which could lead to fuel damage or over-stressing of the reactor coolant circuit. For those faults predicted to occur frequently, a very high reliability is required and diverse means of protection should be provided.

11.34 In the design described in the PCSR, the control rod system is tripped for all faults by the IPS and for faults more frequent than 10^{-1}/year by the secondary trip system in addition. Thus failure to provide a trip signal for frequent faults is claimed to be 'incredible' and subject to detailed checking this is accepted. However the control rod system itself has no diversity and its reliability will be limited by common mode effects: this limit the Inspectorate would place at the lowest at 10^{-5} failures/demand. It follows that in order to meet the design target for fault sequences set by the CEGB it is at least necessary to show an alternative means of reactivity insertion for faults more frequent than 10^{-2}/year.

11.35 The argument offered is that the systems provided to cope with ATWT situations will provide this diversity. The systems required to operate are the pressure relief valves, trip of the two turbines, steam dump blocking, auxiliary feed system and the boron injection system. This argument is the same as that reviewed in the Inspectorate's generic review except that the boron injection system has been added to prevent the occurrence of boiling in the reactor hot legs and reduce reactivity during these faults.

11.36 The Inspectorate has a number of reservations about the argument presented:

(a) It is only shown that these systems are effective for faults more frequent that 10^{-1}/year whereas the requirement described above is for faults more frequent than 10^{-2}/year.

(b) The means for initiating the boron injection system are to detect within the IPS that two or more control rods have failed to drop following a reactor trip signal. Few details are presented of this system and the Inspectorate needs to be convinced that it will have acceptable reliability.

(c) For the ATWT argument to be acceptable, all the systems claimed to operate should be classified as part of the protection system and should be shown to meet the single failure criterion.

(d) The boron injection system requires the reactor coolant pumps to be running to inject the boron. However, the range of faults with frequency greater than 10^{-2}/year includes fault sequences involving the failure of coolant pumps.

11.37 The control rods are a well proven design. However the Inspectorate has the following reservations about the claims made for the rod system:

(a) To achieve a reliability of 10^{-5}/demand for the rod system it is necessary for the fault studies to consider that two have failed to drop, especially in the case of cooldown faults such as a steam line break.

(b) The control rod mechanisms are cooled by the reactor vessel head cooling system. If this cooling system fails it appears likely that the control rod mechanism temperature could exceed the temperature for which they are qualified, making seizure of the mechanisms a possibility.

(c) It appears possible for a control rod or rods to be disconnected from their drive mechanism. If so it would have a considerable effect on the DNB trip and on the shutdown margin available under the technical specifications.

11.38 A fast boron injection system was provided in the plant examined during the Inspectorate's generic review to supplement the control rods for steam line break faults. This has now been deleted and the Inspectorate will need to be convinced about the ability of the rod system to make the reactor sub-critical with two rods failed following a steam line break fault.

11.39 In conclusion, the Inspectorate has important reservations concerning the adequacy of the reactor tripping system. These mainly concern the adequacy of the ATWT argument for the required range of faults and it is not at present satisfied that the proposals so far put forward would give a successful outcome.

Pressure protection

11.40 Since failure of the reactor pressure vessel could lead to a serious release, protection against over-pressure should be to the same standard as the reactor protection. The protection provided against over-pressure conditions has been improved since the generic review. However, a more comprehensive analysis than is at present provided in the PCSR is needed to show that it is adequate to meet the requirements. Furthermore, when the pressure vessel is below full power temperature, the maximum allowable pressure is reduced but the new envelope of allowable conditions has not yet been established. This further information is required before a decision on licensing is made.

11.41 Due to the lack of a specification the Inspectorate has been unable to analyse the pressure protection in any detail. The following concerns have however been identified:

(a) the safety relief valves are not testable *in situ*, which will reduce their effective reliability;

(b) following isolation of the charging system the circuit can still be re-pressurised via the seal injection flow which is maintained;

(c) it is not clear whether the safety relief valve systems are adequate following a single failure;

(d) the power-operated relief valves (PORV) are liable to open when not required either through control failure or valve sticking following operation. This would give rise to small LOCA faults either as an initiating event or as part of another sequence. Block valves are provided to isolate such a faulty valve. Although not described it is understood that it is the CEGB's intention to fit automatic closure control to these block valves which if done in an acceptable manner should reduce the frequency of such occurrences to an acceptable level.

11.42 Further information will be required to remove the Inspectorate's concerns before it can be satisfied that an adequate case has been made in the PCSR for the pressure protection of the primary circuit.

Reactor heat removal systems

General

11.43 There is a frequent need for shutdown heat removal and therefore diversity is required. At pressure, decay heat is removed by evaporating feed water in the steam generators and discharging the steam to atmosphere via the safety relief valves or PORVs. When the temperature and pressure of the reactor coolant system have been sufficiently reduced the residual heat removal system is brought into operation. Diversity has been provided in the steam generator feed and venting routes in order to meet this objective but all high pressure heat removal routes depend upon primary to secondary heat transfer in the steam generators. Any mechanism which prevents such transfer leads to common mode failure of pressurised heat removal. The Inspectorate has identified the presence of non-condensible gases, e.g. nitrogen and hydrogen, leading to the loss of natural circulation, as possibly providing this mechanism. A further route for pressurised heat removal does exist, namely bleed and feed. This is discussed but not claimed in the PCSR. It is concluded that further consideration to improve the safety case for high pressure heat removal is required and, specifically, it is required that an alternative case such as bleed and feed be further examined.

11.44 At pressures and temperatures below 425 psig and 117 °C, decay heat is removed by a two-train, 100% redundant system—the residual heat removal system (RHRS). The two trains are segregated to ensure protection against internal and external hazards. In the Inspectorate's examination of the RHRS, areas have been identified where it considers the safety case should be improved. These are:

(a) Breach of the residual heat removal system (RHRS) leading to LOCA outside the containment. The RHRS possesses the largest connection to the primary circuit outside the containment. Failure of this pipework, not all of which is designed for full RCS pressure, could cause damage to the auxiliary building. Furthermore the auxiliary building is not designed to contain large volumes of highly active water. It is claimed that failure of the RHRS is precluded by its design and isolation provisions. This argument is supplemented by the claim that the system is pressurised and at high temperature for a very small period of time. The Inspectorate understands that changes are proposed to provide a third isolation valve in the suction line and to design the suction pipework up to and including this valve to withstand the full RCS pressure. This modification would be an improvement but does not fully deal with NII's concerns in that it does not consider:

(i) the diversity of interlocking arrangements to ensure that the suction valves cannot be opened above the system design pressure;

(ii) rupture of the RHRS due to stresses induced following normal actuation.

(b) The arrangement whereby the RHRS pumps interlink with the containment spray system.

(c) The approach to inspection and maintenance. The RHRS is a system which is required to be operational whenever irradiated fuel is in the reactor. During inspection or maintenance there may be no redundancy in the system. The reliability analysis depends upon strictly limiting the period of maintenance. Before this strategy can be accepted it should be shown that:

(i) The occasion and period chosen for maintenance is sufficiently small as not to unacceptably degrade the safety of the plant.

(ii) The equipment to be maintained can actually be maintained in the period given with allowance for subsequent testing/adjustment.

(iii) No action during the maintenance process will lead to an increased risk of a demand on or failure of the other half of this sytem.

Heat removal following LOCA

11.45 The mechanism for heat removal following a LOCA depends upon the size and type of breach. For any size of breach greater than 9.5 mm diameter, cold water is injected into the primary circuit from a single source—the refuelling water storage tank (RWST). It is claimed, without supporting evidence, that this inability to meet the single failure criterion will introduce a minimal additional risk. The Inspectorate has questioned this statement and understands that other arguments may exist which would require that this be a single source of water. Although no case has yet been provided the Inspectorate considers that one should be produced. It would need to see a strong argument before accepting a case based upon a single

tank if it is only provided with a single vent and outlet line.

11.46 The water pump to the RCS will be delivered by four high-head and two low-head safety injection pumps. A significant change has been made from the SNUPPS design in that four high-head pumps of an increased capacity are used as compared with two of lower performance in SNUPPS. The increased pump rating has been provided at both the high pressure and low pressure ends of the performance curve. The Inspectorate welcomes the proposed changes in the high head safety injection system which should result in:

(a) Improved reliability of the system in the high pressure injection mode.

(b) Lower peak clad temperatures in small break LOCAs.

(c) The ability, under certain conditions, of the high head pumps to provide a supplementary low head safety injection function.

While there are some reservations about the overall reliability of the system to satisfy a low head safety injection role, NII considers that the four-pump HHSI can provide effective and reliable protection against a small LOCA.

11.47 Evidence shows that small LOCAs could be comparatively frequent events. For example, these have been caused by PORV failures (as in TMI, ref. 17), loss of RCP seals and failure of steam generator tubes (as in RE Ginna, ref. 44). Accordingly the Inspectorate has asked CEGB to justify why a diverse form of high pressure safety injection is not proposed. The response is that PORVs are to be fitted with automatically controlled block valves for isolation, additional seal protection not dependent upon common services such as component cooling water is to be provided for the RCPs and a different design of steam generator will reduce the probability of tube rupture. The Inspectorate also questioned the provision of a single charging system (ECS) pump for this duty in that:

(a) The system does not meet the single failure criterion.

(b) Not withstanding (a) the reliability of a single pump would be insufficient to satisfy the demand on the ECS.

However, it is now understood that an additional ECS pump is to be provided. While this goes some way to satisfy concern about the ECS, the Inspectorate still needs to be satisfied about the system's overall reliability and its ability to meet the single failure criterion in other areas.

11.48 It is the CEGB's intention to reduce the frequency of all forms of small LOCA so that diversity of protection is not required. The Inspectorate will closely examine the evidence produced as detailed design proceeds to ensure that a reduction in the initiating frequency can be achieved. While it appears that all significant small LOCAs can be made sufficiently infrequent events the Inspectorate reserves its position at this stage until the relevant information is provided. Failure to achieve the intent could lead to significant changes in plant and layout.

11.49 Pressurised tanks (accumulators) containing borated water are provided so that in a large LOCA the bottom of the pressure vessel can be rapidly refilled. In the generic review the Inspectorate questioned the ability of the four accumulators to withstand a single failure and still provide sufficient water. US practice is to assume that the accumulator connected to the breached loop discharges via the breach and is lost and that all other accumulators discharge into the vessel. This question does not apply to the Sizewell B design as each accumulator has been increased in capacity by 50%. Thus, even with the loss of one accumulator via the breach, the three remaining can withstand a single failure and still discharge sufficient water to refill the bottom head of the RPV.

11.50 Following a large LOCA, long-term heat removal will be performed by the RHRS operating in a recirculating mode by drawing water from the containment sump and injecting it into the primary circuit. Since the system is likely to be contaminated by radioactive material from failed fuel, post-LOCA maintenance is not proposed. In view of the long recovery period following this type of accident the Inspectorate has concerns about the reliability of the system. It considers that the need for post-accident maintenance should be reconsidered, in case suitable provision can be made at the design stage. This would help to ensure that such work could be performed without undue exposure to operators.

11.51 The Inspectorate has also asked for further information on the performance of the containment sump screens in the LOCA and post-LOCA environment. The close proximity of the two sumps one to another may mean that debris could block both screens simultaneously.

11. 52 It is considered that an adequate safety case for the ECCS has not yet been made, and the Inspectorate requires resolution of the matters discussed before a decision on licensing is taken.

Auxiliary feedwater system

11.53 The auxiliary feedwater system is an automatic system which provides feedwater to the steam generators following reactor shutdown and when feedwater from the main feed system is not available. The reliability required of the auxiliary feedwater system depends on the frequency of fault situations requiring

it to operate and the availability of alternative means of heat removal such as 'bleed and feed'.

11.54 The Inspectorate has been unable to determine what reliability has been specified for the system but it needs to be high and it is noted that diversity has been provided. From the arguments presented, it is considered that the reliability may not be such as to permit plant operation with a pump out of service.

11.55 The method of routine testing described does not check the capability to inject feedwater into the steam generators.

11.56 There is a concern that, on present evidence, the feedwater storage capacity may be inadequate following a seismic event.

Containment systems

11.57 Containment systems are defined by the Inspectorate as those systems or components necessary for the required performance of the containment and any extensions of the main structure, such as pipe work or ancillary structures which communicate directly with the containment atmosphere or the source of radioactivity. In the Sizewell B plant these systems are taken to comprise the containment isolation system, containment cooling system, containment spray system, containment gas mixing and control systems, secondary containment systems, containment ventilation and containment sump system.

11.58 The Inspectorate has reviewed the safety case for these systems and concludes that more information is required than is available in the PCSR and its supporting reports before it can say that all matters have been satisfactory considered. However given resolution of the issues discussed below and those relating to the general design basis (para 11.11 *et seq.*) an adequate case can be made prior to a decision being made on licensing. These items include some where a significant impact on safety or layout may arise and which therefore need to be speedily resolved:

(a) A comprehensive examination of the requirements and function of a secondary containment should be presented, bearing in mind that at the time of writing a secondary system completely enclosing the primary containment is being considered. The principal means of preventing leakage via the equipment hatch is 'strict administrative control'. Failure of this control could result in leakage direct to the environment the consequences of which have not been discussed. Should these prove to be unacceptable then it may be necessary to enclose this hatch within a secondary containment.

(b) Several instances of failure of personnel air-locks to seal have been reported in the United States. The consequences of such failures coincident with a design basis LOCA, steam line break, etc., should be discussed in the PCSR.

(c) Failure of the single sump isolation valves may lead to problems in normal and accident conditions. Satisfactory justification of this provision has not yet been given.

(d) The sizing of the containment purge systems is dependent among other considerations upon the source terms used see, for example, Section 12 on chemistry and corrosion. Since underpredicting these terms could have a significant effect on layout, further justification should be provided at an early date to reduce the risk that subsequent enlargement may be necessary.

(e) Whilst degraded core situations are not included in the safety case in the PCSR, it would nevertheless be prudent to design the containment systems to deal with this situation and qualify the equipment accordingly.

(f) Consideration should be given to isolation of the containment on a high radiation level signal, as being of more direct concern than the high pressure signal alone, particularly in the case of events such as small LOCA and ATWT sequences.

(g) The remedial measures which could be undertaken in the event that the sump filters became blocked following an accident should be discussed.

Services

General

11.59 The protection system requires several services for its correct operation. These include: electrical power supplies, electrical control supplies, compressed air (instrument air), water cooling (CCW and ESW), room cooling (HVAC), steam supplies and the reserve ultimate heat sink (RUHS). In every case these services should be designated as part of the protection system.

11.60 In many areas the Inspectorate has been unable to assess the adequacy of such services because of the lack of a sufficient specification. This is particularly true in the case of services feeding diverse protective actions. The Inspectorate has requested a schedule of the services required for each protection system component showing the exact point of derivation.

11.61 Failure of each service, including the electrical and pneumatic services, should be included in the fault analysis as initiating events.

Electrical system

Introduction

11.62 The electrical system provides the means of feeding the electrical output of the station to the grid

and also of drawing power from the grid to supply a large number of plant items. From the safety viewpoint, supplies to components of the protection system are particularly important since failure of these supplies would cause failure of the protection. Those parts of the electrical system involved should themselves be designated protection system.

11.63 The electrical system provides power for the protection system components at various voltage levels. The basic sources of power are from the grid via the station transformers or alternatively from four diesel generators. Control and instrumentation supplies are supplied by battery 'no-break' supplies. Other features of the electrical system have a less direct but nevertheless important effect on safety since failures can be the main cause of faults requiring action from the protection system.

System assessment

11.64 The system is divided into four essentially independent electrical trains which are segregated for protection against fire and other hazards, generally into two double trains. In some cases, such as low head safety injection pumps, and containment spray pumps, there are less than four trains of equipment to be fed which in turn imposes operational and reliability limitations on the electrical system.

11.65 Although diverse supplies are provided from the grid and diesel generators, the electrical distribution system has little diversity, except in the case of battery-backed control supplies. As a means of providing diversity of reactor heat removal, the station as a whole is designed to withstand complete loss of a.c. power for periods of a few hours by the provision of steam-driven protection systems for heat removal in the pressurised state. Subject to detailed assessment these provisions are generally acceptable.

11.66 However the Inspectorate has identified the following concerns as not yet acceptable and requiring attention at the pre-licensing stage:

(a) An adequate specification of the duty and reliability required of the electrical system is not given. In particular, the voltage and frequency limitations of the electrical plant have not been specified.

(b) The Inspectorate is not yet satisfied that the segregation against hazards provided between redundant trains is adequate. A hazard analysis is proposed by CEGB to demonstrate the adequacy of the proposals and the Inspectorate wishes to have this before a decision on licensing and in time for discussion of alternatives should this be found necessary.

(c) The Inspectorate has been unable to establish to its satisfaction the CEGB's intention in situations where electrical plant items are unavailable due to failure, maintenance or testing. In cases where protection depends on two trains being available, such as following a large LOCA event, the Inspectorate is not yet satisfied that the system will have adequate reliability.

(d) The Inspectorate is not clear at this stage about the derivation of services to permit grid switching operations. Evidence is required that these will be independent of the diesel generators and station services in accordance with the claims made in Chapter 15.

Conclusion

11.67 The electrical system is acceptable in principle at this stage of the assessment subject to resolution of the concerns outlined above.

Instrument air system

11.68 The Inspectorate has doubts about the acceptability of the instrument air system as described in the PCSR since it does not have the same redundancy and segregation as the systems it supplies.

11.69 The Inspectorate is not clear about the total uses that are made of this system to control protective actions and a schedule of all such uses is required. In addition the instrument air system should be designated as part of the protection system (it is stated that it is non-safety) and an analysis performed of the failure modes. From the available information it appears that complete failure of the system would result in loss of ability to maintain stable hot shutdown and prevent achievement of cold shutdown of the plant.

Essential cooling systems

11.70 Heat removed from the essential systems and reactor auxiliaries is dissipated to the component cooling water system (CCWS) and thence to the environment via either the essential service water system or the reserve ultimate heat sink. In view of their close relationship the Inspectorate has examined all three systems together. The CEGB's intent is to provide a combined system which is redundant and in parts diverse so that its resistance to common mode failure is increased. Additional protection against failure has been provided in the form of equipment not relying upon the CCWS for system cooling.

11.71 It is accepted that the essential cooling systems can be designed to operate in normal operation in accordance with the strategy outlined. The Inspectorate has reservations, however, about the claim that operation in the normal mode demonstrates the ability of the systems to perform post-accident. Several changes of status occur immediately after the safety injection signal. These changes include a step increase in heat load of more than 12 times the initial load, with pump flow demand increased by 50%. It is appreciated that full-size demonstration of the LOCA performance would be unrealistic and therefore a

rigorous analysis of the systems to demonstrate their ability to cope with such transients is expected. This has not yet been done.

11.72 The Inspectorate has recently been informed that additional pumps are to be added to the CCWS to provide a direct link between the containment coolers and the reserve ultimate heat sink. At this time there is insufficient information available to permit it to comment further.

11.73 The Inspectorate has also questioned the potential for and consequences of ruptures in the large bore seawater mains of the essential seawater system within the auxiliary building as this has not been considered in the PCSR.

Safety-related instrumentation

Introduction

11.74 Control and instrumentation are involved with all aspects of plant operation and are the main interface between the operator and the plant. Controls and instrumentation that form part of the protection system are covered in the sub-sections dealing with protection. This sub-section covers all other control and instrumentation systems having a significant but less direct effect on safety and which the Inspectorate terms safety-related instrumentation. Such instrumentation includes the following: reactor controls, monitoring of the plant to meet operating rules, monitoring of the protection system, monitoring of accident conditions, communications, and fire detection. These systems are described in the PCSR under Sections 7.3, 7.4 and 7.6 and also under each plant section of the whole report.

11.75 Because of its safety role, safety-related instrumentation should have similar treatment to the protection system namely:

(a) It should be identified. The classification procedure indicated in Chapter 3 of the PCSR is insufficient since it only has two classes for electrical equipment neither of which are appropriate to safety-related instrumentation.

(b) The design basis for each system should be stated, but this does not appear to be the intention. It should include measurement ranges, the situations, including faults and hazards, under which it is required and its reliability or redundancy. This will determine requirements for segregation.

(c) Evidence should eventually be made available to show that the safety-related instrumentation will perform its intended duties.

Accident monitoring

11.76 Instrumentation requried for monitoring accident conditions should be designed to survive and monitor conditions well beyond the design basis accidents. The Inspectorate will require evidence at a later stage that this has been provided.

Reactor controls

11.77 Reactor controls are described in Section 7.6 of the PCSR. Many of these controls are of significance to safety in that they cause and hence determine the characteristics of virtually all frequent faults on the plant.

11.78 Whilst many failures of these controls are included in the fault table in Section 15.1.9 of the PCSR, further analysis is required of the controls for common mode failure.

11.79 The Inspectorate has not at the present time examined the algorithms of these controls since they are based on existing practice with the exception of the reactor power control loop.

11.80 All the controls take signals from the protection system via isolation devices. The signal selection system is mentioned but is not described in sufficient detail to enable any assessment to be made.

Control room

11.81 A control room forms the major interface between the operator and the plant. It should be designed to facilitate safe operation of the plant in all operating modes.

11.82 Two control rooms are provided, a main one and also an emergency one with limited facilities for situations where the main control room cannot be manned. Few details are given of these control rooms but this is acceptable at this stage provided it is clear what are the principles to be followed. The Inspectorate has been told that the CEGB has set up a working party to consider the detailed design of the control rooms and it wishes to be kept informed of this work on a regular basis.

Conclusions

11.83 Because of the limited time available the Inspectorate has not been able to assess or discuss with the CEGB the safety-related control and instrumentation in any depth. However, whilst most of the equipment covered by this report can be detailed by the CEGB and assessed at a later stage, the Inspectorate will need to be satisfied that the CEGB's intentions for safety-related instrumentation are acceptable at the appropriate time.

Overall conclusions

11.84 In the generic review it was concluded that the Inspectorate saw no fundamental reason why acceptable protection arrangements could not be provided for the PWR reactor system considered: this remains the view.

11.85 It is clear that many improvements have been made to the protection system since the generic review. However the safety case as presented in the PCSR is not yet acceptable for licensing. The reasons for this will be found discussed above and require action in the following categories:

(a) Improvements in presentation of the case.

(b) Better specification of the duties required of the protection system.

(c) Firm commitments to be made by the CEGB in a number of cases not least in design intent and principle.

(d) Further argument to demonstrate that the systems offered meet either CEGB or NII principles. Accepting that neither of these are mandatory a safety case should nevertheless show that the agreed objectives have been met.

(e) Further time for discussions to resolve what are in many cases complex issues.

11.86 The Inspectorate expects to see its main concerns resolved before a decision on licensing is made. This can be achieved by clarification of the safety case and design intentions and by giving of firm commitments where appropriate. It can see no fundamental reason why this should not be achieved and an acceptable system provided.

Introduction

12.1 In a PWR, inadequate design and inefficient control of the fluid chemistry of the primary and secondary loops and the associated ancillary circuits may contribute significantly in both normal and fault conditions to serious component degradation and to the collective dose. Aspects of concern include the integrity of the primary circuit, especially the steam generator tubes, and the build-up of primary circuit activity, both solid and dissolved, which may lead to high dose rates or releases to the secondary circuit and to the atmosphere. The more significant problems arising from the assessment of the plant chemistry and corrosion aspects of the PCSR are discussed and summarised below.

Primary circuit activated corrosion products

Introduction

12.2 Experience from operating PWRs suggests that primary circuit activated corrosion products ('crud') constitute the main underlying source (at least 70%) of the occupational radiation exposure from the plant. The demonstration that these levels have been reduced to a level which is as low as is reasonably practicable (ALARP) is fundamental to the case for the control of such exposures. The root of the problem is the presence in the primary circuit materials of particular metal atoms, notably nickel and cobalt (respectively, precursors of the main critical isotopes ^{58}Co and ^{60}Co), which can be released into the coolant by aqueous corrosion and erosion, and then activated in the high neutron flux of the core regions, especially by deposition on the fuel elements. These 'activated corrosion products' are then redeposited around the primary circuit, and may give rise to very high shut-down dose rates in areas where inspection and maintenance are required.

12.3 In Chapter 12.3.5 of the PCSR a number of potential means are identified of reducing these levels, and these are discussed below. The Inspectorate has reservations about the case put forward on these, in particular the reduction of cobalt levels in hard-facing alloys (Stellites), the filtration provisions and chemical decontamination. The Inspectorate has requested a document setting out and justifying the CEGB's strategy for meeting the ALARP criterion for occupational radiation exposure (see Section 14), included in which it expects to find a detailed consideration of the CEGB's position on these three issues.

Materials

12.4 The inherent materials problem arises because about two-thirds of the primary circuit internal surface area is made up by the steam generator tubes for which the Westinghouse licence specifies the high nickel alloy, Inconel 600 (70 – 75% nickel). Consequently about one-third of the metal atoms in contact with the primary coolant are ^{58}Ni, which gives rise to the high ^{58}Co levels in the crud. In addition, the cobalt impurity levels in Inconel 600 can be responsible for about half the crud ^{60}Co inventory. The remaining ^{60}Co arises mainly from the Stellite hard-facing alloys in heavy wear components (valves, control rod drive mechanisms, etc.) which contain 50 – 60% cobalt.

12.5 Whereas the Inspectorate believes that in accepting the proposed steam generator tube material there is little more that it is reasonably practicable to do in lowering nickel levels, there is however some capacity to reduce the cobalt levels. The CEGB has made proposals to reduce cobalt levels in Inconel 600 and if confirmed these are likely to be acceptable. The claim that no low cobalt hard-facing alloy alternatives are available for incorporation in the design needs more justification.

Operating chemistry

12.6 The design intent is to control the primary coolant chemistry, particularly the pH, so as to minimise the rates of general metal corrosion and release out-of-core and, as far as possible, to dissolve and retain in solution the corrosion products during their passage through the core, in order to minimise the potential for their activation. Within the broad operating chemistry pH specification, a narrower operating range is proposed, based on closely correlating the lithium hydroxide levels with the boric acid concentration. This should have beneficial effects on the crud levels. The Inspectorate is concerned, however, that the solubility data on which this operating chemistry is based are derived from magnetite, and not from the predominant crud species, nickel ferrite. What little literature there is on nickel ferrite shows that the solubility behaviour with temperature and pH of the two species is not strictly similar. The Inspectorate therefore wishes to see validation of the chemistry on a nickel ferrite data base, and a greater understanding demonstrated of the fundamental processes of the crud problem.

12.7 The Inspectorate also requires a consideration of the possibly significant effects of the quality of the operating procedures, including human factors and administrative control on the crud levels.

Filtration

12.8 A deliberate attempt has not been made to filter primary coolant crud. The chemical and volume control system (CVCS) reactor coolant filter is too coarse to remove crud efficiently, and reliance is placed on uncontrolled removal by the system ion exchangers. Neither is designed for this purpose. The Inspectorate requires a quantified argument as to why the means of crud removal by filtration cannot be improved. The claims made in the PCSR that the CVCS removes active crud should be supported by quantitative evidence, which should be available from the considerable PWR operating experience.

12.9 An adequate case is not made for the omission of magnetic filtration, or at least for the omission of space for such a plant bearing in mind that space was provided in the April 1981 reference design (ref. 45) and appears to be recommended in the relevant supporting report (ref. 46) by implication. The Inspectorate understands from discussion with the CEGB and from a supporting report (ref. 47) that a developed Westinghouse design is available. The virtues of the technique are that the majority of the crud is ferro-magnetic and thus readily extracted in this way, and that it can process a substantially greater proportion of the coolant than the CVCS, and at reactor temperature. A justification of this omission in terms of what is reasonably practicable is required before a decision is made on licensing since this is a potential means of substantial source term reduction, and has significant layout implications inside the containment.

Decontamination

12.10 Chemical decontamination involves the addition of reagents to dissolve the corrosion products deposited on the primary circuit pipework and components, and the removal of the dissolved activity on to ion-exchange resins for subsequent treatment and disposal. This may be performed either on the whole circuit or individual components. Some operating experience of both methods exists. The potential for dose reduction was highlighted in the Inspectorate's generic review.

12.11 In the PCSR it is claimed that no suitable process is currently available, but that appropriate connections will be provided to incorporate the necessary plant at some future time. Coverage of the present state of the art on possible techniques is however, inadequate, particularly concerning the two most favoured processes, LOMI (low oxidation state metal iron) and POD (PWR oxidative decontamination). Further research and development is in progress, but it is the Inspectorate's view that a more quantitative assessment of the likely advantages and problems associated with whole circuit decontamination can be made on the basis of current knowledge, and this had been requested as a part of the ALARP strategy document.

Off-power chemistry

12.12 The Inspectorate will be looking for more detail on the procedures proposed for pre-conditioning of the primary circuit surfaces before start-up, and for the increase of coolant oxygen potential to control and minimise the cobalt-58 'crud burst' which occurs in refuelling.

Conclusions

12.13 If satisfactory responses are given in the CEGB's ALARP strategy document, the Inspectorate would be able to consider the case on activated corrosion product level reduction on a proper basis. It will not be possible before then to state that no significant modifications would be required, particularly on the Stellite and magnetic filtration issues. Early resolution of these issues is important.

Post-accident chemistry and release mechanisms

Introduction

12.14 This section considers the chemical activity control procedures used in the event of accidents which release activity into the containment, considered in PCSR Sections 6.2.5 and 15.9.5.3.

Assessment

12.15 To mitigate activity releases to the environment in most LOCAs and certain other design basis accidents, significant reliance is placed on the containment spray system to entrain and to immobilise effectively the activity which escapes into the containment building atmosphere and sumps. The Inspectorate has not yet been able to assess the efficiency of the proposed hydrazine and boric acid spray system solution, since not only are doubts expressed in the PCSR as to the particular effectiveness of the hydrazine on releases following LOCAs, but also adequate support references to assess it are not provided. Appropriate documentation is expected later in 1982. The efficiency of the system will also depend on the use of correct and conservative primary coolant activity levels and adequate modelling of activity releases in accident conditions. Adequate short- and long-term control of the chemistry of the post-accident containment sump solution, such that radio-isotopes are converted and maintained in a non-releasable form, remains to be demonstrated. The Inspectorate is not yet satisfied that the dry buffering chemicals in open racks on the containment walls will dissolve, when required, in sufficient quantities to control the sump pH, particularly since they may have formed a crust during storage.

12.16 The Inspectorate also has reservations about the compromise between a high sump pH, needed to maintain dissolved iodine in non-elemental forms and to minimise acid chloride attack on primary circuit and containment steels, and low sump pH, needed to reduce the significant hydrogen evolution from alkali attack of zinc-based paints in the containment.

12.17 These post-accident chemistry control considerations are also of concern to 'degraded core accidents'. The conclusions from a study of those situations may well prove to have a bearing on the present assessment.

Conclusions

12.18 The Inspectorate awaits further information to assess the effectiveness of the containment spray solution and additive in mitigating activity releases in design accidents and to remove its concern about the strategy to control the containment sump solution pH.

Primary coolant chemistry with respect to corrosion of the reactor coolant pressure boundary (RCPB) and auxiliary systems

12.19 At present, insufficient justification is given in the PCSR for various specified levels of the primary coolant chemical parameters. The ability to control pH, oxygen and halide ion levels requires more substantiation, bearing in mind the potential for administrative failures. In particular it is not clear what measures would be taken to control oxygen levels in the coolant, so as to prevent RCPB or auxiliary pipework corrosion, in the event of either failure of the CVCS hydrogenation system or its non-operation during tritium purging of the coolant.

12.20 The Inspectorate is especially concerned that the chemistry regimes which could cause stress corrosion cracking of stainless steel pipework and components, whether sensitised or non-sensi ised, should be identified and it wishes to see provisions made to monitor or forewarn of such corrosion. It is noted that stress corrosion attack ('pure water cracking') by the primary coolant on the Inconel 600 steam generator tubes has been ameliorated by the adoption of a thermally treated material, although adequate chemistry control has nonetheless to be maintained.

12.21 Stress corrosion cracking of auxiliary system pipework by oxygenated, borated water, probably with chloride impurities, nas been prevalent in US PWRs, and is the subject of an NRC inspection and enforcement bulletin (ref. 48), but has not been discussed in the PCSR. This could affect the integrity of a number of systems, notably HHSI, LHSI and containment sprays. In the ECCS case, cracked pipework might be only one valve removed from the primary circuit. The Inspectorate therefore requires a case to show adequate protection for this problem, paying particular attention to impurity ingress control and the reliability of administrative procedures.

Steam generator secondary side chemistry control and corrosion

Introduction

12.22 Secondary coolant chemistry control is a vital part of the prevention or reduction of corrosion of the steam generator tubes. In Section 10 the present overall position on tube integrity is summarised in the light of the problems which have been experienced on earlier steam generators and the design features of the Model F steam generator which are intended to deal with them. This section reviews the specifically chemical aspects of corrosion control. The main concern is the possibility of inter-granular attack (IGA) in the tube sheet crevice region. However, demonstration of chemical control to minimise other forms of tube corrosion, e.g. denting, is also important with regard to radiological issues, such as exposures during maintenance and activity release to the secondary coolant.

Secondary side

12.23 The definitive mechanism for inter-granular attack in the tube-sheet crevice region has yet to be identified, and this form of attack has not been reproduced in the laboratory. Local high concentrations of hydroxide ion seem to be involved, but much more information is required to establish the precise mechanism, particularly the role of metallic impurities. In view of the doubts about the detection of this attack, with or without accompanying stress corrosion fingers, the Inspectorate expects to see further work initiated, particularly long-term model boiler testing using the correct configuration and UK PWR chemistry environment, including representative specification transients and cycling. It requires a sufficient case to be presented to show that concentration of aggressive chemical species is unlikely to occur in a significant number of tube-sheet crevices, whether open or sludge-filled. Current experimental data seem to be very limited and largely confined to crevices that are too shallow.

12.24 The Inspectorate is not yet satisfied that solids accumulation will not occur at these crevice regions since little relevant operating experience appears to exist, but measures adopted in the steam generator thermal hydraulic design and the improved blowdown provisions should substantially reduce the tendency for deposition. The intentions with respect to crevice flushing and lay-up procedures will need to be established, since they may contribute significantly to solids control.

Denting

12.25 Although adequate forewarning of denting as a problem affecting tube integrity should result from the policy of tube inspection and plugging, it may still have radiological significance in terms of operator exposure and activity leakage. The Inspectorate recognises that significantly reduced potential for denting should result from the use of 405 stainless steel support plates with a quatrefoil hole configuration, titanium condenser tubes with double tube plates, and improved solids control (ref. 49). Despite the elimination of copper from the feedwater systems, however, there is evidence that nickel ions present in the water would be equally likely to promote attack (refs. 49, 50). As yet the role of these ions and the exact chemistry of the denting process are still inadequately understood. Prevention of chloride ion ingress to the steam generator is necessary, but there is as yet insufficient information to assess the design and control measures. The supporting experimental data on 405 stainless steel are still short term, but operation of a related steam generator at Surry 2 should provide valuable lead experience of any long-term effects.

General secondary coolant chemistry control

12.26 The Inspectorate will require further information on the secondary coolant chemistry before it can be satisfied that there is adequate control in respect of steam generator tube and other integrity issues. In its view the discussion in Chapter 5.7.5.11 of the PCSR should be better organised. The following are matters of concern:

(a) The measures to counteract the slippage of sodium ions from the condensate clean-up plant resins and the escape of regenerant sodium hydroxide to the feedwater would seem to be mutually conflicting, if high pH levels are to be proposed. Control over escape of regenerant acid and of acid resin fines also needs to be demonstrated.

(b) There should be a discussion of the solids arisings expected through the feed system, including the maintenance of correct pH and oxygen levels, and appropriate choices of feed heater materials.

(c) Monitoring and sampling arrangements will need to be described in more detail to give assurance of their effectiveness and adequacy, particularly regarding measures to be taken if departures from specification occur, the adequacy of the tripping arrangements on high feedwater conductivity and the absence of on-line corrosion monitoring.

(d) More detail is required of lay-up and off-power measures to protect the steam generator tubes from corrosion.

(e) A discussion is required of the concentration of aggressive species during the times when the blowdown system is non-operational, to show that no adverse effects result.

Monitoring for the 'leak-before-break' argument

12.27 The leak-before-break argument for tube integrity monitoring and forewarning places reliance on the ability to monitor accurately the activity leakage rate in the blowdown system. No details are provided of how this is done, or the basis on which the accuracy of the method can be assured.

Conclusions on steam generator secondary side chemistry control

12.28 Further information is required before the Inspectorate can be satisfied that the concentration of aggressive species in significant numbers of tube sheet crevices will not occur leading to intergranular attack in a region where an adequate detection method has not yet been proven.

12.29 The likelihood of denting would appear to be reduced by the design measures adopted, but uncertainties still exist over the mechanism, especially the role of metal ions such as copper and nickel. Only short-term test data are available, and the Inspectorate will look for longer term assurance. Various general chemical control aspects require more attention, particularly the apparently conflicting requirements for preventing significant slippage from the condensate clean-up ion-exchange resins and escape of regenerant chemicals into the feedwater. Monitoring, tripping and sampling arrangements require more detailed discussion in the safety case.

12.30 The provisions for the 'leak-before-break' monitoring of tubes remain to be described.

General conclusions on chemistry and corrosion

12.31 In the chemistry and corrosion area there are a number of concerns arising because a satisfactorily comprehensive case is not yet made in the PCSR. The main issues have been summarised in the conclusions of the previous sub-sections. The Inspectorate considers that they should be addressed with some urgency, particularly since this is the first commercial water reactor in the UK. Because of the safety implications it needs to be satisfied that proper chemistry control is feasible and will be carried out.

Safety assessment basis

13.1 In this section those aspects of the proposed design are reviewed which are concerned with the management of radioactive waste materials from the point of production to their final discharge from the site in acceptable forms and under controlled conditions. The collection, treatment and temporary storage of radioactive waste leads inevitably to some radiation exposure of workers on the site, while its discharge from the site involves the possible exposure of members of the public. The Inspectorate requires the safety case to provide sufficient evidence to demonstrate that the doses to on-site workers and members of the public from radiation sources originating on the site, including radioactive wastes, will be kept within the prescribed limits. Further, it is required that the doses to operators and to members of the general public be kept as low as is reasonably practicable (ALARP).

13.2 As far as waste management is concerned, the application of this latter requirement implies the necessity to arrive at a suitable balance between the dose received by station staff from waste treatment and temporary storage on-site, and the dose received by members of the public from wastes discharged from the site. In this area there is joint responsibility between the Authorising Ministries (DoE and MAFF) and the Inspectorate.

13.3 At this preliminary stage of the assessment, the Inspectorate's main concern has been to ensure that the systems proposed by the CEGB in Chapter 11 of the PCSR for collecting, processing, storing and discharging radioactive wastes are sufficiently flexible to give confidence that they can be engineered so as to allow the above radiological principles to be met. Time has not permitted any in-depth assessment of the detailed engineering provisions for waste management but at least one item has come to light which will have to be resolved before the design is accepted (see para 8.7). The assessment process will continue and intensify so that the Inspectorate can be satisfied that it has identified and satisfactorily resolved all important engineering issues concerned with waste management prior to the appropriate stage of construction of the plant.

Assessment of the safety case in the PCSR

13.4 Design decisions relating to such factors as installed process capability, tank sizings, storage capacity and the ultimate release of activity to the external environment depend on an adequate estimation of the magnitude of the radioactive waste sources, and particularly the predicted level of activity in the primary coolant. The main components of primary coolant activity which are of concern to waste management are fission products from defective fuel, activated corrosion and wear products, and tritium.

13.5 In the PCSR, the notional fission product activity level in the primary coolant is based on an assumed 'failed fuel fraction' in the core (values of 0.2%, 0.02% and 0.005% are used at different places in the PCSR). This makes an artificial correlation between the measured ^{131}I concentration in the coolant and a supposed percentage of pin failures of a certain average type. There seems to be no theoretical basis on which to extend the percentage of activity released as ^{131}I, the only widely measured fission product, to any other isotope, in view of the gross uncertainties in the nature and extent of the fuel defects, the differing behaviour of various isotopes and other broad assumptions made.

13.6 It was pointed out in the Inspectorate's generic review that the concept of a 'failed fuel fraction' was unhelpful and misleading; what is actually required for shielding, waste management and fault calculations is a primary coolant fission product source term based on a wide range of measurements of relevant isotopes from operating reactors. Recent discussions with the CEGB have indicated that it appreciates the uncertainties in using a notional 'failed fuel fraction' and it intends to substantiate the fission product source terms in the PCSR by using a revised computer code which discards the 'failed fuel fraction' concept and instead bases its predictions on more comprehensive operating measurements and fuel escape rate coefficients. According to the CEGB, the predictions of the new code show that the fission product source terms in the PCSR are generally conservative. Whilst welcoming this approach, the Inspectorate has not yet been furnished with the necessary documentation to assess the CEGB claim.

13.7 Another important contribution to the radioactive source term in the primary coolant comes from activated corrosion and wear products ('crud'). It appears that, in spite of the improved data base since the time of the generic review, no long-term correlation has yet been established between effective plant life and crud concentration. Therefore the overall conclusion is basically the same as that in the generic review, namely, that there is insufficient understanding of corrosion product arisings and behaviour to have much confidence in the crud source terms listed in the PCSR. In assessing the detailed engineering provisions, particularly the solid waste treatment and storage facilities, the Inspectorate requires the CEGB to use adequately pessimistic source terms in its calcu-

lations to allow for the uncertainties in the available data, including that relating to crud predictions. The Inspectorate is not currently satisfied that this has been done. For example, of the nine crud isotopes quoted in the PCSR and the relevant supporting report, only two have been given obviously conservative values compared with operating data and no account seems to have been taken of soluble and non-filterable corrosion product levels.

13.8 The third major contribution to the primary coolant source te n comes from tritium. The tritium originates mainly from ternary fission in the fuel, followed by diffusion through the fuel and cladding to the coolant. It is also produced by neutron bombardment of the lithium used for chemical control purposes. Both of these processes can be quantified quite accurately and their treatment in the PCSR appears to be satisfactory at this stage.

13.9 Tritium levels in the primary coolant will be controlled by frequent discharge operations through the chemical and volume control system (CVCS): this is a significant departure from the SNUPPS procedure. At this early stage it is considered that further information about the method should be provided to allow a complete assessment of the safety implications of this change to be carried out.

13.10 Mixing of primary coolant water with water in the refuelling cavity and the spent fuel storage pool (SFSP) leads to the release of some gaseous tritium in the form of water vapour evaporated from the SFSP. This aspect of the waste management strategy will require further assessment in conjunction with the assessment of the tritium discharge policy to ensure that the procedures have been appropriately optimised in respect of doses both to workers and to members of the public. The Inspectorate will require additional information to that provided in the PCSR to permit it to carry out this assessment.

13.11 Although there is a good general description in the PCSR of the waste management systems there is insufficient detail in several areas such as:

(a) the design and materials of construction of process and storage facilities;

(b) the capacity and retrievability provisions of the solid waste storage facilities;

(c) the design of radioactive transfer pipework and drainage systems;

(d) the methods to be used for detecting leakages of radioactive materials;

(e) the plan for liquid waste sampling to ensure appropriate control over discharges;

(f) the active material solidification system;

(g) the provisions for filtration of gaseous activity.

While it is not necessary for detailed information to be supplied in the PCSR on all aspects of the above, the Inspectorate expects sufficient information to be provided for it to be sure that the design intent fully meets the requirements.

13.12 The waste management systems have not been designed specifically to deal with the arisings which might result from a possible whole-circuit decontamination exercise. It is anticipated that the additional waste management facilities which would be needed for such decontamination exercises will be discussed in the document which the CEGB is preparing in support of its ALARP strategy (see Section 14).

13.13 The solid, liquid and gaseous waste management systems described in the PCSR are, in general, judged to be sufficiently flexible to allow a proper balance to be achieved between the exposure of on-site workers and the general public, each being as low as is reasonably practicable. However, although the PCSR gives some preliminary information on the effective dose equivalent to the individuals most at risk from liquid and gaseous releases, the Inspectorate has not yet been able to assess the validity of this information. Consequently it cannot judge the extent to which the present design achieves a proper balance between the dose to workers on-site and that to members of the public from waste management. This aspect will be pursued, in consultation with the Authorising Ministries, as the more detailed design develops, and the CEGB will be required to make use of available techniques (such as cost/benefit analysis) to demonstrate that the proper ALARP balance has been achieved.

13.14 The facilities have not been designed specifically to deal with the radioactivity which might be released in serious accidents. In the remote event that a serious accident should occur, additional capacity and dispersal arrangements would have to be made subsequent to the event, whilst relying on the containment to contain the activity for such a period as to allow remedial measures to be taken.

Summary and main conclusions

13.15 For a number of engineering aspects of the radioactive waste management system there is insufficient detail in the PCSR to allow a full assessment to be carried out. The Inspectorate expects the CEGB to provide sufficient additional information to allow it to identify and resolve all important waste management engineering issues prior to construction of the relevant plant.

13.16 There are some reservations about the predicted arisings of radioactive waste and, in particular, the Inspectorate needs to be satisfied about the

degree of conservatism in the estimation of fission product activity levels in the primary coolant.

13.17 Nevertheless, it is concluded that the radioactive waste management facilities described in the PCSR are sufficiently flexible to give confidence that the likely arisings, resulting from the normal operation of the reactor, can be handled in a safe manner.

13.18 Further information will be required to enable a judgement to be made of the extent to which a proper balance has been achieved between doses to on-site workers and those to members of the public. The Inspectorate will be consulting fully with the Authorising Ministries to ensure that the proper balance has been achieved.

Safety assessment basis

14.1 In the NII's Safety Assessment Principles there are three fundamental principles which apply to the radiological protection of persons on and off the site during normal operation, namely:

(a) No person shall receive doses in excess of the appropriate dose equivalent limit as a result of normal operation.

(b) The exposure of persons shall be kept as low as is reasonably practicable.

(c) Having regard to principle (b), the collective dose equivalent to operators and to the general public as a result of operation of the nuclear installation shall be kept as low as is reasonably practicable.

To demonstrate compliance of the design with the 'as low as is reasonably practicable' (ALARP) principle, the safety submission should specify a strategy for the limitation of doses to persons working on site, site visitors and members of the public from normal station operation, maintenance and inspection. This strategy should consider all sources of radiation and should incorporate all reasonably practicable measures for reducing doses. It is required prior to licensing in order that the Inspectorate may ensure that the more important aspects of plant layout and choice of design options are properly addressed at an early stage.

14.2 In reviewing the proposed provisions to minimise the radiological impact of the plant as set out in Chapter 12 of the PCSR, the Inspectorate has been conscious of the exposure records of PWRs already operating, and particularly those operating in the USA where extensive radiation dose data are available. Regular analyses (for example ref. 51) show that the average annual collective operator dose equivalent is currently more than 400 man-rem per annum for the average US PWR. A breakdown of this average annual collective dose shows that maintenance accounts for almost 70%; refuelling, about 7%; operation and surveillance, about 10%; waste processing, about 5%; and in-service inspection, about 7%. Since maintenance, particularly of steam generators and primary coolant pumps, contributes such a large fraction of the collective dose, special attention is needed to ensure that maintenance doses are made as low as reasonably practicable.

14.3 The high doses experienced during maintenance operations on PWRs are caused by activated corrosion products (crud) deposited on the inner surfaces of primary circuit pipework and components. The principal isotopes of concern are ^{58}Co and ^{60}Co and these dominate the shut-down dose rates around the primary circuit. An assessment of the formation, transport and deposition of crud is given in Section 12.

14.4 From the point-of-view of minimising the individual and collective doses received from maintenance and inspection the ALARP strategy should arrive at the appropriate balance amongst the following options:

(a) choice of primary circuit materials to minimise the formation of activated corrosion products, particularly ^{58}Co and ^{60}Co;

(b) choice of operating conditions to minimise the formation and transport of crud;

(c) incorporation of all reasonably practicable techniques to remove crud from the primary circuit before it can deposit in out-of-core areas, especially those areas to which access is necessary for maintenance and inspection;

(d) establishment of reasonably practicable techniques for removing deposited crud, i.e. decontamination;

(e) design of shielding and plant layout so as to minimise the need for persons to enter high dose rate areas;

(f) provision of remotely operated devices to assist with operations, such as fuelling, in-service inspection and maintenance, which would otherwise involve personnel working in high dose rate areas.

A suitable technique should be used where practicable to quantify the benefits and the associated costs of each option.

14.5 While the following discussion of the PCSR safety case emphasises the need to reduce the maintenance dose, due attention should also be paid to ensuring that doses during reactor operation, waste processing, etc., are as low as reasonably practicable.

Assessment of provisions for dose control during reactor operation

14.6 During reactor operation the main source of radiation, in addition to the fission process itself, is ^{16}N arising from neutron activation of oxygen atoms in the primary coolant. These processes can be quantified accurately and the relevant PCSR source terms are accepted as adequate for the general design of shielding and primary plant layout although the details will be subject to continuing assessment as the project proceeds. However, the shielding requirements for a number of primary plant components, such as resin

beds, depend on the assumed level of failed fuel in the circuit. The Inspectorate's reservations about the use of a notional failed fuel fraction to generate the fission product source term in the primary coolant have been discussed in Section 13. Nevertheless, it is accepted that the use of a pessimistic notional failed fuel fraction of 0.2% is likely to result in an adequate general level of shielding, although reservations remain about the adequacy of certain detailed parts of the shield design, which will have to be resolved in the detailed assessment phase prior to construction.

14.7 The shielding calculational methods have not yet been assessed in any detail but the Inspectorate does not anticipate any particular problems in accepting these since they are quite well established and have been used for several years on other reactor systems in the UK.

14.8 The secondary coolant of a PWR may become radioactive as the result of steam generator tube leakage. A conservative prediction of secondary coolant activity is necessary to ensure:

(a) adequate shielding and access provisions for certain secondary systems;

(b) adequate capacity and performance of the condenser evacuation filtration system; and

(c) the correct radiological classification of the turbine hall, both in terms of direct radiation and contamination from secondary circuit leaks or faults.

14.9 It is judged that the case presented in the PCSR is not yet sufficient to justify the claim that the secondary coolant activity levels are conservative. Apart from concerns about the level of conservatism in the primary coolant source term, the assumed steam generator leak rate is only two-thirds of the measured value from a number of operating Westinghouse plants with detectable activity in the secondary circuit. Also, the methodology for estimating the partition of isotopes to the steam generator gas phase is based on inadequately validated and even incorrect and conflicting data, and does not consider a sufficient range of isotopes. Further information will be required at the detailed design stage to provide assurance that the secondary coolant activity levels are adequately conservative, both in normal operation and under fault conditions.

14.10 The waste management strategy, and the current uncertainties in predicting the doses resulting from it, have already been discussed in Section 13.

Assessment of the PCSR case that doses are ALARP

14.11 The CEGB's radiological guidelines are intended to provide a framework within which a design can be developed which satisfies the principle that doses should be ALARP. Specific design targets are laid down for maximum operator dose in normal operation and a further design objective is that the station collective dose equivalent should not exceed 0.2 man-rem/year per MWe installed capacity (240 man-rem/year for the 1200 MWe Sizewell B plant). The Inspectorate accepts that this latter, purely arbitrary, target is ambitious and, if achieved, would rank Sizewell B with the top 10% of operating PWRs in the USA. However, no adequate discussion is presented in the PCSR of the overall strategy for meeting the ALARP principle and, in particular, it does not justify the apparent emphasis on items (b), (e) and (f) in the list given in para 14.4 above, with less attention being apparently given to the other methods of dose reduction.

14.12 The claim in the PCSR that the predicted doses for the Sizewell B plant are ALARP is based on the results of detailed consultation with Westinghouse and Bechtel as well as detailed discussions with the operating, maintenance, chemistry and health physics staff of many operating plants, plus a survey of the relevant literature. It is not disputed that this has given the CEGB a good insight into the problem of minimising doses on a PWR. This insight has contributed significantly to the detailed dose budgeting exercise that was carried out in support of the PCSR. However, from the point of view of demonstrating ALARP, this approach has two drawbacks:

(a) it is impossible for an assessor to form a view on safety case arguments which are based on someone else's discussions and personal consultation, and

(b) the use of existing experience from operating plants will tend to condition the designer to incorporate design features which are included in those plants and to be less enthusiastic about possible design features which have not been incorporated in them.

14.13 Following discussions with the Inspectorate, the CEGB accepted that the ALARP case in the PCSR needed to be set down in a more quantified manner and undertook to provide a supporting document later in 1982, outlining the ALARP approach used in the design and including, where relevant, the use of cost/benefit analysis to assist in forming a judgement on the extent to which ALARP has been met. The CEGB has expressed confidence that this document will satisfy the reservations currently held in respect of the demonstration of ALARP in the PCSR.

Summary and main conclusions

14.14 The CEGB's radiological design guidelines are intended to provide a framework within which radiation doses can be controlled and the ALARP principle can be demonstrated for both on-site workers and members of the public as a result of the normal operation of the Sizewell PWR.

14.15 At this preliminary stage it is considered likely that the shielding and layout provisions will prove to be generally adequate. However, further information will be required concerning a number of detailed areas, including the adequacy of the design provisions to cope with conservative secondary coolant activity levels, both during normal operation and under fault conditions.

14.16 It is accepted that its widespread discussions and consultation with other PWR designers and operators have given the CEGB a good insight into the problem of minimising doses on a PWR. This insight has contributed significantly to the dose budgeting exercise that has been carried out in support of the PCSR, and which has assisted the Inspectorate considerably in its assessment of the radiological impact of the proposed plant.

14.17 The PCSR does not give a sufficient description of the design strategy for keeping all exposures as low as is reasonably practicable. In good radiological protection practice priority is first given to the control of sources of ionising radiation before that of control of individuals. In particular, the design aim should be to reduce as far as is reasonably practicable the quantity of activated corrosion products in the primary circuit, unless special personnel protection measures, such as temporary shielding, and remotely operated inspection and maintenance equipment can be shown to be more cost effective and to be capable of reliable operation in service.

14.18 The CEGB has agreed to furnish the Inspectorate with a further report explaining its ALARP strategy and justifying its claim that it has done all that is reasonably practicable to minimise the production of crud and remove it from the primary circuit. To assist the formation of a judgement about what is reasonably practicable in the light of present technology (e.g. in respect of reduction of cobalt in primary circuit materials, in-line filtration of suspended crud particles, decontamination, etc.), the CEGB has been asked to demonstrate it has made reasonable attempts to quantify its ALARP judgements by the use of cost/benefit analysis on the lines recommended by the ICRP (ref. 52).

15 Fuel storage and handling

Introduction

15.1 There are several aspects of both new and irradiated fuel handling and storage in the PWR which are of safety significance. Potential hazards include excessive radiation exposure, release of radioactive material from damaged fuel, and inadvertent criticality.

15.2 An examination has been made of the safety case set out in Chapter 13 of the PCSR for fuel storage and handling, from the receipt of clean fuel, loading into the reactor, subsequent discharge and storage of irradiated fuel, and finally its dispatch in flasks from the site.

Assessment

15.3 The main points arising from our review to date are summarised as follows.

Administrative control

15.4 A general problem of concern is the use of administrative control for safety purposes which arises in several of the handling sequences which may be carried out manually and where the associated reliability appears not to be questioned. In the PCSR such imprecise phrases as 'administrative interlocks', and 'strict administrative control' are used. The Inspectorate needs to know both the detailed intentions and the confidence that can be placed on these actions, particularly when such administrative actions may constitute the first line of defence against hazards. A particular example of such a situation arises in the case of loading fuel into the reactor. There remains the possibility with manual control that a fuel assembly, either new or irradiated, could be loaded into an incorrect position in the reactor core. It is the CEGB's stated intention to examine the reliability of such administrative controls and show them to be acceptable.

Size of storage pond

15.5 There is some uncertainty in the PCSR concerning the long-term storage of irradiated fuel on the site. The policy has implications in terms of the initial number of fuel storage positions and the possible need to add further storage positions, probably in the presence of irradiated fuel already stored. Associated with this is a decision on the final overall size of the fuel storage pond. The intent should be agreed before licensing because of the possible impact on construction and on transportation arrangements.

Loss of cooling

15.6 It is proposed to disconnect the irradiated fuel storage pond from its cooling system for certain operations. When there is substantial fuel present, the heat generated could cause significant water temperature rise and evaporation. The effects of the water vapour on the ventilation system have not been evaluated nor the potential effects of high temperatures on the pond structure. The Inspectorate understands that this problem is recognised and is being re-examined by the CEGB.

Maintenance of sub-criticality

15.7 Sub-criticality in the storage ponds should always be guaranteed. This is achieved, as described in the PCSR, by various means. They include the use of soluble boron dissolved within the cooling water, physical isolation, and suitable design of the fuel storage racks including built-in absorber. The design intent is generally acceptable but the details of the criticality safety case remain to be assessed when a report under preparation by the CEGB is received.

Flask movement

15.8 An acceptable analysis of the movement of the loaded irradiated fuel transport flask is not made in the PCSR. Two main aspects require attention. One is the evaluation of the consequences if the flask itself is damaged due to mishap. The other is the evaluation of the damage the flask might do to various associated structures, particularly damage which would result in loss of cooling to the remaining irradiated fuel within the fuel storage plant.

Failed fuel

15.9 The procedures for dealing with failed fuel have not been adequately described in the PCSR. Further information should be provided, to include the treatment of fuel which is identified as having failed within the reactor, as well as fuel which fails in storage.

External hazards

15.10 The Inspectorate is concerned that the effects of seismic shock on the pond structures appear not to have been considered, whilst noting that measures are proposed for the detection of water leakage from the pond structure.

Radiation dose to operators

15.11 The control of radiation dose to station personnel during fuel storage and handling operations has been included in the radiological protection assessment reviewed in Section 14.

Conclusion

15.12 While many aspects of the safety case presented are acceptable at this stage of licensing, there are areas affecting the strategy and the engineering design information about which the Inspectorate has reservations. Some questions are raised because of inadequate presentation of the safety case, while other issues, although presented in enough detail for assessment at this stage, nevertheless fall short of requirements. While some issues need to be considered prior to construction, the remainder should be resolved prior to operation.

16 Safety analysis

Introduction

16.1 A large part of the PCSR, namely Chapter 15, is devoted to the analysis of faults. The analysis is done by determining the range of potential faults and examining those faults to ensure that the plant includes adequate provisions for dealing with them. The overall aim is to show that the full spectrum of potential faults has been covered and that the likelihood of a fault terminating in a release of radioactive material has been reduced to a low enough level consistent with the size of the release.

16.2 The main potential for the release of radioactivity from the plant arises from the escape of fission products from within the fuel and thence from the primary circuit. Fault and event trees have been drawn up for selected faults and studies have been done by the CEGB to determine the transient behaviour of the reactor primary circuit and core components, in particular the fuel, during the course of the fault. These studies take into account the behaviour of the secondary circuit and of the various protection systems that may come into play and affect the probability and magnitude of a release to the atmosphere.

16.3 Despite the provision of a protection system, there is the possibility, however remote, that it might fail. A significant part of the safety analysis involves the production of fault and event trees tracing fault sequences which allow for possible failures of systems, and determining the effect these failures will have on the potential outcome. In principle, if the outcome is unacceptable a further line of defence could be added to the design. There is a point, however, when the likelihood of the sequence of failures becomes so remote that this is not justified.

16.4 In the safety case, the CEGB has drawn a line between those fault sequences for which the protection is claimed to be sufficiently effective (the design basis faults) and the remaining remote sequences which are 'beyond design basis faults'. There is a further class of faults, the CEGB's so-called 'incredible' faults, which may be regarded as a sub-class of 'beyond design basis' faults. These faults are claimed in the PCSR to be so remote that protection against them need not be considered. These claims generally relate to failures of pressure circuit parts and, as such, are assessed in Section 10 of this review.

16.5 For the protection against design basis faults to be judged effective the Inspectorate would expect it to be shown that, at the frequency attributed to the fault sequences, the resultant radioactivity releases are within the CEGB's design criteria. Part of the demonstration of this involves analysing the transient behaviour of the plant in relation to fuel and other plant limits. (The transient analysis is discussed in paras 16.64 *et seq.*)

16.6 In the case of faults or fault sequences beyond the design basis it is necessary to show that their contribution to the overall risk from the plant is acceptably small. The CEGB goes some way towards this in the PCSR by developing fault trees covering sequences generated from a selection of fault initiators and estimating the contribution to the risk.

16.7 'Incredible' faults are not covered by fault or event trees, the safety case for those plant items being covered in the relevant chapters of the PCSR.

16.8 An important feature of the safety case presented in the PCSR is that, in general, it makes no claim for the performance of any of the plant when taken beyond its design basis. Going beyond the design basis means entering an area of uncertain consequences and hence, in the Inspectorate's view, the pessimistic assumption has to be made that an uncontrolled release of radioactivity may result. It is recognised that in many cases this is grossly pessimistic, but it is adopted at this stage of the assessment as a matter of prudence. Further analysis would be expected to show a less serious outcome for some of these faults with a consequent reduction in their contribution to the risk.

16.9 It is evident from the PCSR (Chapters 2 and 15) that this pessimistic approach was intended by the CEGB. In the production of the fault trees, however, it appears that the intention has not been fully implemented in practice. An additional class of fault has been introduced comprising sequences which are beyond the design basis but which, it is claimed, will not lead to a significant release of radioactivity. Those sequences have not been included in the fault trees and hence do not contribute to the estimated frequency of an uncontrolled release. The Inspectorate's view is that, as presented, this procedure is unsatisfactory and has led to an inconsistent presentation of the safety case. It raises questions about some of the results of the fault tree analysis and, as a consequence, about conclusions drawn about the risk from beyond design basis faults. The Inspectorate would wish to see further work done here to resolve the anomaly.

16.10 The fault sequences, transient and probability analyses presented in Chapter 15 of the PCSR and in the supporting reports, comprise a substantial amount of material and the time required to deal with this, together with the late receipt of some of the reports, has meant that assessment of this work is not complete and hence the views presented here can only be provisional.

Fault schedule

16.11 The fault schedule presents a list of initiating events based upon, but more extensive than, lists produced in safety reports for previous PWRs. The schedule also includes a summary of the protection provided and this is discussed briefly in Section 11 of this report. In the PCSR these events are placed into 12 categories:

(a) Inadvertent reactor trip

(b) Increase in heat removal by the secondary system

(c) Decrease in heat removal by the secondary system

(d) Electrical supply faults

(e) Decrease in reactor coolant system flow rate

(f) Reactivity and power distribution anomalies

(g) Increase in reactor coolant inventory

(h) Decrease in reactor coolant inventory

(i) System-related faults

(j) Radioactive release from a sub-system or component

(k) Internal hazards

(l) External hazards

16.12 While not included in the schedule, 'incredible' faults have been listed in Chapter 2 of the PCSR, although the list is probably not yet complete. In several cases, notably steam generator (SG) tube rupture, the Inspectorate is not yet satisfied that the specification of the design basis fault covers a sufficiently severe event. Overall it is considered that there are a number of omissions from the fault schedule and the shortcomings are expected to be rectified in later submissions.

Fault analysis

Fault sequences

16.13 Each of the initiating events listed in the fault schedule can give rise to a number of fault sequences depending upon the state of the plant, the severity of the fault, the effect of control systems, other plant failures, etc. Of these initiating events, the 12 shown below have so far been subjected to event tree analysis in the PCSR. The corresponding category in the list of para 16.11 is shown in brackets, from which it can be seen that only six of the 12 categories are represented.

Inadvertent trip (a)
Steam line break inside containment (b)
Steam line break downstream of MSIVs (b)
Loss of main feed (c)
Inadvertent closure of MSIVs (c)
Feedline break (c)
Loss of all 11 kV supplies (d)
Small LOCA (h)
Large LOCA (h)
SG tube rupture (h)
Loss of all CCW (i)
Loss of main cooling water supply (i)

Event trees

16.14 The main purpose of the event trees presented with the PCSR is to identify explicitly, at the system level, those sequences within the design basis (the success paths) which then require justification by transient analysis of the claim that they lead to a safe shut-down state. The event trees also identify those sequences which go beyond the design basis (the failure paths) which are subsequently analysed by means of fault trees.

16.15 The 12 event trees presented with the PCSR are claimed to be representative of many other faults. Trees have not yet been drawn, however, for reactivity faults, radioactive waste storage plant faults and those involving internal and external hazards.

16.16 The methodology adopted employs several techniques for reducing the size of the event trees to manageable proportions. These include division of the tree into two parts (initiating and safeguards event trees), application of a low frequency cut-off, multiple branching, and the recombination of divergent branches where these are claimed to be equivalent. These techniques are acceptable in principle but the Inspectorate has reservations about the details of their application. In particular, the low frequency cut-off level of 10^{-7} per year appears to be too high, when applied to a tree in which a large number of branches are terminated in this way, in view of the CEGB's target of 10^{-7} per year for each group of initiating faults.

16.17 Event trees require analysis of the transient behaviour of the plant, firstly as an input to determine the expected sequence of actions, and secondly to demonstrate that design limits are not exceeded for the claimed success paths. From the Inspectorate's examination of the submissions provided so far, it should expect to see a better connection established between the event trees and the transient analysis. Each of the claimed success paths should be clearly identified with a transient analysis which is claimed to bound it.

16.18 The events considered in the tree are generally limited to systems required to operate and they exclude consequential passive failures, operator errors and systems which, while not required to operate, may in fact do so during the course of the fault. The latter may be significant where, for example, a relief valve or a pressuriser spray valve may open and then fail to reclose.

Fault trees

16.19 Fault trees have been produced in the PCSR corresponding to 11 of the faults listed in para 16.13, i.e. excluding steam generator tube rupture. The fault tree analysis gives information both about the basic failure modes and the probabilities of achieving the top event of the tree (plant failure) or subordinate gates of the tree, where these are of interest. The analysis enables an estimate to be made of the combined frequency of all failure paths for a given initiating event. The fault trees are developed at two levels, one identifying the functions involved and the second evaluating, down to component level, the routes whereby those functions might fail to be provided.

16.20 A radioactive release occurs because the protective systems provided to guard against plant failure do not perform their duty adequately. This information is implicit both in the functional fault trees and also in the event trees; consistency between the two should be demonstrated for all 11 faults. This has so far only been considered in the case of inadvertent reactor trip (ref. 53).

16.21 System fault trees are a distillation of a study of the possible fault situations for the system. The trees by themselves provide too terse a summary of these studies to allow a judgement of their completeness to be made, and they should be backed by failure mode and effect analyses linked to the system description.

16.22 Analyses of the fault trees for individual protective systems have not been given. The Inspectorate expects to see failure modes for each system in terms of its component parts and support services derived, so that a picture of the overall failure pattern can be constructed and any weak systems identified. The present method of analysis identifies only weaknesses in certain support services without reference to the systems they serve. While overall plant failure probabilities are given, the omission of system level information makes assessment of individual systems difficult. The CEGB has given a commitment to provide further information in order to make good this deficiency.

16.23 System fault trees have been drawn up which so far exclude several types of fault, for example control system faults and faults in a number of common services, as well as human error. The significance of these omissions will not be known until more information has been provided and analysed.

16.24 The code used in the analysis of fault trees is WAMCUT. This code uses a probability cut-off for minimal cut-sets and the Inspectorate is concerned that the cut-off value used may lead to potentially important cut-sets being missed. Overall, there appear to be no obvious drawbacks with this code but validation of the code should be provided in due course.

16.25 The failure rates quoted in the PCSR are for relatively broad categories of components, rather than being specifically related to the components. As far as the fault tree analysis is concerned the use of such generic failure rates is acceptable in principle at this stage of the design, but special attention will need to be devoted to ensuring that the assumed reliabilities can be achieved in practice, and maintenance and testing proposals will need to be carried through to the procedures eventually adopted on the plant.

NII effective barriers assessment

General comments

16.26 Satisfaction of the NII's safety assessment principles in relation to effective barriers is, as discussed in Section 3, an important aspect of the Inspectorate's assessment of the safety case for any nuclear plant. The fault analysis submission in the PCSR does not immediately provide the information necessary to allow a proper assessment in this area and what the Inspectorate has been able to accomplish has also been limited by the short time available. Hence, the present conclusions give an interim view, to be revised when time and the provision of better information allow, which for all significant aspects should be before a decision on licensing is made.

16.27 The basic principles used by the Inspectorate in making judgements on the adequacy of safety provisions are given in Part 2 of the Safety Assessment Principles document. Principles 13 to 15 relate to radiological doses less than the emergency reference level (ERL). Fault sequences leading to such comparatively small doses are not systematically addressed in the PCSR, the intention being to treat the question at a later stage. This is acceptable, and a judgement on this consequence band has not been made by the Inspectorate at present. The principles require the ERL to be made 'as remote as reasonably practicable' and the requirements of the safety provisions in terms of effective barriers, against which such faults are assessed, are given in Principle 26. For fault sequences at this level of severity which are judged to have a frequency of occurrence greater than once in a reactor programme there is a requirement for two effective barriers, while for less frequent faults one barrier is deemed sufficient. When two barriers are required, they are expected to be independent and diverse.

16.28 An effective barrier is essentially a set of engineered provisions which will prevent a release of activity for a given fault sequence or reduce the release to an acceptable level. This set includes all the systems, e.g. power supplies, component cooling and control systems, required to support the protective systems directly involved, and also includes any operator actions required. The barrier defined in this way bears no simple relationship to physical barriers to the

release of radioactivity, such as the fuel cladding or the reactor coolant circuit boundary.

16.29 The NII's principles in general require highly reliable barriers, a well proven barrier being expected to have a reliability of about one failure in 10^4 demands. Where two barriers are required, but where this is a marginal requirement, a somewhat lower reliability might be acceptable for one of the barriers. Where only a single barrier is required but the sequence frequency is low (much less than once in a reactor programme) the Inspectorate might be prepared to accept a lower reliability requirement for that barrier.

16.30 Safety provisions which satisfy the probability targets of the CEGB's design safety guidelines are expected generally to satisfy the NII's barrier requirements, but individual cases need to be assessed on their merits. While the assessments discussed here are based upon studies supporting the PCSR, certain plant and test procedure changes proposed recently, but not yet assessed, could improve the protection provided and alter these conclusions.

Diversity of decay heat removal (DHR)

16.31 A general area in which our examination of the provision of safeguards against frequent faults so far indicates that the requirements for two diverse barriers are not met concerns decay heat removal with the RCS at pressure. Although there is diversity in feed and steam dumping, reliance is placed on the steam generators (SG) for heat removal from a pressurised circuit. The SGs provide a highly reliable heat removal route, but failure of all four units is possible, though most unlikely.

16.32 The Inspectorate's basic approach is that reliance should not be placed on a single redundant system when high reliability is required, even though no specific common failure modes can be foreseen.

16.33 In fact there is the possibility of a diverse heat removal route, known as 'bleed and feed', in which steam is released from the primary circuit via a pressuriser power operated relief valve (PORV) under operator control and cold water is injected by the high head safety injection (HHSI) pumps. Bleed and feed is described in the PCSR but no credit for it is claimed in the safety case. If the procedure could be substantiated it might be acceptable for many, if not all, cases where a second barrier is required.

Emergency charging system

16.34 One important system which appears as a barrier element for several faults is the emergency charging system (ECS). As specified in the PCSR, the ECS has only one pump and hence would have inadequate reliability, as well as violating the single failure criterion. The CEGB has recognised the weakness of this system and is to redesign it with two pumps to a target reliability of 10^{-3} failures per demand (see para 11.47).

Diversity of shutdown

16.35 Because of the lack of diversity in the control rod system, there is a significant set of sequences involving failure of this system (ATWT) for which the effective barrier principle has not yet been shown to be met. This problem is discussed in some detail in paras 11.33 *et seq.* and 16.126 *et seq.*

Systems interactions

16.36 There is the possibility in this plant, as in others, of unexpected failure of equipment, plant components, etc., as a result of interactions between systems. Such interactions can occur for a variety of reasons and, in order that any need for changes to the plant can be recognised, or further precautions provided, at an early enough stage, an examination of the design is necessary from the following viewpoints:

(a) Spatial interactions—escalation of failures can occur as a result of the proximity to failed buildings, systems or components due to either impact or changes in local ambient conditions.

(b) Functional interactions—where systems are linked, performance faults or other failures in one system could lead to unacceptable performance or even failure in one or more of the linked systems.

(c) Operational interactions—the operator provides a link between many independent systems and, as experience shows, both his actions and the written procedures on which his actions are based are subject to human error, which can lead to unacceptable interactions.

(d) Hazard-induced interactions—the contribution of both internal and external hazards towards interactions between both buildings and systems needs consideration, since segregation and separation can be adversely affected by such events.

16.37 At the present stage of its development, the design does not include many detailed aspects of plant lay-out; incomplete information is available on auxiliary and service system pipework, on power supplies and on control systems; operating procedures are not yet available and a full consideration of hazards has still to be undertaken. In view of this, only limited progress on systems interactions is to be expected. However, while accepting that there will be some difficulties in carrying out a comprehensive examination of systems interactions, the Inspectorate wishes to see a more systematic approach to this topic than is presented in the PCSR. The CEGB should carry out a sufficiently comprehensive study, before licensing, of any aspects which would be difficult to correct after the main features of the design are frozen. A longer term commitment is also required, to ensure that the as-built plant satisfies the design intent and that possibilities of

interaction have been foreseen as far as is reasonably practicable.

Barrier assessment for selected faults

16.38 The Inspectorate has assessed the adequacy of the barriers for five of the faults for which fault and event trees have been submitted. These cases are discussed briefly below. Any judgements made here exclude consideration of contributions from common services and from systems interactions which have not yet been identified. They are also subject to satisfactory resolution of any reservations expressed elsewhere in this report on engineering aspects of the system.

(a) Main steam line break (MSLB) inside the containment

16.39 This fault leads to pressure and temperature loads which approach the design limits for the containment and it also has the potential to cause steam generator (SG) tube failures which would increase those loads. The claimed frequency of the fault is 10^{-4} per year, which would give a requirement for a single effective barrier.

16.40 The actions required to protect against the basic MSLB (without SG tube failure) and to reach cold shutdown have been identified from the event tree and transient analysis in the PCSR, and these constitute some 18 barrier elements. Applying a common mode failure limitation of 10^{-4} failures per demand (f/d) to most of these elements (a few incorporate diversity) could add up to a significant failure probability for the barrier. In addition, some elements are expected to have a lower reliability. These include MSIV closure, containment spray, isolation of charging line, SG PORV operation for cooldown, and termination of HHSI, the last two being subject to the possibility of maintenance or operator error. Thus the overall barrier reliability appears to fall short of the expectation of the NII's principles though further work needs to be done before a firm conclusion can be reached.

16.41 The case of MSLB with consequential SG tube failure is outside the design basis in the PCSR, which means that no effective barrier has been demonstrated. The PCSR does give a sensitivity study for a single SG tube rupture with MSLB, but the Inspectorate has reservations on this analysis (see para 16.139 *et seq.*). Compared with the basic MSLB, the case with a single SG tube rupture would involve more stringent requirements on containment systems and on auxiliary feedwater (AFW) isolation and also some additional operator actions. The consequential reduction in barrier reliability would have to be judged against the lower frequency of the sequence, but examination suggests that an effective barrier could be demonstrated for this case. There is, however, a concern that multiple SG tube failures could occur with a MSLB (see Section 10), albeit at an even lower frequency. The Inspectorate has not yet come to any conclusion as to whether a sufficiently reliable effective barrier can be found for this case. Further work needs to be done on this fault to refine the analysis in relation to the radioactive release which might occur, to obtain a better understanding of the failure limits of the containment, and to improve the prediction of SG tube failure when subjected to the loads produced in this accident.

(b) Steam generator tube rupture

16.42 The design basis fault is a single ended rupture of one SG tube at a claimed frequency of 10^{-3} per year, which puts it on the borderline between the one and two barrier requirements. It is clear that only a single barrier is provided and the Inspectorate's assessment is directed towards its effectiveness. The main concern is the escape of radioactive primary coolant to the atmosphere via the failed tube and a secondary circuit relief valve.

16.43 Although the operator is not required to act for 30 minutes, it is expected, nevertheless, that he will act as quickly as possible to isolate the faulty SG and bring the plant to cold shutdown (about seven main actions) in order to minimise the release of primary coolant activity. Hence the probability of operator error is judged to be higher than for other faults in which he has fewer actions to perform and when the timing of those actions is not critical.

16.44 The reliability of the automatic protective actions is likely to be adequate, but the overall failure probability of the barrier may be dominated by operator error and it could be too high for a single barrier at this fault frequency. Further work needs to be done on the analysis of this fault; e.g. it may be possible to justify some reduction in the assumed fault consequences and to explore ways of minimising the possibility of operator error.

(c) Loss of component cooling water (CCW)

16.45 The main feature of this fault is that it results in the loss of a large number of operational and protection systems, including the reactor coolant pumps (RCPs), chemical and volume control system (CVCS), containment spray and fan coolers, motor driven AFW, HHSI and residual heat removal system (RHRS). Thus the only state in which the plant can be maintained is intermediate shutdown. The claimed frequency of 10^{-4} per year implies the need for a single effective barrier.

16.46 Two cases are considered, both starting with the plant at power. These are loss of CCW with no further faults and the grouped set of loss of CCW with all further failures identified on the event tree.

16.47 In the first case the barrier comprises some eight elements. These include RCP trip on motor bearing temperature (which is not protection grade), the ECS (which, it is assumed, will be upgraded from the PCSR specification, see 16.34 above), the press-

uriser heaters (which need to be available in the long term) and the fuel storage pond make-up. Subject to the provision of substantiated reliability figures for the systems involved, the barrier is likely to be acceptable.

16.48 The second case includes loss of controlled main feed and a variety of additional failures giving secondary side depressurisation. The combined frequency of this set of sequences is estimated from the event tree to be about 3×10^{-5} per year. Sequences with blowdown via two SG relief valves would normally require HHSI for RCS make-up and, since this is not available, it is recognised in the loss of CCW study (ref. 54) that the ECS will need to be shown to be adequate for this duty. It will also have to be shown, however, that the high shut-off head of the ECS does not invalidate the excessive cooldown analysis. The barrier elements additional to those for the first case comprise some seven protective actions. The overall reliability of the barrier for this second case is likely to be low enough to raise doubts about its effectiveness, but the low frequency of the set of sequences may permit a somewhat less onerous reliability requirement than for a more frequent fault.

16.49 This fault will need to be reassessed in the light of changes now proposed to the CCW system.

(d) Small LOCA

16.50 The concern for small LOCA is twofold. The radioactive primary coolant which is released to the containment could, with additional failures, escape to the atmosphere. Secondly, the loss of coolant could, with failure of the ECCS, lead to the core being uncovered and the possibility of meltdown. In either event the potential release would lead to a radiation dose greater than the ERL. As with SG tube rupture, only one barrier is provided, although the claimed fault frequency of 10^{-3} per year puts it on the borderline between requiring one and two barriers.

16.51 The main elements of the barrier are reactor trip, the containment systems, the ECCS and the AFS. The combined probability of the possible modes of containment failure in the original fault tree analysis was estimated to be 1.5×10^{-2}f/d, and design and procedural changes have been proposed by the CEGB to reduce this value. However, it still remains to be shown that, with the changes proposed, the containment now constitutes an effective barrier.

16.52 Given the initiating small LOCA, the subsequent probability of a degraded core is estimated in the PCSR as about 1.4×10^{-3}, allowing for proposed improvements in test frequencies. This indicates an unacceptably weak barrier for a fault of this frequency. It has not yet been possible for the Inspectorate to identify the dominant contributors to this high failure probability from the analysis submitted, but a large factor appears to derive from the CCWS, which is required to support a number of the ECCS and AFW sub-systems.

16.53 Further consideration will need to be given to this fault sequence, particularly in the light of the proposed changes to the CCW system which should improve the position.

16.54 The case in the PCSR for the 'interface LOCA' of the Rasmussen study (ref. 7) needs to be strengthened. Modifications are now proposed by the CEGB to the isolation between the primary circuit and the RHRS which should make an improvement. However, the Inspectorate requires further study to be done on this fault.

(e) Inadvertent reactor trip

16.55 This fault involves the spurious generation of a reactor trip signal during normal operation. It is assumed to occur ten times per year and therefore requires two effective barriers. Subsequent failures can lead to LOCA, ATWT or sequences involving rapid cooldown of the primary vessel. Most such sequences are of sufficiently low frequency to require only one barrier.

16.56 Two sequences however cannot be treated in this way. ATWT sequences may lead to a degraded core unless the emergency boration system, together with sufficient primary pressure relief, operates and stringent feed conditions are met. Pump seal LOCA sequences need two barriers for seal protection since loss of cooling to the seal may often be accompanied by loss of cooling to the containment functions, the most important safeguard function following seal loss.

16.57 These special requirements, together with the general requirements for the initial inadvertent trip fault, lead to the requirement for two barriers each involving ten elements. Of these, eight diverse provisions are available in one of which, it is assumed, the ECS will be improved as noted in para 16.34, otherwise the seal protection element of the barrier would be unacceptable. Neither pressuriser heating nor the RHRS have diverse alternatives; the two barrier criterion can be met only if the two states (intermediate and cold shutdown) which require these two functions are regarded as alternatives. However, when cold shutdown is necessary, once or twice a year, the single non-diverse RHRS is required. In order to satisfy the NII's barrier principles, either the possibility of returning to and maintaining intermediate shutdown, as put forward in the PCSR, should be established with a high degree of reliability, or an alternative mode of removing decay heat needs to be demonstrated. Barry (ref. 55), for example, considers several alternatives.

Conclusions from fault analysis

16.58 The Inspectorate welcomes the considerable effort which has been devoted to producing the probability analysis in support of the safety case and the

attempt made to show that the design meets the probability targets in the CEGB's design safety guidelines. The fault and event tree analysis is extensive and NII has so far assessed only a part of it. Furthermore, a revision of the fault trees has recently been received and is awaiting assessment. The Inspectorate's comments and conclusions at this stage can, therefore, only be regarded as provisional.

16.59 The analysis has made a valuable contribution to the safety case. However, the selection of faults analysed is not yet complete in that it does not contain representatives from some potentially significant classes of fault. The analysis also has limitations in that it excludes protection initiation systems and many support services, operator errors and consequential passive failures, such as breach of steam generator tubes.

16.60 It is necessary for the CEGB by analysis in the safety case to show that individual fault sequences meet the intent of its design safety guidelines, or else to justify those cases where this cannot be demonstrated. So far, the PCSR addresses only 11 faults and a number of these apparently fail to meet the CEGB's 10^{-7} year target by more than an order of magnitude. The required coverage of the entire spectrum of potential faults must eventually allow assessment against more detailed consequence/frequency requirements.

16.61 The Inspectorate has carried out some limited assessment against its effective barriers requirements. There is insufficient information available so far on which to make firm judgements, though it is clear that some of the CEGB's proposed design changes will help to remove shortcomings shown up by that assessment. However, other potential shortcomings remain, for example in relation to sequences involving many operator actions, and in due course the Inspectorate will need to be satisfied, for example by well defined procedures or by suitable plant provisions, that effective barriers can be demonstrated.

16.62 The overall approach to locating and taking account of potential systems interactions will also need to be improved. Any aspects in these areas involving significant implications for the plant design will need to be cleared before licensing.

16.63 Finally, it should be noted again that the judgements made here are subject to satisfactory resolution of issues arising from the Inspectorate's assessment of the engineering of the systems involved in the fault analysis.

Transient analysis

16.64 In the safety analysis there is a discussion on the division of faults between those within the design basis and those outside it. For those faults within the design basis, it is claimed in the PCSR that the fault consequences satisfy the CEGB's criteria. To demonstrate this, the transient behaviour in design basis faults is studied in Chapter 15 of the PCSR. Part of Chapter 4 claims to show that the starting point used for the transient analysis represents the bounding limits to the range of conditions which might be met during the life of the plant. The design basis fault transients aim then to satisfy another set of limits, chosen to ensure that only a limited amount of fuel failure occurs so that any release of radioactive material to the atmosphere is within the CEGB criteria. In Section 7 of this report the Inspectorate expressed reservations about the bounding limits and about the fault limits. The assessment of fault transients reported here was done within the confines of the information provided on transient analysis in the PCSR, but any conclusions drawn are subject to the reservations of Section 7, which has implications for the whole of that analysis.

16.65 Reactor faults can broadly be divided into those involving loss of coolant (LOCA) as the initiating fault and other, non-LOCA, faults. The former have, in the history of PWRs, been subjected to more study since, in general, the latter can, in any case, endanger the public only in the event of some subsequent release of coolant from the primary circuit.

16.66 Loss-of-coolant accidents tend to be associated with gross failure of the primary pressure circuit, but less improbable events can occur involving, for example, release of coolant through the power operated relief valves (PORVs) or the safety valves. Other release mechanisms include failure of steam generator tubes, leading to escape of primary coolant to the steam generator secondary side, and failure of pump seals.

16.67 Most of the remaining transient studies involve sequences which could lead to conditions resulting in failure of the fuel in what is essentially an intact circuit, although a number of these could then lead to high primary circuit pressures which might result in PORV operation and the possibility of release. Other studies examine transients which might pose a threat to the integrity of the primary circuit and hence turn into a LOCA. These types of fault are discussed in para 16.103 *et seq*.

Loss-of-coolant accidents (LOCA)

General

16.68 The Inspectorate devoted significant effort to this fault at the time of the generic review. In principle, the fault is the same, though the systems provided for dealing with it have changed. In the generic review the desirability of considering alternative, potentially better, ECC systems was pointed to. In particular the system adopted in Germany, which

pumped cooling water to both hot and cold legs, appeared attractive. The CEGB, however, has chosen to stay with cold leg injection on the grounds that this is a well studied design. The argument is accepted by the Inspectorate, in view of the improvements made to the ECC provisions.

16.69 The process occurring during the course of the fault were described in the generic review and are further described in the PCSR. This report does not repeat that discussion but limits itself to a review of the points arising from the assessment of the LOCA safety case documents which the Inspectorate has so far assessed. In addition to examining the effect of LOCA transients on the fuel, the loadings on the containment due to temperatures and pressures produced by the steam release in the LOCA and the potential radiological consequences of the faults have also been assessed.

16.70 The detailed analysis of loss-of-coolant accidents has long been recognised as difficult. Over the years, the complexity of the theoretical models describing the system has increased both in the degree of detail in terms of the number of nodes and in the representation of two-phase flow processes, which has changed from a homogeneous equilibrium description to a variety of two-fluid models. Despite these advances there are still many areas of uncertainty. The standard approach for dealing with these has been to use models for the analysis which have been pessimised according to rules established initially by the Nuclear Regulatory Commission (NRC) in the USA. One of the problems with this approach is that these so-called evaluation models do not describe the physical processes particularly well. It is also difficult to determine how conservative the results are.

16.71 At the time of the generic review the Inspectorate expressed a preference for codes based upon a proper physical description of the fault processes. With such codes the aim is to get a best estimate of the transient, to which appropriate safety factors can be applied. In the event, such codes have not been developed sufficiently and the evaluation model approach has been used in the PCSR.

Assessment

16.72 The overall aims are to be satisfied that the analysis has covered the full range of potential LOCAs, that, after making appropriate assumptions about plant availability and performance, the conditions stay within specified limits, and that the calculational methods give results of an acceptable accuracy.

16.73 With regard to the specified limits, those chosen in the PCSR were produced by NRC for licensing purposes in the USA. The criteria used relate to the peak fuel temperature reached in the course of the LOCA and to the degree of oxidation, both local and core-wide, which must not be exceeded. The Inspectorate has required the CEGB to justify these and other criteria used in the safety case. A brief discussion of the criteria is given in Section 7 of this report.

16.74 A wide range of LOCAs are studied in the safety submissions. They range from those with very small leak rates, which are within the capacity of one charging pump, up to failure of the major primary circuit pipes. Within this range there are sensitivity studies aimed at confirming the choice of bounding fault and investigating the uncertainties referred to earlier. However, the link between the sequences studied and the output of the fault and event tree analysis is not made clear. It is difficult to assess, therefore, whether the range of faults analysed is adequate but, from the Inspectorate's preliminary work, it appears to be so.

16.75 The LOCA safety argument rests almost entirely on computer calculations. In view of the difficulty in understanding physical processes like blowdown, refill and reflood, and modelling them for a plant as complex as a PWR, the Inspectorate considers that the main question to be addressed concerns the adequacy of the calculation methods. The calculations are claimed to be conservative. The approach used is to impose a bias on dominant parts of the calculation to an extent which is claimed to outweigh the uncertainties and produces an overestimate of clad temperatures. However, concern was expressed in the generic review that conditions might be produced during a LOCA which would invalidate the claims to conservatism of the evaluation models. In particular, the possibility was suggested of a LOCA transient which might cause the fuel cladding to balloon so that it could no longer be cooled and sooner or later would exceed the temperature limit. This topic is discussed in Section 7.

Validity of LOCA calculations

16.76 In view of the importance of the code calculations, the Inspectorate has laid great stress over the period of this review on the need for the CEGB to provide validation of the codes used in the LOCA safety case. To date only part of the validation package has been received. Confidence in the CEGB's calculational methods should be enhanced when the whole of it is available. In the meantime, those problems highlighted as a result of this review are discussed below.

16.77 Small breaks have received more attention over the last few years, but any doubts about the calculations tend to be overcome by the proposed HHSI provisions which result in large safety margins to the fault limits being calculated. Therefore, the modelling of the codes would need to be seriously in error in order for the situation to be unacceptable. No phenomenon has been identified to date which would give a large enough effect to do this, though small break phenomena are still being investigated. The code

validation package is expected to enhance confidence in this area.

16.78 As the break size studied is increased, a change occurs in the dominant flow regimes. This change is not sufficiently explored in the PCSR when analysing intermediate sized breaks. The current calculations, however, provide some assurance that intermediate sized breaks will not prove to be limiting faults.

16.79 The numerical representation in the LOCA codes is another matter of some importance. The properties of stability, convergence and accuracy are requirements of the codes. The safety submission needs to be improved in this area. It would greatly increase confidence in the codes if some indication of their numerical accuracy could be given. In the safety submission it should be acknowledged that the LOCA codes used do not give a converged solution and give reasons for the coding scheme chosen. The sensitivity studies used to demonstrate large break convergence are not entirely convincing. For small breaks nothing has been done in this area. The Inspectorate requires this aspect of the case to be improved before licensing.

16.80 The codes contain numerous correlations and assumptions. The range of applicability and the accuracy of the correlations need to be given. Similarly, the limitations imposed by assumptions, such as thermal equilibrium, need to be considered.

16.81 The safety submission is based on codes proprietary to Westinghouse and there are no independent users of the codes, though they have been approved by the NRC. Confidence in the results would be greatly enhanced if the codes were open to outside use, as has been the case with the RELAP series of codes. Some comparison of proprietary codes and RELAP have been given. More comparisons are required in the code validation submission.

16.82 Confidence in the codes will also be enhanced when they can be shown to agree with simple well-instrumented experiments. Plant codes tend to lack the flexibility to do this. In the case where a code is based upon results from one facility, as applies to WREFLOOD and the FLECHT experiments, comparisons with similar experiments on a different facility are of particular interest.

16.83 To be acceptable, the codes must be able to make reasonable predictions of integral experiments. The USNRC have organised an extensive series of standard problem exercises which can be used to allow comparison with calculation. Westinghouse have participated with their proprietary codes, but the results have not so far been made available to the Inspectorate. The active participation of the NNC in the standard problems exercises organised by the CSNI of OECD-NEA is welcomed. They did not, however, use the proprietary codes on which the safety case is based.

16.84 The use of conservative codes makes validation more difficult and the steps in the validation procedure need to be clearly stated. Claims to conservatism need to be justified by estimating the uncertainties in the various areas of the calculation.

16.85 Finally, it is possible for errors to occur in procedures such as coding and the preparation of input data. Such errors have been found in many codes, including those produced by Westinghouse. The Inspectorate has asked, therefore, that the CEGB carries out an independent check of the safety case codes and the input data used. The Inspectorate will, in addition, wish to audit this activity.

Large breaks

16.86 This and subsequent sections comment on specific aspects of the transients studied in the PCSR.

16.87 The highest peak clad temperatures result from large breaks in the cold leg. The largest break considered gives a slightly lower temperature than the limiting case. For the limiting case a 200 °C margin to the fuel limits is calculated. This margin is in addition to the bias that is built into the calculations.

16.88 The clad temperatures during the transient depend on the power distribution in the core. In the PCSR, the CEGB claims to have found the limiting distribution. However, an explanation is required as to why a symmetric distribution is limiting in view of the asymmetric nature of heat removal during a LOCA.

16.89 In the PCSR the possibility of heat transfer degradation during a LOCA due to a swelling of the fuel clad is considered briefly. This issue will need to be taken further as part of the clad ballooning argument, since in its absence the present discussion is not sufficient.

16.90 With the present design of ECCS, the calculated clad temperatures are sensitive to leakage across the SG tubes. In view of this sensitivity the Inspectorate will need to be assured of a high level of integrity of SG tubes under the action of blowdown forces.

Small breaks

16.91 In the PCSR, the CEGB claims that a cold leg break is the worst of small break possibilities. The increased HHSI provision provides, as expected, a significant reduction in peak clad temperature. The remaining small break calculations produced no large sensitivities. Again, while welcoming the range of studies that has been done, the Inspectorate expects further analyses to be made in later submissions. In particular, the possibility of maloperation of the plant following the initiation of a small LOCA is likely to lead to a requirement for some sensitivity studies.

16.92 The proposed in-service inspection facilities have overcome the concern which the Inspectorate felt

about small breaks in the bottom of the vessel (see Section 9). The transient analysis that has been provided for this fault gives added assurance.

Stuck open pressuriser relief valve

16.93 Only the initial stages of this fault are considered in the PCSR and it is demonstrated that the DNBR criterion is not violated. The long-term behaviour in this fault is bounded by large breaks in the hot leg. The Inspectorate's concern about the frequency of this and other small LOCA faults is discussed in paras 11.47 *et seq.*

16.94 A stuck open PORV following a loss of feed fault is viewed as being important since it can start from initial conditions which are different from those currently assumed for small break LOCAs, and the Inspectorate expects the CEGB to give further consideration to this point.

Breaks outside the containment

16.95 Whilst most of the pipework directly connected to the primary circuit which lies outside the primary containment is small bore, the consequences of failure in terms of release of radioactivity can be significant. In the PCSR four such breaks are examined: failure of sampling lines, failure of lines in the let-down system, valve leakage into the RHR system, and steam generator tube rupture. The completeness of this list has still to be assessed. For breaks in the sampling and let-down lines, the leakage and hence the release of radioactivity is a direct function of the time taken by the operator to isolate the line.

16.96 Steam generator tube rupture is important in that there is no direct means of isolating it. The Inspectorate's concern over this fault has already been expressed in the fault analysis discussion (16.42 *et seq.*).

Containment pressurisation

16.97 During a LOCA a large quantity of heat will be transferred from the primary system into the containment. It will give rise to an increase in pressure there, with the potential for causing a significant deterioration of the leak tightness of that structure and the release of the radioactive products contained within it. However, from the PCSR it would appear that the limiting fault for containment pressurisation is not a LOCA but the main steam line break. This fault is discussed in para 16.103 *et seq.* and containment thermal hydraulics in para 16.139 *et seq.*

Pressure vessel integrity

16.98 The concern here is that the combination of the applied stress and temperature to which the reactor pressure vessel is subjected as a result of a LOCA would cause the vessel itself to fail. The Inspectorate is not yet satisfied that the limiting LOCA in terms of pressurised thermal shock has been identified in the PCSR and further information needs to be provided.* The limiting fault in this regard is not, however, expected to be a LOCA, though that still needs to be confirmed.

Conclusions

16.99 Subject to any further points arising from the Inspectorate's fault analysis assessment and to the comments made above, the range of LOCA faults covered in the PCSR and the safety case for them is judged to be generally acceptable. However, some faults which are stated in the PCSR to be beyond the design basis and which the Inspectorate considers could defeat the ECCS provisions have been identified, e.g. multiple SG tube failure consequent on a large break. The Inspectorate has further work in hand to see whether this can be accepted or whether further information will be required.

16.100 With the present limits, suitable safety margins are demonstrated in the PCSR. Resolution of the clad ballooning issue might, however, lead to a revision of the limits. This current view must therefore be seen as provisional.

16.101 The code validation package is available only in outline as yet and it is not possible to form an opinion on its acceptability. The Inspectorate has no evidence which would negate the claim for overall conservatism in the calculations. However, code validation is of particular importance to the substantiation of the LOCA safety case.

16.102 Finally, although it is not discussed in this section (see Section 18), in the Inspectorate's view it is important that the CEGB should gain access to information produced in international LOCA research programmes and should actively participate in on-going programmes in order to add to the data base necessary to support the LOCA safety case.

Non-LOCA faults

Introduction

16.103 For non-LOCA faults the Inspectorate needs to be satisfied on essentially the same general points as those already discussed in relation to LOCA: the range of faults covered, satisfaction about the specified fuel and radiological release limits, and the validity of the calculations. However, there is a difference in that for LOCAs the physical processes involved are so complex that the computer modelling problems can be difficult, whereas in most of the non-LOCA faults there is not the same degree of complexity and modelling is correspondingly less difficult.

16.104 The Inspectorate has questioned in Section 7 the justification of the fault limits specified and the input data which characterise the fuel in the initial conditions assumed for the fault calculations. Satis-

faction on the range of faults covered in the PCSR is again a matter to be covered under the longer term fault and event tree assessment. Thus most of the assessment discussed below will be confined to the extent to which the specified fault limits are satisfied. The fault categories covered here involve:

(a) increase in heat removal by the secondary system,

(b) decrease in heat removal by the secondary system,

(c) anticipated transients without trip (ATWT),

(d) reactivity and power distribution anomalies.

Increase in heat removal by the secondary system

16.105 This fault can be brought about by decrease in feedwater temperature or increase in flow, and by excessive increase in secondary steam flow, by means including failures of steam system pipework and inadvertent opening of steam relief or turbine bypass valves. The PCSR contains five faults in this category, the most onerous being rupture of the main steam line, which is discussed below.

16.106 No investigations have been presented in the PCSR on faults of this nature which have actually occurred on existing plant, such as the overfeeding on Rancho Seco in March 1978 (ref. 56). The need for such studies as background to the safety case has been put to the CEGB and a commitment has been given to review these incidents.

Main steam line break (MSLB)

(a) General

16.107 In the PCSR, breaks are considered both upstream and downstream of the main steam isolation valve (MSIV) but not in the region between the valve and the containment, where such a rupture is claimed to be incredible. (This claim is discussed further in Section 10.)

16.108 Depending upon the particular sequence, the MSLB can have important potential consequences in relation to the integrity of three parts of the plant: the pressure vessel, the fuel, and the containment. The escape of steam from the secondary side of the SG causes severe cooldown of the primary coolant and can subject the vessel to high pressure at low temperature and to a high rate of reduction in temperature. A reactor initially in the hot zero power condition may be returned to power, as a result of the positive reactivity feedback induced by the cooldown, with a resultant increase in fuel temperature. The escaping steam may place a pressure and temperature load upon the containment. Finally a MSLB occurring outside the containment has the potential for the largest release of radioactive material from design basis faults in this category.

(b) Assessment

16.109 The analysis of the faults presented in the PCSR was made using an iterative process between LOFTRAN and the 3D code TURTLE to take account of the effect of a stuck rod. A full code validation is required, to complement the PCSR submission, before licensing.

16.110 LOFTRAN assumes perfect mixing of the primary coolant and the injected HHSI fluid at the point of entry. If this did not occur then the pressure vessel walls might suffer greater cooling in the downcomer region. The Inspectorate expects the CEGB to investigate the effect of imperfect mixing.

16.111 In the SNUPPS design upon which the Sizewell B plant is based there is provision for injection of high concentration (20 000 ppm) boron solution from a boron injection tank (BIT) into the coolant. This provision has been deleted from Sizewell B with the result that, after the initial MSLB transient, there is a subsequent return to a significant power level. The Westinghouse TROJAN plant, which preceded SNUPPS, was provided with a shut-down margin greater than that proposed for Sizewell B (1.69 Niles compared with 1.3 Niles), the greater negative reactivity provision reducing the subsequent power rise. In addition, the PCSR calculation assumes that only one of the shut-off rods fails to enter the core. The Inspectorate expects the assumption to be that two rods would fail, which would produce a greater power rise.

16.112 The main argument in favour of deleting the BIT is that the DNBR limit, which is generally acceptable for other faults (though we have expressed some criticisms in Section 6), is not violated in the PCSR calculation of this fault. It is also argued that the high concentration solution used in the BIT can cause problems of deposition in cooler parts of the pipework. Despite these arguments, the Inspectorate has asked the CEGB for justification that it has done all that is reasonably practicable, specifically in relation to the BIT system and the shut-down margin.

16.113 As far as fuel integrity is concerned, it is concluded provisionally from the Inspectorate's assessment that the sensitivity studies show the design basis faults analysed to be bounding. However, a firm conclusion cannot yet be given since the assumptions about AFW and HHSI performance in the PCSR do not correspond to the Sizewell B design. The design offered should be an improvement, but this needs to be demonstrated.

16.114 For the pressure vessel integrity case, calculations are not presented to demonstrate that the faults are bounding. The Inspectorate will also need to be convinced that the assumption of availability of off-site power is conservative.

16.115 For MSLB inside the containment, sensitivity calculations have been made to determine the bounding fault in relation to containment integrity.

However, the assumption of water entrainment in the escaping steam will need to be shown to be conservative. It is clear from the studies that the successful closure of MSIVs is crucial to the integrity of the containment.

16.116 Consequential single or multiple SG tube failures are stated in the PCSR to be beyond the design basis for this fault. Although some sensitivity studies have been presented this matter has still to be resolved, as discussed in paras 16.139 *et seq.*

Decrease in heat removal by the secondary system

16.117 In the PCSR ten faults in this category are considered, the following three being identified as the most important as they require the greatest reliability of the engineered safety features:

(a) reduction in feed to all SGs—puts greatest demands on reliability of the AFW,

(b) closure of all MSIVs—greatest demands on reliability of primary and secondary circuit overpressure protection,

(c) main feedwater line break inside containment—greatest demands on reliability of systems to maintain integrity of the fuel, primary and secondary coolant systems, and containment.

The last of these faults the Inspectorate believes to be the most significant and it is discussed briefly below. The assessment and conclusions drawn are generally applicable to the group as a whole.

Main feedwater line break (MFLB)

(a) General

16.118 Depending on size and location of the rupture and on the plant conditions, this event could cause either cooldown or heat up of the primary circuit, with the heat up being considered the more important. Breaks could occur upstream (inside the containment) or downstream of the non-return valve (outside the non-return valve (outside the containment). Such a fault determines the minimum auxiliary feedwater requirements and presents a challenge to the pressure limits of the primary and secondary circuits and the containment. The latter is bounded by the steam line break fault.

(b) Assessment

16.119 Fuel integrity calculations claim to show that no boiling occurs in the primary circuit and the fuel does not suffer DNB. The Inspectorate expects to see further consideration given to SG tube failure in these faults, because of the increase in stress to which they are subjected as a result of the fault.

16.120 For main feedwater line failure occurring outside the containment, the fault is essentially the same but additional failures of non-return valves and main feed isolation valves are taken into consideration. The CEGB needs to justify bounding claims made in relation to the radioactive release for this fault.

16.121 The assumptions and data for the fault transient analysis are in general conservative. While some sensitivity studies have been provided they will need to be assessed by the Inspectorate before it can decide whether they provide an adequate appreciation of the margins involved.

16.122 The results of the cases for each fault category for which transients are produced show that plant limits are not exceeded and that boiling in the primary loop does not occur. However the claim that this case bounds a number of other cases requires further justification, preferably by carrying out transient analysis for the other faults.

16.123 During some faults the SG tubes uncover and the consequential reduction in heat transfer is of prime importance to the course of the transient. Only limited discussion of the modelling of the SGs is provided, despite the importance with regard to primary loop boiling and pressure relief through the PORVs and this omission should be rectified. A more detailed discussion is required and consideration also needs to be given to stuck open PORVs.

16.124 The return of the reactor to the hot shutdown condition following the initial transient should not, in principle, be difficult for these faults, though the discussion of this in the PCSR needs to be expanded. Details of the energy release and mass loss from the primary and secondary coolant are also required to check whether the pressuriser relief tank (PRT) capacity would be exceeded.

16.125 In the case of the 'reduction in feed to all SGs', it is accepted that loss of feed to all SGs bounds that to a single SG. Nevertheless there is the possibility of an asymmetric temperature distribution being developed in the core for the latter fault. Further analysis is required in support of the PCSR arguments.

Anticipated transients without trip (ATWT)

(a) General

16.126 Since the Sizewell B design possesses only one fast shutdown system with a reliability probably no better than 10^{-5} per demand, for frequent faults the Inspectorate would expect an additional means of shutting down, which could be by means of an inherent characteristic of the system. The PWR has a negative temperature coefficient of reactivity, which will effect shutdown. However, the CEGB has provided in the Sizewell B design an emergency boration system (EBS) which will provide an additional, but relatively slow, negative reactivity input when two or more control rods fail to insert.

16.127 It is necessary to show, for faults in the appropriate frequency range, that the plant protection

is acceptable in the event of failure of the main shutdown system to operate. The faults in which such failures occur are called anticipated transients without trip. In the PCSR, the ATWTs discussed are limited to initiating faults in the frequency range 10^{-1}/year or greater. Within that range seven have been selected as potential ATWT initiators and, of those, the design basis faults in the categories inadvertent reactor trip, reduction in feed to all SGs, and coastdown of a single reactor coolant pump, bound the rest of the initiators.

(b) Assessment

16.128 For the studies presented in the PCSR it has been shown that, while the EBS does little to reduce the severity of the initial pressure transient, it suppresses boiling in the hot leg and controls the subsequent recriticality and repressurisation long enough to enable the operator to effect more permanent shutdown. The results of the studies presented are generally satisfactory but they do not go far enough and the Inspectorate is left with a number of concerns expressed below and in Section 11.

(i) In the absence of a fast diverse shutdown system, ATWT events need to be studied in the frequency range at least down to 10^{-2} and possibly to 10^{-3} per year. The CEGB has given a commitment to extend the studies to cover this range and to modify the EBS if the existing design does not meet requirements.

(ii) The calculations in the PCSR use best estimate data, with a number of conservative assumptions. This is acceptable subject to the determination of the uncertainties in the predicted values of key parameters by a programme of sensitivity studies.

(iii) Justification is required for the primary circuit pressure limit applied to ATWT faults.

(iv) The discussion in the PCSR of the return of the plant to the hot-shutdown condition after an ATWT has occurred needs to be expanded.

(v) Justification is required for bounding claims related to the release of primary coolant into the containment and the radiological consequences of this.

16.129 The Inspectorate expects further information to be provided before a decision on licensing is made to satisfy these concerns and demonstrate an acceptable outcome for this range of faults.

Reactivity and power distribution anomalies

16.130 Faults in this category cause the fuel to generate power in excess of the cooling provisions. Such faults can be brought about by, for example, single control cluster withdrawal, withdrawal of banks of control clusters, or reduction in the degree of boration of the primary coolant. Two of these are discussed below.

Rod cluster control assembly (RCCA) bank withdrawal

(a) General

16.131 This fault involves the uncontrolled addition of reactivity to the core caused by withdrawal of RCCA banks. This causes a power excursion. A frequency of 10^{-2}/year has been assigned to this class of fault in the PCSR. The overpower transient has the potential for causing fuel failures, overpressurisation, and radiological release. The insertion rate studied is claimed to exceed the rate which can be achieved by the simultaneous withdrawal of two banks of rods, this being claimed as the maximum possible with the proposed design.

16.132 Faults have been studied in the PCSR starting from the subcritical condition, and including low power and power levels between 10 and 100%. For the latter a range of reactivity ramp rates has been studied.

(b) Assessment

16.133 While the results obtained appear acceptable, the information presented needs to be augmented in a number of ways:

(i) Justification is required for the claims made on maximum speed of control rod bank withdrawal and on the number of banks which can be withdrawn simultaneously. The withdrawal rate will also need to be linked to the reactivity rates assumed in the analysis.

(ii) Adequate supporting evidence is required for claims that Doppler coefficient and moderator temperature coefficient are pessimistic.

(iii) The effects of the trip parameters proposed for the Sizewell B plant, as distinct from the SNUPPS tripping scheme, will need to be demonstrated. The effects of tripping on each of the two lines of protection will need to be determined.

RCCA ejection

(a) General

16.134 This infrequent fault could occur as the result of mechanical failure of the pressure housing of a control cluster assembly causing ejection of the assembly and drive shaft. As a result, a rapid positive reactivity insertion occurs in the presence of an adverse core power distribution and a small LOCA. The initial transient is so fast that it is terminated only by Doppler reactivity feedback, and trip occurs well after the initial power spike has been terminated. Hence the effect of the initial power spike on the fuel can be dealt with separately from the subsequent pressure and temperature transient. This secondary transient is dependent on whether or not the hole is blocked. In the longer term the effects of a LOCA discharging through a 7 cm diameter hole need to be considered if the hole remains clear.

(b) Assessment

16.135 The extensive set of studies given in the PCSR and supporting documents includes sensitivity studies and the effect of assuming 1D and 3D neutron kinetics.

16.136 It is accepted that the analytical methods have given pessimistic results. However, the treatment of fuel failures may not be pessimistic since the DNBR fuel failure limit has yet to be shown to be conservative (see Section 7) and pellet-cladding interaction may provide an additional fuel failure mechanism.

16.137 A complete assessment cannot be made until additional information is provided on this point and on the determination of the Doppler weighting and hot spot analysis. Additionally, it is noted that some of the supporting information may not be entirely relevant as it is based upon a 15×15 design.

Conclusions

16.138 The submission made on the transient analysis of non-LOCA faults, as far as the Inspectorate has assessed it to date, is generally acceptable, though a number of detailed reservations have been made above. The following points are of most significance.

(a) Multiple steam generator tube failures could cause problems for the containment integrity and, in some faults where the containment is bypassed, a significant increase in radiological hazard. This problem will need to be dealt with in a more comprehensive manner than it has been so far in the PCSR.

(b) Further information should be provided, and has been promised, in support of the ATWT case to demonstrate a satisfactory outcome for the full range of such faults.

(c) Validation is required of all the codes which play a significant part in the analyses.

(d) Systematic sensitivity studies will be required for the most severe faults to determine the effects of plant modelling and data.

(e) More effort will need to be devoted to studying the effect of stuck open PORVs and SRVs, since these constitute LOCAs starting from non-standard initial conditions.

(f) The effect of operator error will need to be considered in the analysis.

(g) The claim that asymmetric faults are bounded by other faults requires justification.

Containment thermal hydraulics

Introduction

16.139 It is implicit in judgements made in the transient analysis, specifically in relation to those transients which subject the containment to thermal and pressure loads, that the containment remains intact when these loads remain within the design basis. It is necessary to check, therefore, that the safety case adequately demonstrates that accidents claimed to be within the design basis do not subject the containment to loads which might cause its failure. It is additionally necessary to ensure, based upon the fault analysis, that the necessary range of faults has been considered and that the codes used in the analysis do correctly predict the loads on the containment and the behaviour of the containment when subjected to these loads.

16.140 In this section the thermal hydraulic analysis with which these loads are calculated is considered. The behaviour of the containment structure in response to the loads is discussed in Section 8.

Assessment

16.141 The first objective of the containment thermal hydraulics calculations in the PCSR is to show that the containment design pressure and temperature are not exceeded for a number of limiting design basis faults. The containment design pressure and temperature for the Sizewell B plant are 3.44 bar gauge (50 psig) and 160 °C (320 °F), respectively. The design basis leakage rate for the containment at this pressure is 0.1% of the enclosed volume per day. At pressures above 50 psig, the limiting design basis leakage may well be exceeded; in addition, the structural integrity of the containment may be at risk.

16.142 In addition to the calculations for the main containment structure, calculations are also presented to demonstrate the integrity of the internal structure housing the components of the nuclear steam supply system (NSSS) within the containment, and to establish the bounding pressure and temperature values in the LOCA calculations.

16.143 The thermal hydraulic pressure and temperature calculations presented in the PCSR have been assessed from the point of view of the physical processes described in the codes to identify the conservatisms in the assumed parameters and correlations, to ensure that the bounding fault conditions have been analysed, and therefore to establish the acceptability of the design pressure and temperature. The Inspectorate has a number of reservations about the modelling of various heat-transfer processes in the COCO code and about some of the assumptions made. Particularly significant is the use of the Uchida condensation heat-transfer correlation in the passive heat-sink model and the claim that this correlation is conservative for the containment calculations needs justification.

16.144 As a consequence of these and other concerns, further calculations will be required to justify the claim that the calculated peak pressure is lower than the containment design pressure for all the limiting design basis fault conditions and to determine the particular fault which would result in the highest peak

pressure. In addition, the containment temperature design limit is exceeded for two of the design basis faults and this will need further consideration.

16.145 Although it is assumed in the PCSR that steam generator tube rupture coincident with a main steam line break is beyond the design basis, the CEGB has in addition produced sensitivity studies intended to show that steam generator tube rupture would not cause the containment design pressure to be exceeded. However, in the Inspectorate's view these studies were not carried out for the correct transient. From other studies (ref. 57) it appears that, had the correct transient been used, the rupture of a single steam generator tube could cause the design pressure to be exceeded. In the event of more than one tube rupture the design pressure might be significantly exceeded. It is therefore considered that relevant sensitivity studies, using the correct limiting design basis transients, should be carried out for main steam line break with coincident steam generator tube ruptures to assess the peak containment pressure. Similar studies should also be carried out for LOCA coincident with one or more steam generator tube ruptures. In addition, analyses are required for the steam line break fault with failure of more than one relevant MSIV to close.

16.146 It is not possible at this time to give an assessment of acceptability of the subcompartment calculations in the PCSR since sufficient details concerning the basis and validation of the TMD code have not yet been supplied by the CEGB. However, the calculations provided show that in some areas of the steam generator and pressuriser compartments the design pressures are exceeded. The claimed conservatisms in these calculations will need to be adequately demonstrated since, if the subcompartment design pressures were exceeded, extensive structural damage involving failure of pipework, component supports, instrumentation, etc., could possibly lead to a degraded core.

16.147 Finally, details should be provided of the calculation of jet impact loads and thermal loads which could damage the subcompartment structures, as well as pipe restraints and instruments located in the path of the jets. Suitable modelling of jet effects will be required in order to assess the possibility of degraded core situations resulting from their impact loads.

Conclusions

16.148 In summary, it is considered that whilst the codes used in the thermal hydraulic calculations for the containment are generally acceptable, a number of further analyses will be required before it can be accepted that the containment design pressure and temperature are set at the appropriate level so that the containment will withstand the thermal hydraulic and other forces which could result from the relevant fault conditions. These analyses will be required prior to a decision on licensing. They should not raise any major difficulties in the Inspectorate's future assessment provided that satisfactory results are obtained from relevant sensitivity studies, particularly on main steam line break coincident with steam generator tube ruptures.

Fault sequence probabilities and consequences

16.149 The radiological consequences of the faults analysed in the PCSR have been calculated using methods and data which have generally been endorsed by the PWR Radiation Physics Group, consisting of relevant specialists from CEGB, NNC and UKAEA. From the preliminary assessment it is accepted that the models used are generally satisfactory although the Inspectorate still requires further information about certain detailed aspects, particularly concerning the dose models used.

16.150 The Inspectorate is more concerned about the mixture of 'best estimate' and 'conservative' assumptions that have been used in the consequence calculations in the PCSR. In general, conservative assumptions appear to have been adopted in the atmospheric dispersion and dose models. However, the assumed equilibrium fission product inventory in the primary circuit is a best estimate value derived from operating Westinghouse plants and corresponds to a notional failed fuel fraction of 0.005%, whereas the reactor could be operated with significantly higher coolant activity. Also the fission product 'spiking' model, which represents the increase in iodine and caesium activity that occurs when the reactor is tripped or the primary circuit depressurised, appears to give best estimate rather than conservative values. Again, the assumed primary to secondary leak rate in the steam generators is less than the average value measured on a number of Westinghouse reactors which had detectable activity in the secondary coolant. As the design progresses the Inspectorate will require sensitivity studies on these and certain other of the more important assumptions in order to be able to assess the conservatisms in the calculated doses and hence identify any fault sequences which do not appear to be satisfactory, so that they can be given closer attention. In addition, it would expect such calculations to be used by the CEGB, to determine operational parameters such as the maximum allowable primary coolant fission product activity level ('failed fuel fraction'). Some preliminary information has recently been provided on the sensitivity of the calculated consequences to certain major assumptions but the Inspectorate has not yet had the opportunity to assess it.

16.151 In the PCSR it is claimed for most of the design basis faults that there are large margins between the calculated dose at the site boundary and the Inspectorate's assessment reference level. However, there are some reservations about the analysis upon which these claims are based, in particular, those expressed in Section 7 of this report. In view of these

and the points made above the Inspectorate cannot as yet say whether or not the margins are sufficient.

16.152 Time has not allowed a detailed assessment of the extent to which releases from the higher frequency faults satisfy the NII's principles and the requirements of the CEGB's Design Safety Guidelines, but in general it is claimed in the PCSR that these releases are small. In any case the consequences of such releases, being mainly within the acceptable release levels for normal operation, are small.

16.153 The situation with regard to faults beyond the design basis is less satisfactory. As pointed out earlier, the fault tree studies carried out to date do not cover the whole spectrum of potential faults. The CEGB claims in the PCSR, however, that the faults chosen are those which place the most onerous demands on the various protective functions and goes on to conclude that the summated frequency of these faults, which is calculated to be below 10^{-5}/year, represents the contributions from all 'beyond design basis' faults. The Inspectorate does not, however, accept without supporting analysis that the faults which have not yet been the subject of fault tree analysis, and failure modes excluded from the analysis, will make a negligible contribution to the overall risk of the plant. Hence, it is concluded that the PCSR does not show how far the CEGB has gone towards satisfying its design target of 10^{-6}/annum for all faults giving a significant release.

16.154 Despite these comments, the Inspectorate considers that the event and fault tree analysis has made an important contribution to the safety case and has provided a useful demonstration of the techniques. It needs, however, to be improved and expanded. NII is also concerned that the numerical results obtained should not be used or quoted without careful qualification as to their limitations.

16.155 Finally, the Inspectorate expects the CEGB to extend its analysis of 'beyond design basis' faults further than those sequences considered in Chapter 15 of the PCSR, to explore the potential for any escalation in the predicted consequences of such remote fault sequences and to explore the comparative overall risk from this range of faults. To satisfy this requirement the CEGB is preparing an analysis of such 'degraded core' accidents in parallel with the DBA fault studies presented in the PCSR. This analysis has not been completed early enough to allow it to be included with the PCSR but the Inspectorate understands it will be supplied in mid-1982 so that it should be possible to publish a preliminary assessment before the public inquiry.

Conclusions

16.156 The Inspectorate's main concern about the radiological consequence calculations arises from the apparent lack of pessimism in a number of the assumptions made. Preliminary sensitivity studies have recently been carried out by the CEGB for some of the main assumptions and the Inspectorate understands that these are to be extended; so far it has not had the opportunity to assess their validity.

Conclusions from the safety analysis

16.157 The analysis produced for this part of a safety case is extensive and complex. The different parts of the analysis, the fault and event trees and the transient studies, have to be linked together and this involves iteration from one set of studies to the other to produce a consistent and satisfactory safety case. As plant deficiencies are indicated by the analysis there has to be further iteration with the designers. When this process is coupled with the large number of faults that are covered, the time taken to reach a position considered satisfactory to the Inspectorate is necessarily long.

16.158 This section is being written at an early stage of the iteration process; the Inspectorate's assessment is based mainly on an early draft of the PCSR. It is inevitable, therefore, that the Inspectorate should find numerous deficiencies. As the process proceeds and the CEGB responds to the comments, the plant may be modified (this has already happened, though in general too late to assess the consequences of the changes), additional studies may be done, or it may convince the Inspectorate that the criticisms were unfounded. Shortcomings have been found in the range of faults for which event and fault trees have been produced. Conclusions drawn about the summated risk of large releases from the plant have been criticised; the correlation between the fault analysis and the transients studied needs to be improved and more transient analyses are required. Computer codes used throughout the analysis need to be validated.

16.159 On the other hand, the Inspectorate welcomes the use of event and fault trees in the safety case and the commitment to do more work in this area. Generally, the transient analyses are extensive and thorough. In matters like the possible effect of clad ballooning on the course of LOCA transients, while NII is not yet satisfied, it is well aware that considerable expense and effort are being expended to address the problem.

16.160 The Inspectorate expects the CEGB to deal with the various points raised here in future submissions. Any deficiencies will need to be corrected. Representative studies covering the whole spectrum of faults will need to be produced prior to a decision on licensing. It may be that some of the concerns will require changes to the plant. Some of the points made in the effective barrier assessment are in this category.

Of particular concern are the possible problem of steam generator tube failure and the implications of consequential tube failures on containment integrity. Operator errors and potential systems interactions are two other areas which require closer study. Finally, the Inspectorate expects the CEGB to ensure that, as far as reasonably practicable, the design satisfies the target criteria of its design safety guidelines.

17 Decommissioning

Introduction

17.1 Each nuclear power station must be decommissioned at the end of its operational life and the CEGB's proposed strategy and general procedures for the decommissioning of Sizewell B are outlined in the PCSR. The very valid point is made that some hundreds of PWRs will have reached the decommissioning stage before this particular reactor, and the experience gained will be a major influence in determining the decommissioning procedure and methods that will be adopted. The proposals in Chapter 16 of the PCSR deal with the phasing of the operation over a number of years and indicate the general magnitude of the task as well as highlighting particular features.

17.2 The overall approach is reasonable and acceptable, but more information will be needed for full acceptance.

General procedure for decommissioning

17.3 In the PCSR the main sources of radioactivity present after final shut-down are identified and the anticipated specific and total activity of certain major components are specified.

17.4 The three-stage procedure outlined is in accordance with international consensus and some indication is given of the time-scales involved. In particular it is estimated that all irradiated fuel should be removed from the reactor and from the site within five years from shut-down, thereby significantly reducing any potential hazard to the public from the shut-down reactor.

17.5 Those types of accident which might cause hazard to the public in the later stages of decommissioning are noted and a commitment is made to perform suitable detailed safety analyses at the relevant time during the decommissioning procedure to minimise their chance of occurrence.

17.6 It is recognised that the control of doses to workers during the dismantling operations will be a major determinant both in the timing of the decommissioning and in its mode of operation.

Comment

17.7 The approach in the PCSR on decommissioning is generally acceptable. Clearly when one is dealing with a process which will be taking place some 50 or 100 years in the future it is not possible to provide exact details of what will be done and when, if only because the technology which will then be available cannot be properly conceived at this time. However, it is reasonable and acceptable to demonstrate in broad terms how the work will be performed, to indicate what are likely to be the main constraints and to show that the operation will be technically feasible. In this latter respect some of the statements in the PCSR need to be substantiated.

17.8 The main defect of the case put forward is that it does not examine what might be done now at the design stage to assist in the decommissioning of the plant in the future.

17.9 More information should be provided on the following:

(a) Those features adopted to assist in the actual dismantling of the plant, bearing in mind the difficulty of operating in a radioactive environment.

(b) Those active isotopes which will be dominant at various times following shut-down and which will thereby play a major role in determining the pace and mode of decommissioning to be adopted.

(c) The manner in which the effects of such isotopes can and will be minimised by action taken at the design stage, e.g. by specification of materials, replacement of some elements, etc.

(d) The action taken to identify the essential information required for decommissioning purposes and the consequent action at the design stage to ensure that such information can be made available at the end of the reactor life.

(e) The design features to be adopted to minimise to the extent practicable the production of waste, particularly those forms of waste which are likely to present the greatest difficulties in disposal.

(f) The features incorporated in the design to assist in decommissioning following an accident.

Conclusions

17.10 The Inspectorate considers that the case presented is acceptable as a general statement of decommissioning intent with some indication of the likely main constraints and the procedures to be adopted during the decommissioning process. However it is concluded that the information supplied needs to be considerably augmented in certain areas before the submission can be considered to be complete.

17.11 Nevertheless it is agreed that decommissioning is technically feasible and that once the fuel has been removed the residual installation should not potentially present a significant hazard to the public. For these reasons it is accepted that decommissioning is not a major safety issue in the licensing process.

18 Research and development

18.1 This section is based mainly upon Chapter 1 of the PCSR but takes into account information contained in a number of other chapters.

18.2 In general the CEGB's programmes are aimed at providing a balanced investigation into the more important aspects of the PWR from an 'informed buyer' viewpoint only. There is no requirement in the PCSR for basic R & D work except for cases identified in the NII's generic review and TMI – 2 (ref. 58) requirements. The main issues from the generic review are covered by the R & D programmes of the CEGB and the NNC, backed by the same basic UKAEA programme.

18.3 Part of the strength of the PWR safety case lies in the world-wide programmes of safety research devoted to the system. The UK has become involved in these programmes, for example via participation in the Halden Project and in the NRU fuel rod cluster experiments, and entry to further projects is being negotiated.

18.4 Validation of LOCA calculational codes is an area that relies heavily upon the USNRC LOFT facility. Not having built commercial PWRs, the UK has not so far participated in the LOFT project. Unfortunately, the future of this facility is in doubt after mid-1983. A US decision not to proceed would leave a significant gap in the availability of large experimental facilities. A proposal has recently been made to continue the project with increased funding being required from outside participants. The Inspectorate would expect the CEGB to become involved or to encourage UK participation in this project through the UKAEA unless an alternative can be offered.

18.5 In a number of areas, including RPV and steam generator tube integrity, the PCSR makes reference to R & D programmes, but as noted earlier, the CEGB has not provided in the PSCR sufficient details of their work content or objectives. In view of the seriousness of failure in these and other such components the focus of the various R & D programmes should be expanded and further information provided.

18.6 In the case of the RPV, substantial programmes of R & D will be needed to give effect to the LWRSG (ref. 25) recommendations. Further experimental programmes may be needed to meet the concerns expressed in Section 9 for validation of the R6 fracture methodology. Completion of the defect detection trials (DDT) and collaboration in the PISC – II programme will help to support the so far encouraging results of the initial DDT programme. The requirement to measure toughness rather than charpy energy in surveillance specimens may necessitate further research. Both research and development activity may be required in connection with the setting up of an independent validation centre for inspection.

18.7 The Inspectorate has identified the need for specific programmes to address the issue of crevice inter-granular attack in steam generators. Similarly, in support of the case for the reactor coolant loops and internal structures there is a need for research in developing vibration signature monitoring and acoustic emission techniques to provide information on a continuous at-power basis on the integrity of critical components.

18.8 The range of NRC unresolved safety issues which require R & D inputs does not appear to have been considered directly in the R & D programme. In particular, confirmation is necessary that sufficient understanding has already been acquired, or will be acquired at the appropriate time, in the areas of the unresolved safety issues so as to remove any doubts in relation to them concerning the basic design decisions for Sizewell B.

18.9 A systematic and comprehensive accumulation and analysis of fault and incident data from world experience of PWR operation is an essential ingredient in the safety assessment of the plant. The Inspectorate has developed and applied for its own use a methodology for utilising such data. It is concerned that there is little evidence that the CEGB has yet developed such procedures to an adequate level.

18.10 In summary, UK work on PWR safety has been limited in the past and is still far from comprehensive. It is a continuing process, and the Inspectorate would wish to see a greater part played by the CEGB, in particular to address the issues raised in this review. There is a general need for increased UK effort in this field and for greater international participation by the CEGB.

19 Conclusions

19.1 In considering the views expressed in the various sections of this report, and the conclusions reached, it should be borne in mind that the pre-licensing process involves a dialogue between the licence applicant and the Inspectorate which, in the normal course of events, would extend over some two or more years. This process was temporarily suspended at an early stage in the Inspectorate's assessment of the CEGB's pre-construction safety report and its supporting documentation so as to provide a review of the position for the public inquiry. Indeed, because of the timing of this report, and of the interactive process carried out between the Inspectorate and the CEGB up to the time it was written, the PCSR published in May 1982 is different in a number of details from that of the draft of December 1981, which is substantially the subject of this review. This is to be expected, and it reflects a process of continual development and improvement of the design and the safety case as a result of both internal appraisal and re-appraisal by the industry and the CEGB, and also discussion with the Inspectorate of the case presented and the safety issues.

19.2 The safety case set out in the PCSR describes a design which is based on the Westinghouse SNUPPS plant and has been written using information from the standard safety analysis report for that system in the United States as its basis. However, the treatment is in parts uneven, for example, in some places the text is related to American requirements, or even to the SNUPPS design, rather than to the UK PWR. More importantly, there are shortcomings in the manner in which the safety case—the argument to show that the design intent meets the safety criteria and requirements—has been presented. The Inspectorate expects the CEGB, since as the operator it will be responsible for the safety of the plant, to justify the safety of its design. As a part of this, the CEGB should satisfy the intent of its own criteria. It is all the more important that a clear demonstration of this is given for a system which has not previously been licensed for commercial operation in this country. Whilst many of the reservations made in the generic review have been considered in the PCSR there are a number, of importance in relation to safety case requirements as well as design features, which have not yet been dealt with. The Inspectorate expects to see an improvement in this area in subsequent issues of or amendments to the PCSR.

19.3 The conclusions of this review are set out in the various sections of the report as appropriate. The position with regard to the more important safety aspects is summarised here for convenience (the numbers refer to paragraphs in the text):

(1) The basic intent with regard to design criteria for components, systems and structures is generally acceptable though a number of issues remain to be resolved, notably in relation to the need for the CEGB to do further work to demonstrate a satisfactory design basis in the case of earthquake loadings (4.2 – 4.9, 4.12 – 4.14).

(2) Although the human factors issue is not adequately considered in the PCSR, the CEGB has given a commitment to apply ergonomic principles to the design and operation of the station. Provided it shows evidence of utilising sufficient expertise and resources this should lead to an acceptable position (4.24).

(3) The CEGB's broad approach to quality assurance is acceptable. However, written programmes and procedures for the main safety items have not yet been made available and are required as a matter of urgency especially in relation to the early order items (4.29).

(4) The case made for protection against internal and external hazards is not yet satisfactory and needs to be cleared before a decision is made on licensing. In particular further information is required in relation to fire (4.41), aircraft crash (5.20), gas cloud explosions (5.21) and earthquakes (4.11, 5.23).

(5) The Sizewell site was accepted for the existing station as one which fell within the policy and characteristics for more remote sites, and it remains within that class of sites which would be acceptable for any reactor system licensed for commercial operation in the UK (5.11).

(6) For the most part the Inspectorate is satisfied with the information on the nuclear design and see no reason why its concerns, which require additional information or further justification, cannot be met by the time a decision on licensing is required (6.15).

(7) In the case of fuel behaviour in general, most of the main fuel issues raised in the generic review have been taken into account. However, reservations remain about the adequacy of the case set out in the PCSR to demonstrate satisfactory fuel performance in the design basis accidents and further information will be required before licensing (7.39 *et seq.*).

(8) The safety case has not yet been presented on clad ballooning, and so a judgement cannot yet be made on this topic (7.42).

(9) Whilst there are a number of specific concerns and qualifications which will need to be cleared, the Inspectorate is generally satisfied that the proposals made in the PCSR for the containment and other civil works and structures provide an acceptable basis for licensing (8.12).

(10) Though much valuable progress has been made since the generic review, a satisfactory safety case to meet the Inspectorate's requirements has not yet been made for the reactor pressure vessel. A number of shortcomings in the case put forward have been identified which should be put right, and more information should be provided, before the CEGB's claim that failure of the RPV is 'incredible' can be accepted. Whilst these shortcomings inhibit acceptance of the safety case as presented in the PCSR, the Inspectorate believes, nevertheless, that there are no reservations that cannot be overcome and that an acceptable safety case can be made. It requires a satisfactory case to be provided before a decision is made on licensing (9.49 *et seq.*).

(11) The Inspectorate is not yet satisfied with the case made to support the claim of 'incredibility' of failure for a number of pressure circuit components (other than the pressure vessel), including the coolant pump bowl, pressuriser, steam generator shell and head, ECCS accumulators, primary circuit component supports, reactor internals and the main steam line 'no break' zone. There are also reservations about the case made for steam generator tube integrity. Apart from the latter, the concerns relate mainly to the supply of information rather than to the technology available and, if the appropriate information is provided, it should be possible to make a satisfactory case before a decision is made on licensing (10.57 – 10.59).

(12) The general design basis for the protection system is not yet satisfactorily presented in the PCSR. Before licensing the Inspectorate requires an improvement in the safety case in the following areas: classification of protection systems, application of the single failure criterion, hazard design levels, segregation against fires and technical specifications for main plant items. In addition, justification is required where protection provisions included in earlier plants appear to have been downgraded, in particular, the reduction in shut-down margin and the removal of the boron injection tank system (11.19, 11.38, 16.112).

(13) The integrated protection system is a new system, not previously licensed for nuclear protection duties. Whilst the Inspectorate has no objection in principle to the technology employed, it is not yet satisfied that the hardware and software have been shown to be acceptable and there are a number of specific concerns which need to be resolved (11.28).

(14) In the generic review it was concluded that the Inspectorate saw no fundamental reason why acceptable protection arrangements could not be provided for the PWR reactor system considered; this remains the view. It is clear that many improvements have been made to the protection system since the generic review. However the safety case as presented in the PCSR is not yet acceptable for licensing. The Inspectorate expects to see its main concerns resolved before a decision is made on licensing, by clarification of the safety case and design intentions and firm commitments made where appropriate, and can see no fundamental reason why this should not be achieved (11.84 *et seq.*).

(15) There are a number of concerns arising from the Inspectorate's assessment of the case for plant chemistry and corrosion due mainly to the need for more information to support the intentions set out in the PCSR. This information is needed to show that proper chemistry control is feasible and is to be applied, and to satisfy the Inspectorate with regard to the case for control of activated corrosion products in the primary circuit, before licensing (12.1 *et seq.*).

(16) The radioactive waste management facilities described in the PCSR are considered to be sufficiently flexible to give confidence that the likely arisings, resulting from the normal operation of the reactor, can be handled in a safe manner. Further information will however be required to satisfy the Inspectorate that the estimates of primary coolant activity levels are conservative and to enable a judgement to be made of the extent to which a proper balance has been achieved between doses to on-site workers and those to members of the public (13.15 *et seq.*).

(17) With regard to radiological protection, it is considered likely that the shielding and layout provisions will prove to be generally adequate. However, further information will be required concerning a number of detailed areas, particularly the CEGB's design strategy for keeping all exposures as low as reasonably practicable and the adequacy of the design provisions to cope with conservative secondary coolant activity levels, both during normal operation and under fault conditions (14.14 *et seq.*).

(18) The safety case for fuel storage and handling is in general terms acceptably stated in relation to the hazard. However, some issues arise because neither the strategy nor the engineering design information required to confirm an acceptable safety standard are adequately presented. The Inspectorate expects these issues to be resolved at the appropriate time (15.12).

(19) Overall it is considered that the fault schedule is incomplete and the Inspectorate expects the shortcomings to be rectified in later submissions (11.20, 16.12).

(20) The probability analysis, and the event and fault trees, put forward in support of the safety case are extensive and the Inspectorate has only assessed them in part. However, it is noted that the selection of faults analysed is not yet complete in that it does not contain representatives from some potentially significant classes of fault and it excludes protection initiation systems and many supporting services, operator errors, and consequential passive failures such as breach of steam generator tubes. Furthermore, it is necessary for the analysis in the PCSR to show that individual fault sequences meet the CEGB's design safety guidelines (16.58 *et seq.*).

(21) There is insufficient information available and there has been insufficient time so far on which to make firm judgements in relation to the NII's effective barrier principles, though it is clear that some of the CEGB's proposed design changes will help to remove shortcomings shown up by that assessment. However, other potential shortcomings remain, for example in relation to sequences involving many operator actions and to the overall approach to locating potential systems interactions. Further information needs to be provided and further assessment carried out, so that those aspects having significant implications for the plant design can be cleared before a decision is made on licensing (16.61, 16.62).

(22) Subject to any further points arising from the Inspectorate's fault analysis assessment and to the reservations about fuel behaviour and limits, the range of LOCA faults covered in the PCSR and the safety case for them is judged to be generally acceptable (16.99).

(23) The code validation package is available only in outline as yet and it is not possible to form an opinion on its acceptability. The Inspectorate has no evidence which would negate the claim for overall conservatism in the calculations. However, code validation is of particular importance to the substantiation of the LOCA safety case (16.101).

(24) The submission made on the transient analysis of non-LOCA faults, as far as the Inspectorate has assessed it to date, is generally acceptable though a number of detailed reservations on the case put forward remain. The more significant points include: protection against ATWT faults; steam generator tube failures; validation of the codes used; systematic sensitivity studies; further study of the effect of stuck open PORVs and SRVs; and the effect of operator error (16.138).

(25) The codes used in the thermal hydraulic calculations for the containment are generally acceptable. However, further analysis will be required before it can be accepted that the containment design pressure and temperature are set at the appropriate level so that the containment will withstand the thermal hydraulic and other forces which can result from relevant fault conditions (16.148).

(26) With regard to decommissioning, whilst some improvement will be sought in the case put forward, there are no issues which are sufficiently important at this stage to influence licensing (17.10, 17.11).

(27) R & D work in the UK on PWR safety is a continuing process, and the Inspectorate would wish to see a greater part played by the CEGB, in particular to address the issues raised in this review. There is a general need for increased UK effort in this field and for greater international participation by the CEGB (18.10).

19.4 During the course of the generic review and the Inspectorate's subsequent assessment of information provided in support of the Sizewell B safety case leading up to the PCSR, a number of important safety issues were identified. These are summarised in para 2.10. The Inspectorate's assessment of the PCSR to date suggests that, while there are still concerns outstanding, a substantial number are now judged to be satisfied, or should be capable of being satisfied, mainly by provision of further information and argument in support of the CEGB's case. The Inspectorate is satisfied with the progress being made with these issues and they should not be a bar to licensing although, as has been indicated, a position acceptable to the Inspectorate will have to be reached before a decision on licensing is made.

19.5 However, there are some important areas remaining where the position is not yet satisfactory, namely:

(i) hazards presented by fire, aircraft crash and earthquakes, where an improved case needs to be made or design changes may be required;

(ii) fuel clad ballooning, where an acceptable strategy for developing a safety case has been presented but the case is awaited. If this does not prove to be acceptable then an alternative case, possibly based on changes to the fuel design or to the mode of operation of the reactor, will need to be made;

(iii) there are still reservations about the case made for steam generator tube integrity and the effect of multiple tube failures in fault conditions. Some development work or design changes may be necessary;

(iv) the reactor protection system, including the integrated protection system, where further justification of the proposed design is necessary and more time will be required to develop the case;

(v) safety analysis assessment, which will require more time and more information and where the Inspectorate has concerns which require attention, such as code validation and the adequacy of protection against the full range of ATWT faults.

In addition, the case for severe accidents is to be made as a separate submission and has not yet been received.

19.6 In summary, the Inspectorate's view at this stage is that the safety case provides confirmation of the view expressed in the generic review. There is no fundamental reason why a PWR should not be licensed for commercial electricity generation at Sizewell B. However, further assessment work will be necessary before NII can be satisfied that the design described in the PCSR is acceptable for licensing although in a number of important areas, such as the case for integrity of the pressure vessel and the use of microprocessor technology for reactor protection, the Inspectorate is now satisfied in principle that a case can be made. It expects more work to be done by the CEGB also, to provide further information to demonstrate its case in the areas where a satisfactory case has not been made or where there are safety issues to be resolved. This may require further modifications to the design.

19.7 In the Inspectorate's view a satisfactory design is achievable and can be developed so as to meet the safety objectives and give assurance that there will be a small chance of significant changes to the design needing to be made for safety reasons once construction has started. Only when the Inspectorate is satisfied that this is the case will a licence be granted.

Her Majesty's Nuclear Installations Inspectorate (NII/R/37/82) June 1982.

20 References

1 Hansard, 18 December 1979.

2 HSE, A Report by the Health and Safety Executive to the Secretary of State for Energy on a review of the generic safety issues of pressurised water reactors, Health and Safety Executive 1979 (HMSO 1982).

3 National Nuclear Corporation Ltd, Sizewell B PWR reference design, PWR/R500, September 1981.

4 Central Electricity Generating Board, Sizewell B PWR pre-construction safety report (Draft), GDCD/SYB/XRO2, December 1981.

5 Central Electricity Generating Board, Sizewell B PWR pre-construction safety report, April 1982.

6 National Nuclear Corporation Ltd, Sizewell B nuclear power station reference design, April 1982.

7 N Rasmussen, Reactor safety study. An assessment of accident risk in US commercial nuclear power plants, WASH 1400, (1975).

8 United Kingdom Atomic Energy Authority, An assessment of the integrity of PWR pressure vessels—a report by a study group under the Chairmanship of Dr W Marshall, UKAEA Report, HMSO, 1976.

9 HM Nuclear Installations Inspectorate, The generic safety issues of pressurised water reactors: an account of the study carried out by the Nuclear Installations Inspectorate of the Health and Safety Executive, Health and Safety Executive, July 1977.

10 Hansard, 25 January 1978.

11 US Nuclear Regulatory Commission, Unresolved safety issues summary, NUREG – 0606.

12 HM Nuclear Installations Inspectorate, Safety assessment principles for nuclear power reactors, HSE, April 1979. (HMSO, July 1982).

13 Central Electricity Generating Board, Design safety criteria for CEGB nuclear power stations, HS/R167/81 (Revised), March 1982.

14 Central Electricity Generating Board, Pressurised water reactor design safety guidelines, DSG 2 (Issue A), April 1982.

15 American Nuclear Standards Institute, Nuclear safety criteria for the design of stationary pressurised water reactor plants, ANSI N18. 2 – 1973.

16 US Code of Federal Regulations, General design criteria for nuclear power plants, 10 CFR 50, Appendix A.

17 The accident at Three Mile Island, Report of the President's Commission, October 1979, Washington DC.

18 International Atomic Energy Agency, Safety guide on seismic analysis and testing of nuclear power plants, 50 – SG – S2, Vienna 1979.

19 HM Nuclear Installations Inspectorate, Ergonomics/human factors in the design and operation of pressurised water reactors, Operators in Nuclear Safety Working Group report NII-ONSWG(82) P.1, 1982.

20 HM Nuclear Installations Inspectorate, A guide to the quality assurance programme for nuclear power plants, NII/R/38/78, Issue 2, December 1978.

21 W S Gronow, Application of safety and siting policy to nuclear plants in the United Kingdom, paper SM – 117/21 from IAEA Conference on environmental contamination by radioactive materials, IAEA, Vienna, 1969.

22 Hansard, 5 December 1973.

23 George Wimpey and Co Ltd and Soil Mechanics Ltd, Investigation of Sizewell site, 1968 – 80.

24 National Nuclear Corporation Ltd, Resistance against liquefaction of the Sizewell site, PWR/R253, Issue C, November 1981.

25 UK Atomic Energy Authority, An assessment of the integrity of PWR pressure vessels, Second Report of a Study Group chaired by Dr Walter Marshall, CBE, FRS, March 1982.

26 LE, Steel, Status report on the surveillance of radiation damage of US reactor pressure vessels, Post-SMIRT Seminar No. 8, Paris, August 1981.

27 House of Commons, 1st Report from the Select Committee on Energy, Session 1980 – 81, Vol. III, App. 20 and Vol. II, pp. 455, 456.

28 National Nuclear Corporation Ltd, PWR materials property data base fracture mechanics parameters, PWR/R422, Issue C, November 1981.

29 S J Garwood, Crack propagation toughness of structural steels at temperatures above the brittle-ductile transition temperature, Report 3545/8/79. The Welding Institute, March 1979.

30 Plate inspection programme, Report from the Plate Inspection Steering Committee on the Ultrasonic Examination of Three Test Plates using the 'PISC' Procedure based on the ASME XI Code. OECD/NEA. Committee on the Safety of Nuclear Installations, November 1979.

31 US Nuclear Regulatory Commission, List of generic tasks in the NRC program, Task No A – 3, NUREG – 0510.

32 US Nuclear Regulatory Commission, Steam generator tube experience, NUREG – 0886.

33 US Nuclear Regulatory Commission, Overall steam generator program, Policy Issue statement by William J Dircks, SECY – 82 – 72 dated 18 February 1982.

34 US Nuclear Regulatory Commission, Coordinated program for steam generators, Policy Issue statement by William J Dircks, SECY – 82 – 72, dated 25 March 1982.

35 US Nuclear Regulatory Commission, In-service inspection of steam generator tubes, Regulatory Guide 1.83.

36 US Nuclear Regulatory Commission, Basis for plugging degraded pressurised water reactor steam generator tubes, Regulatory Guide 1.121.

37 US Nuclear Regulatory Commission, Evaluation of steam generator tube rupture events, NUREG – 0651.

38 C V Dodds, *et al.*, Eddy current inspection for steam generator tubing, Annual Progress Report for Period ending 31 December 1980. Contract No W – 7405 – Eng26. Prepared for USNRC by Oak Ridge National Laboratory, June 1981.

39 G Dau, *et al.*, Special report—Section 4—Steam generator tube integrity, Electric Power Research Institute, Report EPRI – NP – 2088 – SR, Charlotte, NC, December 1981.

40 EPRI Study, Assessment of industry valve problems, EPRI – NP – 241, November 1976.

41 US Nuclear Regulatory Commission, Summary and bibliography of operating valves in LWRs, August 1979.

42 National Nuclear Corporation Ltd, Separation/segregation design for Sizewell B, PWR/R398, Issue A, March 1982.

43 National Nuclear Corporation Ltd, An assessment of the Westinghouse IPS for the British PWR, PWR/R382, Issue A, 16 March 1982.

44 US Nuclear Regulatory Commission, NRC Report on the January 25, 1982 steam generator tube rupture at R E Ginna Nuclear Power Plant, NUREG – 0909, April 1982.

45 National Nuclear Corporation Ltd, Sizewell B nuclear power station reference design issue A, PWR/R330, April 1981.

46 National Nuclear Corporation Ltd, Review of primary circuit chemistry and its implications on occupational exposures, PWR/R524 Issue B, January 1982.

47 National Nuclear Corporation Ltd, Shielding source terms for the radwaste plant and secondary system demineraliser, PWR/R465 Issue A, August 1981.

48 US Nuclear Regulatory Commission, Pipe cracks in stagnant borated water systems at PWR plants, NRC IE Bulletin 79 – 17, 26 July, 1979.

49 Westinghouse Electric Corporation Nuclear Energy Systems, Reliability and safety evaluations of the Westinghouse Model F steam generator, WCAP 9922, part 2, rev. 1.

50 E L White and W E Berry, Effects of copper and nickel compounds on the corrosion of pressurised water reactor steam generator materials, Nuclear Technology 1981, *55*, pp. 135 – 50.

51 US Nuclear Regulatory Commission, Occupational radiation exposure at commercial nuclear power reactors: 1979 Annual Report, NUREG – 0713, Vol. 1, March 1981.

52 Recommendations of the International Commission on Radiological Protection, Oxford, Pergamon Press, ICRP Publication 26, Ann, ICRP 1, No. 23 (1977).

53 National Nuclear Corporation Ltd, The role of event trees and fault trees in the safety case, PWR/R520, Issue A (Preliminary).

54 National Nuclear Corporation Ltd, Event tree analysis total failure of component cooling water, PWR/R543, Issue B.

55 D L Barry and P R Bennet, Study of alternate decay heat removal concepts for light water reactors—current systems and proposed options, US Nuclear Regulatory Commission NUREG/CR1556, April 1981.

56 B C Lexal and H Wyckoff, Instrument and control bus power loss at Rancho Seco on March 20, 1978, Nuclear Safety Analysis Center, NSAC – 13 November 1980.

57 H Pearce, Calculations of containment conditions following a major LOCA or a steam line break, National Nuclear Corporation Ltd, PWR/R503, July 1981.

58 US Nuclear Regulatory Commission, Special Report to Congress, Identification of new unresolved safety issues relating to nuclear power plants, NUREG 0705, March 1981.

21 Abbreviations

AFS	—	Auxiliary feed system
AFW	—	Auxiliary feed water
AGR	—	Advanced gas-cooled reactor
ALARP	—	As low as reasonably practicable
ANSI	—	American National Standards Institute
ASME	—	American Society of Mechanical Engineers
ASTM	—	American Society for Testing Materials
ATWT	—	Anticipated transients without trip
BIT	—	Boron injection tank
BNFL	—	British Nuclear Fuels Ltd
CCP	—	Condensate clean-up plant
CCW(S)	—	Component cooling water (system)
CEGB	—	Central Electricity Generating Board
COCO	—	Westinghouse code for containment pressure analysis
CVCS	—	Chemical and volume control system
CRDM	—	Control rod drive mechanism
CSNI	—	Committee on the Safety of Nuclear Installations (OECD – NEA)
CSS	—	Containment spray system
DDT	—	Defect detection trials
DNB	—	Departure from nucleate boiling
DNBR	—	Departure from nucleate boiling ratio
EBS	—	Emergency boration system
ECCS	—	Emergency core cooling system
ECS	—	Emergency charging system
ECT	—	Eddy-current testing
ERL	—	Emergency reference level
ESWS	—	Essential service water system
FLECHT	—	Full length emergency heat transfer
FSAR	—	Final safety analysis report
GDCD (CEGB)	—	Generation Design and Construction Department
HAZ	—	Heat affected zone
HHSI	—	High head safety injection
HSD (CEGB)	—	Health and Safety Department
HVAC	—	Heating, ventilation and air conditioning
ICRP	—	International Commission on Radiological Protection
IGA	—	Inter-granular attack
IPS	—	Integrated protection system
LEFM	—	Linear elastic fracture mechanics
LHSI	—	Low head safety injection
LOCA	—	Loss-of-coolant accident
LOFT	—	Loss-of-fluid test
LOFTRAN	—	Computer code which is a library of transient routines
LOMI	—	Low oxidation state metal ion
LWRSG	—	Light Water Reactor Study Group
MFLB	—	Main feedwater line break
MSIV	—	Main steam isolation valve
MSLB	—	Main steam line break
MWd/te	—	Megawatt days/tonne
MWe	—	Megawatt electrical
NNC	—	National Nuclear Corporation
NSSS	—	Nuclear steam supply system
OBE	—	Operating basis earthquake
PCI	—	Pellet/clad interaction
PCSR	—	Pre-construction safety report
PISC	—	Plant Inspection Steering Committee
POD	—	PWR oxidative decontamination
PORV	—	Power operated relief valve
PSR	—	Preliminary safety report
QA	—	Quality assurance
RCCA	—	Rod cluster control assembly
RCP	—	Reactor coolant pump
RCPB	—	Reactor coolant pressure boundary
RHRS	—	Residual heat removal system
RIA	—	Reactivity initiated accident
RPV	—	Reactor pressure vessel
RUHS	—	Reserve ultimate heat site
RWST	—	Refuelling water storage tank
SFSP	—	Spent fuel storage pool
SG	—	Steam generator
SLB	—	Steam line break
SNUPPS	—	Standardised Nuclear Unit Power Plant
SRV	—	Safety relief valve
SSE	—	Safe shut-down earthquake
SSEB	—	South of Scotland Electricity Board
TMD	—	Transient mass distribution code for containment subcompartment analysis
TMI	—	Three Mile Island
TURTLE	—	Two-group, two-dimensional neutron diffusion code
USNRC	—	United States Nuclear Regulatory Commission
UKAEA	—	United Kingdom Atomic Energy Authority
WREFLOOD	—	Westinghouse code simulating reflood conditions
ZPA	—	Zero period accelaration

22 Glossary of terms

This glossary is intended to provide a helpful explanation for the reader without going into the detail necessary for technically accurate definitions.

Activity (radioactivity): the number of nuclear transformations occurring in a quantity of material in unit time. In this report radioactivity, radioactive material and activity are used in an interchangeable fashion.

Axial offset: a measure of the extent by which the axial neutron flux shape differs from a symmetrical distribution.

Buffering: a property of certain chemicals to maintain a relatively constant pH irrespective of the amount of acid or alkali added.

Crud: metal oxide and other corrosion products which become entrained in the primary coolant water, and which can become activated and deposited around the primary circuit.

Crud burst or spike: the spontaneous dissolution of solid crud, into the primary coolant, which occurs regularly at the start of refuelling hence causing a significant increase in coolant ^{58}Co activity.

Departure from nucleate boiling ratio (DNBR): term used to define the safety margin between operating conditions and the departure from nucleate boiling.

Dose equivalent: the quantity which expresses the biologically effective dose resulting from the exposure of humans to ionising radiation. Dose equivalent limits for workers and members of the public are recommended in ICRP 26.

Effective barrier: a set of engineered provisions which prevent a release of activity for a given fault sequence.

Magnetic filtration: a means of extracting ferromagnetic solid particles from the coolant water by trapping them in some magnetised matrix appropriately positioned in the coolant circuit.

Pellet/clad interaction (PCI): an effect which causes a local increase in stress in the fuel rod cladding due to mechanical interference with the expanding fuel pellet.

Protection system: all equipment or systems which act directly in the event of faults to prevent damage that could lead to the escape of radioactivity.

Segregation: a means whereby redundant or diverse systems are protected from hazards which might otherwise disable all of them. Segregation is normally achieved by physical barriers or by spatial separation.

Separation: one form of segregation which is achieved by maintaining redundant or diverse systems some distance apart, this distance being dependent upon the hazard being considered.

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

Train of equipment: one of several sets of identified redundant equipment capable of performing protective action.

Printed in England for Her Majesty's Stationery Office
by Hobbs the Printers of Southampton
(1431) D801956 C40 7/82 G380

A catalogue of HSE publications is available on sale from government bookshops. Indexed by subject headings, the catalogue is an invaluable source of reference for anyone who needs access to advice and information on the requirements of the 1974 Health and Safety at Work Act and related legislation and publications issued prior to the formation of the Health and Safety Executive.

HER MAJESTY'S STATIONERY OFFICE

Government bookshops

49 High Holborn, London WC1V 6HB
13a Castle Street, Edinburgh EH2 3AR
41 The Hayes, Cardiff CF1 1JW
Brazennose Street, Manchester M60 8AS
Southey House, Wine Street, Bristol BS1 2BQ
258 Broad Street, Birmingham B1 2HE
80 Chichester Street, Belfast BT1 4JY

Government publications are also available through booksellers

£5.50 net

ISBN 0 11 88 3652 8

HSE JULY 1982

HA3

SIZEWELL B A review by HM Nuclear Installations Inspectorate of the pre-construction safety report

HMSO