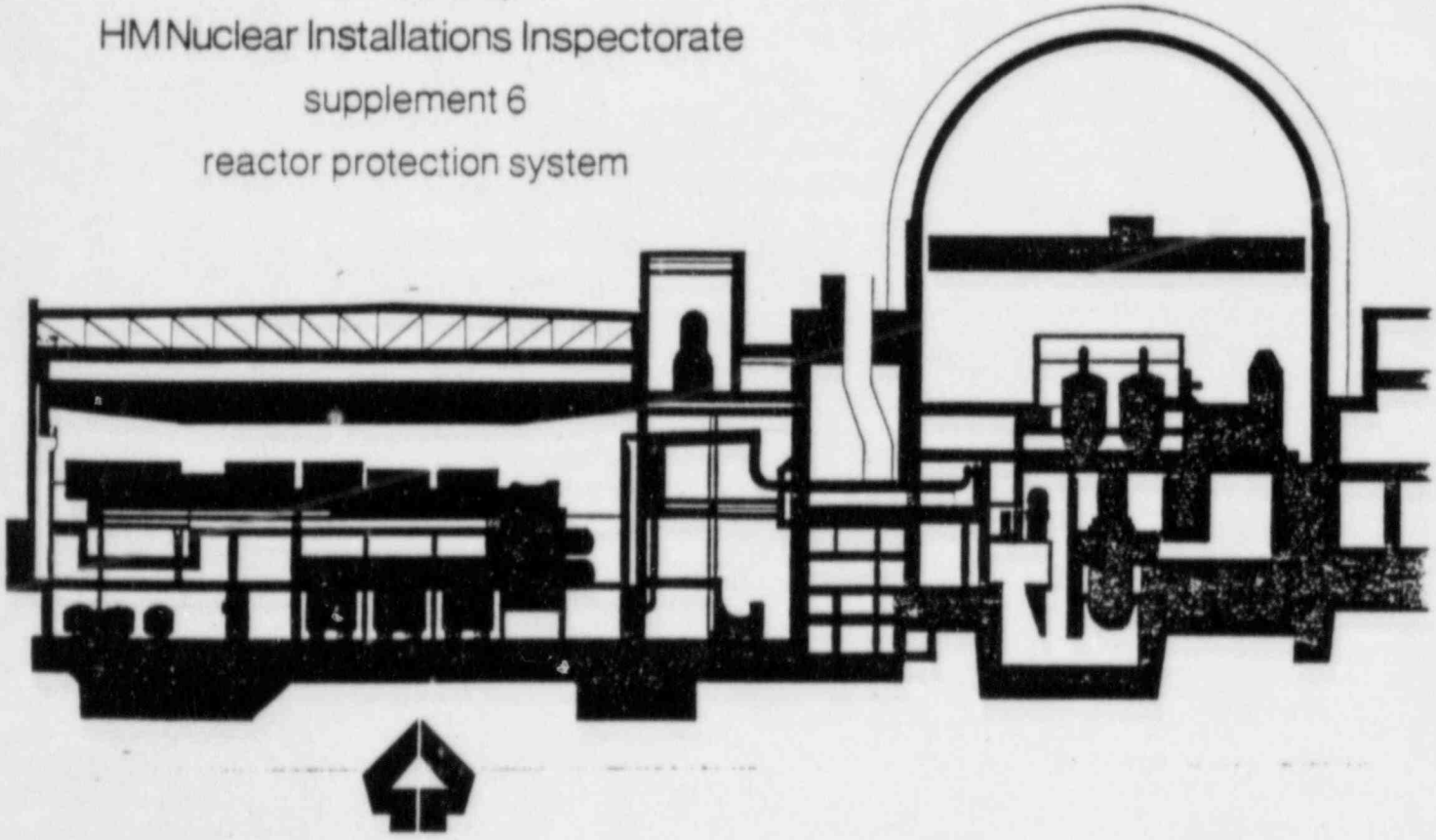
NII 01 (SUPP 6)

Sizewell B

a review by
HM Nuclear Installations Inspectorate
supplement 6
reactor protection system



Sizewell B

A review by HM Nuclear Installations Inspectorate
Supplement 6: Reactor protection system NII 01 (SUPP 6)

Health and Safety Executive
January 1983

CONTENTS

INTRODUCTION

1. The Inspectorate published the Review of the CEGB's pre-construction safety report (PCSR) for Sizewell B in July 1982 (ref 1). Section 11 of that Review sets out the Inspectorate's position in regard to its assessment of the protection system and safety related instrumentation as at March 1982.

2. Since March 1982 a dialogue has taken place between the Inspectorate and the CEGB culminating in the CEGB issuing a formal response to the Review as report PWR R686 November 1982* (ref 2) which addresses the Inspectorate's concerns on a point by point basis.

3. This supplement is an updating of the position taking into account information received from the CEGB up to 20 December 1982 and should be read in conjunction with the Review and R686. For convenience the main paragraph numbering except for the Introduction and Conclusions is identical to that of the Review.

4. Attention is again drawn to the potentially confusing differences in terminology as noted in paragraph 11.2 of the Review. In this supplement the Inspectorate has used terms as defined in its Safety Assessment Principles (NII/S/2).

5. At this stage of the licensing process it is important for the Inspectorate to understand and agree the basis and principles to be employed especially in the case of novel systems such as the integrated protection system (IPS). The detailed implementation of these principles can then be considered on a longer timescale as the project proceeds.

6. The Inspectorate has taken note of the introductory sections 1 to 4 of R686 setting out the current position and the further information promised. This has been taken into account in the comment on each section and in the conclusions.

---

* R686 and many other supporting reports are NNC documents which are endorsed by the CEGB and constitute part of their safety case.

GENERAL

11.1 to 11.5 No further comment required.

GENERAL PROTECTION SYSTEM STRATEGY

11.6 In regard to the comment made in the Review, although the position has become clearer in some areas, the Inspectorate cannot be satisfied with the general design basis for the protection system until a satisfactory schedule and comprehensive specification for this system have been provided.

11.7 The position on protection system diversity remains as stated in the Review. The fault schedule in the PCSR, section 15.1.9, sets out the general intent on diversity but the insufficiency of analysis referred to in the Review has yet to be remedied in order to show that the systems meet the intent. Further discussions will be necessary on the CEGB's response on steam generator (SG) level measurements and systems dealing with anticipated transients without trip (ATWT) situations. In the latter case the transient analysis promised for frequent faults has not been received at the time of writing.

11.8 It is agreed that all aspects of the protection system and services need not be fixed at this stage in the design process. The aspect with which the Inspectorate was concerned in the Review was that a PCSR should establish how the principles in the CEGB's design safety guidelines, particulary reliability and diversity, are to be met by the protection initiation and service systems provided. The principles document and the analysis of reactor trip system reliability referred to by the CEGB have not been received by the Inspectorate at the time of writing.

11.9 The response in R686 contains a discussion of the overtemperature and overpower T trip functions of a non integrated protection system. This supports the Inspectorate's view that in some cases the fault studies are not relevant to the integrated protection system. The improved protection claimed should be supported by inclusion in the fault schedule of relevant faults such as control rod banks out of line and supporting fault studies. The Inspectorate

will examine this question further when the promised specification for the protection system and the relevant studies are available.

11.10 Whilst the CEGB's assumption, that any issues arising out of the generic review have been included in the Review, is correct in most cases, it is not universally correct. However, the issues from the generic review which are still outstanding have been discussed with the CEGB on 5 November 1982 and 4 January 1983 and the Inspectorate is satisfied that work is in hand by the CEGB which could provide solutions to its concerns.

GENERAL DESIGN BASIS

11.11 The Inspectorate notes the CEGB's agreement to provide comprehensive schedules for the protection system but considers the time scale of September 1983 to be late for such basic information. Without such a schedule responses to several other questions, eg cable segregation, are not sufficiently definitive.

11.12 The Inspectorate notes the CEGB's response and the definition of class 1E equipment. It will examine IEEE 323 for acceptability. The proposals for non 1E equipment go some way towards meeting the Inspectorate's concern but are not completely acceptable since the Inspectorate remains of the view that it is essential to classify that portion having a significant safety role (as exemplified by the NII designation "safety related instrumentation") in order to ensure proper control at all stages.

11.13 The Inspectorate notes that a comprehensive analysis of single failures is intended and will wish this to be carried out against its definition of "the single failure criterion" to allow exceptions to be considered in an orderly manner.

11.14 The Inspectorate considers the response in R686 to be inadequate since it may be interpreted as referring to a 10^{-4}/year event. It considers that the relevant parts of the protection system and safety related instrumentation should be qualified to hazard levels corresponding to a 10^{-6}/year event and consistent with the CEGB

design risk target for the station. Further information on to the studies to be undertaken and the level at which qualification will be carried out have been requested and should be agreed with the Inspectorate before a decision on licensing can be made.

11.15 On 20 December 1982 the Inspectorate only had issue A (draft) of report PWR/R684 (ref 3). This indicates an intent to provide four way segregation against fire for the whole of the primary protection system which is a significant improvement over the PCSR proposals. The schedule of systems within the primary and secondary protection system mentioned in 11.11 above is required before the full implications of this intent can be understood. Further, the Inspectorate is still not clear as to the CEGB's intentions on the routeing and segregation to be provided for safety related instrumentation. The Inspectorate is not yet satisfied as to the acceptability of the means of providing segregation. This topic will be considered further in Supplement 8 to the Review.

11.16 Further consideration of technical specifications (operating rules) must await the provisional statement promised for March 1983.

11.17 The Inspectorate has not yet been satisfied on the concerns set out in the Review relating to sensors and further discussion will be required. In particular it may be noted that:

(a) Sensor failure modes: the response in R686 is noted but no further analysis of failure modes has been provided.

(b) Use of common tappings: the information provided in the CEGB's response deals with certain aspects only and does not give the Inspectorate the required assurance that sensors claimed to be independent will have separate tapping points.

(c) Testing of sensors: the Inspectorate has not been convinced that it is not reasonably practicable to provide arrangements for testing sensors remotely.

11.18 The Inspectorate is now satisfied that the CEGB has established a satisfactory policy on valves as indicated in its report R690 Issue B (ref 4).

11.19 Though further information is to be provided, until it is received the position remains substantially as it was in the Review. Before a decision on licensing can be made an improvement in the case is required in relation to 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) It is noted that operation with less than four loops is not currently intended and this satisfies the Inspectorate's concern.

(b) The Inspectorate will examine the information promised on the instrument air system when it becomes available. It will also require similar information on all other relevant instrument supplies.

(c) The Inspectorate is still not satisfied that the preliminary analysis of common mode failure of transmitters (sensors) presented in the PCSR section 15.11.13 produces worse situations than would be caused by stuck or out of tolerance sensors.

(d) The response in R686 removes the ambiguity of statements in the PCSR and is acceptable. It allows the reactor coolant pump (RCP) speed trip to be claimed for 1, 2 or 3 RCP failure faults.

(e) The Inspectorate will examine the analysis of spurious actuation of protection actions promised when it becomes available.

(f) The Inspectorate accepts that control room indications is a subject which can be dealt with as the design proceeds. The maintenance strategy should however be agreed sufficiently in advance of operation.

PROTECTION INITIATING SYSTEM

11.21 and 11.22 No further comment required.

11.23

(a) No further comment required.

(b) The Inspectorate has been informed by the CEGB of several improvements to the integrated protection system (IPS) which overcome many of its earlier concerns. The Inspectorate can now agree that the implementation of micro-processor technology in the Westinghouse IPS is acceptable. However the Inspectorate is still awaiting reliability information which has been promised. It also awaits the results of the CEGB and NNC's assessment of the software.

(c) It is noted that the RCP speed trip is incorporated in the secondary protection system (SPS). The implications of the two zone fire segregation in that system have yet to be examined by the Inspectorate.

11.24

(a) The Inspectorate's concern regarding the use of by-passes has been satisfied by the provision of four group segregation of this system as noted in 11.15 above.

(b) The response given in R686 as to limitations on the use of the by-pass system is acceptable.

(c) The Inspectorate will examine the promised study of operational by-passes when it becomes available. No preliminary statement has been received at the date of writing.

(d) The Inspectorate is not yet convinced about the adequacy of the boron injection signal derivation. It has not been provided with a description of the hardware involved, the effects of failures nor the preliminary reliability assessment.

11.25 The Inspectorate's concern over lack of definition of certain primary protection system actions is not adequately addressed by the CEGB's response since it does not give sufficient detail as to how or where they will be provided or what specification they will meet. It will expect to see these actions included in the schedule and specification mentioned under 11.6 above.

11.26 Although further details of the secondary protection system are given, most of this was already in the PCSR as a statement of intent. The Inspectorate's position remains that there is as yet no information available on the hardware intent for the SPS. It is noted that a bypass system will now be provided which removes the concern on failed sensors.

11.27 No change in position from that stated in the Review.

11.28 Whilst a number of the Inspectorate's concerns have been overcome, particularly in regard to the integrated protection system as a result of the improvements that have been made, further information is still to be provided and will need to be assessed.

CONTROL AND PROTECTION

11.29

(a) If the response in R686 means that all control faults will be protected by means of sensors which are diverse and

independent from those causing the fault, it is acceptable: this will need to be confirmed by the CEGB. The control signal selection described is acceptable in principle and will be examined further as the system is developed.

(b) The CEGB response in R686 largely concerns protection cabling and does not indicate a clear and firm intent for the segregation of control cabling. The statement that these (non 1E) cables will be allocated to groups 5 and 6 with only electrical segregation may prove to be unacceptable because of the possibility of fires producing multiple control faults.

11.30 The Inspectorate's concern that fires and power supply failures could cause multiple control faults beyond the protection system design basis has been acknowledged but until it has details of the methodology proposed it cannot comment further. The Inspectorate considers that generally it would be better to place emphasis at the design stage on preventing unwanted consequences by segregation rather than analysing the complex effects of fires and other events on the existing arrangement.

INTERLOCKS

11.31 and 11.32 As a statement of intent for the design of protection interlocks the Inspectorate finds this response acceptable. However at the present time it has little information on these interlocks and further consideration can only be given when the promised information becomes available.

REACTOR TRIP SYSTEM

11.33 No comment required.

11.34 and 11.35 The Inspectorate has examined the two reports on control rod reliability referred to by the CEGB (ref 5 and ref 6) but, because of limitations set by common mode failure, has not been

persuaded to change the statement made in the Review, ie that the control rod system reliability should not be claimed to be better than 10^{-5} failures per demand.

It is noted that the CEGB intends to provide analysis or additional protection such that faults more frequent than 10^{-2} per annum are satisfactorily covered by the case for anticipated transients without trip (ATWT) argument which is claimed as an acceptable alternative to a diverse tripping system. This analysis has not been received at the time of writing.

11.36

(a) See 11.34 and 11.35 above.

(b) The additional information on the logic of the boron initiation system has been noted but the Inspectorate currently has no details of the equipment involved nor evidence of adequate reliability particularly following single failures and this is required. Since the emergency boration system (EBS) is claimed as part of the protection provided for a number of ATWT faults the Inspectorate needs to be satisfied about its acceptability.

(c) The response that these systems will be scheduled as part of the protection and analysed for single failures is noted and is satisfactory as an intent. The Inspectorate will consider any exceptions claimed (see 11.13 above).

(d) The range of faults to be considered will now include failure of reactor coolant pumps and its consequent effect on the boron injection system. This is acceptable.

11.37

(a) The choice of the number of control rods (RCCAs) assumed to have failed to drop when deriving the system reliability is a complex one and the Inspectorate has insufficient information at present to reach a conclusion.

Table 1 appears to indicate that the EBS will now be claimed to augment the control rod system for primary protection as well as providing the alternative ATWT reactivity insertion. The Table also ignores the 10^{-5} limit which the Inspectorate would place on the control rod system. At present the Inspectorate is still of the view that two rod failures should be considered bearing in mind other possible mechanisms for reduction of shutdown reactivity margin such as covered in 11.37 (c) of the Review. (paragraph 38 of Supplement 2 to the Review (ref 8) also considers this issue).

(b) Subject to confirmatory evidence of the statements made by the CEGB, the margin of 50°C between the faulted condition and the temperature at which the control rod mechanism is qualified is acceptable.

(c) Whilst it is accepted that administrative procedures will make disconnection of RCCA's from their drive mechanism unlikely it is not in the Inspectorate's view so unlikely that it can be ignored. Further consideration of the consequences is therefore required.

11.38 Although the CEGB's argument in R686 is that a large margin will exist to departure from nucleate boiling (DNB), the Inspectorate is still of the opinion that the reactor should remain sub critical following any tripped fault. The CEGB's response indicates that this is not achieved for cooldown faults. However it is accepted that the faults considered in the PCSR under this heading have extreme pessimisms included and it would be acceptable if the requirement were met for any sequence of frequency greater than 10^{-7} per annum (see paragraph 38 of Supplement 2 to the Review).

11.39 Whilst the CEGB has made advances in the safety case for the reactor trip system, and further information has been promised, this is not yet sufficient to change the Inspectorate's general position from that stated in the Review.

PRESSURE PROTECTION

11.40 The response in R686 relates only to overpressure conditions when below full power temperature and the Inspectorate still considers that a more comprehensive analysis than is provided in the PCSR is required to justify that the protection provided against all overpressure conditions is to the same standard as that for reactor protection. However for the case of cold overpressurisation, the Inspectorate is able to accept figures 15.15/1 and 15.15/2 in the PCSR as an adequate indication of the envelope of allowable conditions and the analysis provided in R561 (ref 7) gives useful supporting information.

11.41

(a) Providing that the devices for testing the safety relief valves described are to be fitted the Inspectorate will be satisfied on this point.

(b) Subject to the promised confirmation, the response in R686 to the Inspectorate's concern about repressurisation of the reactor coolant system (RCS) by the seal injection flow would be acceptable.

(c) It is noted that the primary pressure relief system will withstand a single failure for all faults. Subject to the acceptability of the technical specifications covering these valves and the Inspectorate's acceptance of the boron injection system this would be acceptable.

(d) The Inspectorate accepts that the power operated relief valve (PORV) and block valve controls described will adequately reduce the frequency of small loss of coolant accidents (LOCAs) caused by PORV failures. They will also provide acceptable cold over-pressure protection to maintain the reactor coolant circuit within the envelope discussed in Section 11.40 above.

11.42 Some of the Inspectorate's concerns on pressure protection have now been adequately resolved. However a specification for the systems involved will need to be included in the protection system specification to be provided together with the analysis mentioned in 11.40 above.

REACTOR HEAT REMOVAL SYSTEMS

11.43 The Inspectorate is not yet satisfied that adequate diversity of heat removal is provided with the reactor at pressure since no justification has been given for the effectiveness of "bleed and feed". Further consideration will be required of mechanisms which could cause loss of heat removal via the steam generators and on the effectiveness of the bleed and feed procedure now claimed (see also paragraphs 19 and 20 of Supplement 2 to the Review (ref 8).

11.44

(a)(i) The Inspectorate is satisfied that the addition of a diverse interlock and an extra isolation valve make the probability of a LOCA via this route acceptably low.

(ii) It is considered that the reactor heat removal system (RHRS) can be designed to the required reliability but the Inspectorate will require the CEGB to confirm that the stresses induced by thermal transients on system initiation are properly taken into account in the system design in the manner indicated in R686.

(b) The Inspectorate is not yet satisfied that the arrangements proposed for interconnecting the spray and RHR systems are acceptable. The arrangement shown in figure 2 of R686 does not as it stands achieve the stated objective since with valve HVO66A open, both pumps will preferentially inject into the cold legs instead of the containment spray.

It is noted that it is proposed to delete the hydrazine spray additive system but to date the Inspectorate has not received an adequate justification that this modification will not result in larger radioactivity releases post accident.

(c) The Inspectorate accepts the intent for maintenance of the RHRS set out in R686 and will consider this question further when the details of intended maintenance become available.

11.45 The Inspectorate has noted the arguments presented for not providing redundancy of the refuelling water storage tank (RWST) and associated pipework systems. It now considers that the single tank provided would be acceptable if redundant vents and outlet lines were to be provided.

11.46 No further comment required.

11.47 With regard to the response in R686 to the Inspectorate's concerns on causes of frequent LOCAs:-

(a) It is accepted that the provision of automatically controlled block valves will reduce the frequency of small LOCAs due to PORV failure to an acceptable level.

(b) The information provided in R686 and the programme of future work described in R685 (ref 9) relating to steam generator (SG) tube integrity goes some way towards satisfying the Inspectorate's concern. The proposed sensitivity study concerning coincidental failure of the high head safety injection (HHSI) will be an important input to the Inspectorate's further examination of this issue

(c) The Inspectorate still has reservations concerning the apparent relatively high frequency of RCP seal failures other than those caused by loss of seal cooling and awaits

the demonstration based on data sources promised by the CEGB. Two emergency charging system (ECS) pumps are now provided which removes the Inspectorate's main concern about this system. However, further examination will be required of other single failures which would cause the system to fail as part of the analysis referred to in 11.13 above.

11.48 Whilst advances have been made by the CEGB in reducing the frequency of certain forms of small LOCAs, as stated in paragraph 11.47 above the Inspectorate is not yet completely satisfied that the frequency of small LOCAs caused by steam generator tube failures and RCP seal failures reported on operating plants has been shown to be sufficiently low to be consistent with the protection provided.

11.49 No comment required.

11.50 The Inspectorate is pleased to note that a study will be undertaken to establish the required feasibility of maintenance post LOCA.

11.51 The Inspectorate will consider this question of blockage of containment sump screens by debris further when the promised analysis becomes available.

11.52 Whilst progress has been made towards satisfying the Inspectorate's concerns it will be apparent from the foregoing that some issues still remain to be resolved before a decision on licensing can be taken.

AUXILIARY FEED WATER SYSTEM

11.53 No comment required.

11.54 The Inspectorate has noted the response to its concern on the reliability of the auxiliary feedwater system but still considers that individual system target reliabilities can and should be stated for

the classes of faults identified. Notwithstanding the reference to redundancy and accepting that an averaged unavailability will be assumed in the fault analysis, it remains to be satisfied that the reliability of the auxiliary feedwater system (AFWS) will be acceptable during the time a pump is out of service.

11.55 The Inspectorate agrees that the testing described for the auxiliary feed water system is acceptable in principle.

11.56 The position on seismically qualified feed water storage is now clearer and the capacity indicated is considered acceptable provided the qualification is to the appropriate seismic level so as to be consistent with the CEGB's design risk target.

CONTAINMENT SYSTEMS

11.57 No comment required.

11.58

(a) The Inspectorate has noted the fuller description of the secondary containment in R686 and in ref 10. From a preliminary examination this is acceptable to the Inspectorate provided the specification for the primary containment is not relaxed. The means for preventing the spread of radioactivity between the areas requiring access will need to be examined.

(b) The concern on the reliability of personnel airlocks is satisfied by the improvements proposed to the design and by the provision of the secondary containment system to process any leakage.

(c) The Inspectorate will need to give further consideration to the case justifying the provision of single rather than double sump isolation valves when the CEGB's proposals become firmer as the design develops, but is of the view that an adequate solution can be found.

(d) The Inspectorate reserves its position on this question of sizing of the containment purge system until the additional data promised becomes available.

(e) The Inspectorate maintains the view expressed in the Review that it would be prudent to qualify the containment systems for degraded core situations. This has not been adequately covered by the CEGB's response which relates only to establishing potential margins.

(f) It is noted that consideration is being given to isolating the containment sump pump lines on high containment activity signals. However, the Inspectorate has not yet been convinced that complete containment isolation should not be initiated on a high radiation level signal which would give a more direct indication of the need to close the containment.

(g) The Inspectorate's response is dependent on its consideration of the proposed analysis referred to in 11.51 above.

SERVICES

11.59 No comment required.

11.60 The response that the contribution of the service systems will be included in the protection system schedule to be provided is noted and is acceptable (but see 11.11 above).

11.61 The Inspectorate's concern related to all services which supply the protection system whilst the response in 11.20(b) is acceptable only in regard to the instrument air system.

Electrical System

11.62 The response, that those parts of the electrical system which are required for the operations of safeguards equipment, and which

therefore contribute to the overall ability to mitigate the consequences of faults will be included in the protection system schedule to be provided, is noted and is acceptable (but see 11.11 above).

11.63 No comment required.

11.64 The Inspectorate now understands that the part of the system feeding the primary protection system is to be segregated against fire into four trains. This is acceptable subject to definition of which systems are within the primary protection system. The Inspectorate's concern on operational and reliability limitations in the case of two train systems has not yet been resolved since no additional information has been provided.

11.65 No change in the position from that stated in the Review.

11.66

(a) A draft report covering electrical systems reliability was received on the 15 October 1982 but the final report is not yet available at the time of writing. This draft report, whilst clarifying many aspects, does not give an adequate specification for the reliability required of the electrical systems nor does it give the diversity requirements. The Inspectorate awaits the promised information on voltage and frequency limitations of plant items before further assessment can be done.

(b) As noted in 11.64, the primary protection system is segregated against fire into 4 trains. However, the Inspectorate is still uncertain as to how far this segregation applies to the electrical systems particularly since they also feed the secondary protection system which is two-way segregated. Issue B of Report PWR/R684 which is referred to in the CEGB response in R686 was not received by the Inspectorate until 21 December 1982 and has not yet been assessed.

(c) The Inspectorate is still not clear about the CEGB's intentions for dealing with situations where electrical plant items are unavailable and awaits the further information promised.

(d) The CEGB's response that control supplies for grid switching will be independent of the diesel generators and station services is noted and subject to the air reservoirs being sized for 24 hours relevant duty, the proposal is acceptable.

11.67 Whilst the Inspectorate considers the proposals for the electrical system will prove to be acceptable, only limited progress has been made towards resolving the concerns expressed in the Review.

Instrument Air System

11.68 and 11.69 The response in 11.20(b) of R686 promises a full assessment of the instrument air system by May 1983 and this is awaited. It is still considered that the redundancy and segregation of the instrument air system in its present form could prove to be unaccceptable due to its susceptibility to common mode failures.

Essential Cooling Systems

11.70 No comment required.

11.71 The Inspectorate welcomes the undertaking to provide a detailed stress analysis to justify the post LOCA performance of the component cooling water and essential service water systems.

11.72 The Inspectorate notes the additional information given on the reserve ultimate heat sink (RUHS) pumped subsystem. A more complete specification and clarification of which fault sequences it is effective against is required before the Inspectorate can make a decision on this arrangement.

11.73 The design change to remove the essential seawater system components from the auxiliary building indicated by the CEGB's response overcomes the concern expressed in the Review.

SAFETY-RELATED INSTRUMENTATION

11.74 No comment required.

11.75

(a) As stated under 11.12 above the Inspectorate is not satisfied with the proposal not specifically to identify safety related instrumentation.

(b) The CEGB's response to 11.12 of R686 indicates a general intent to provide a specification which would be satisfactory if coupled with adequate identification as under (a) above.

(c) The CEGB's response in 11.12 of R686 falls short of an intent to provide evidence (by qualification) that such instrumentation will meet its performance specification.

11.76 The Inspectorate accepts the CEGB's commitment to provide instrumentation to monitor accident conditions beyond the design basis and will review this instrumentation at a later stage when the CEGB review is available.

11.77 No comment required.

11.78 The Inspectorate notes that the need for further analysis of reactor control common mode failure is accepted and will examine the analysis promised when it becomes available.

11.79 No change in the position from that stated in the Review.

11.80 The control signal selection described under 11.29(a) of R686 is acceptable in principle and will be examined in more detail as information becomes available.

11.81 and 11.82 First stage specifications for the main (ref 11) and emergency (ref 12) control rooms were received by the Inspectorate in August 1982. The Inspectorate has examined the specification for the

main control room in some detail and found shortcomings which have been communicated to the CEGB as the first stage in agreeing the principles to be applied in the design of the control rooms.

11.83 The position is essentially as stated in the Review. Further information has been provided and more is promised by the CEGB. This will be examined when received.

CONCLUSIONS

1 As will be apparent from the preceding commentary, progress has been made on a substantial number of items. This includes changes in the design which improve the safety of the plant and further information to support the safety case such as set out in R686.

2 In the case of the integrated protection system, whilst many of the Inspectorate's concerns have been resolved by changes to the system, others await further work which is promised. In particular the software assessment will not be available until further into 1983.

3 In a number of other areas the position remains as set out in the Review, mainly because further information or agreement on important principles is still awaited. It is disappointing that much of the information the Inspectorate had expected to receive by now is not yet available to it. For example, the Inspectorate is still finding it particularly difficult not having a schedule and specification for the complete protection system; this is basic information which it considers should have been provided in the PCSR and which will not be available until September 1983.

4 At this stage of the licensing process, the Inspectorate would not expect all details of the protection to be available. However it does expect that all elements of the system should be identified and a specification provided

together with clear statements of the principles to be applied on matters such as segregation, protection against hazards, qualification of components etc. There should also be adequate analysis to show that the system described is capable of meeting these basic requirements.

5 The Inspectorate sees no reason to change the view stated in the Review that an acceptable protection system can be provided but it expects to see the concerns it has expressed resolved to its satisfaction before a decision on licensing can be made.

HM NII, February 1983

REFERENCES

1 HSE. Sizewell B: A review by HM Nuclear Installations Inspectorate of the Pre-construction Safety Report for Health and Safety Executive HA3, (HMSO July 1982), NII 01.

2 R J Burton. Response to NII review of the PCSR July 1982 protection and essential systems. NNC report PWR/R686 issue B. November 1982.

3 M H Goldemund. Response to NII review of the PCSR July 1982 - safety aspects of fire protection. NNC draft report PWR/R684 issue A. November 1982.

4 D P Luckhurst. Response to NII review of the PCSR July 1982 - Reactor pressure circuit component integrity. NNC Report PWR/R690 Issue B. December 1982.

5 G K Roberts. Report entitled Westinghouse control rod drive mechanism failure to trip data. April 1982. (4874B:1).

6 M A Langton. Assessment of the reliability of the primary shutdown system. NNC report PWR/R680 Issue A October 1982.

7 S C Bubb. The Westinghouse Cold Overpressure Mitigating System in SNUPPS plants. NNC report PWR/R561 Issue A May 1982.

8 HSE. Sizewell B. A review by HM Nuclear Installations Inspectorate - Supplement 2 - safety analysis (NII 01 (Supp 2)).

9 J R Clarke and D J Shepherd. Response to NII review of the PCSR July 1982 - Steam generator tube integrity. NNC report PWR/R685 Issue B November 1982.

10 CEGB. Paper giving background information on the Secondary Containment System sent to the Inspectorate on 23 September 1982.

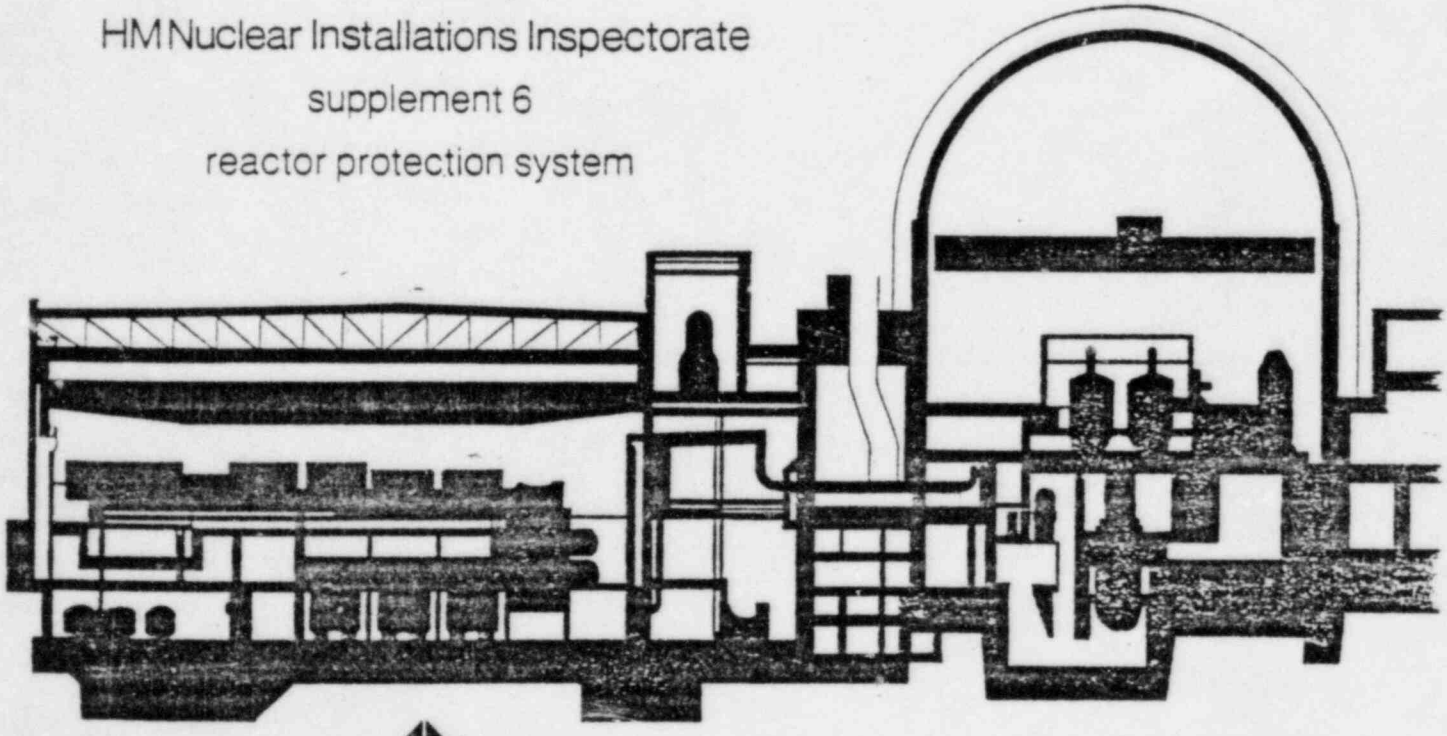
11 BBOO/RM/IRL/PS808946 First stage specification for the Sizewell B main control room and MCR equipment. NNC June 1982.

12 BBOO/RM/IRE/PS809263 First stage specificatior for the Sizewell B auxiliary shutdown room and ASR equipment. NNC June 1982.

NII 01 (SUPP 6)

Sizewell B

a review by
HM Nuclear Installations Inspectorate
supplement 6
reactor protection system



Sizewell B

A review by HM Nuclear Installations Inspectorate
Supplement 6: Reactor protection system NII 01 (SUPP 6)

Health and Safety Executive
January 1983

CONTENTS

INTRODUCTION

1. The Inspectorate published the Review of the CEGB's pre-construction safety report (PCSR) for Sizewell B in July 1982 (ref 1). Section 11 of that Review sets out the Inspectorate's position in regard to its assessment of the protection system and safety related instrumentation as at March 1982.

2. Since March 1982 a dialogue has taken place between the Inspectorate and the CEGB culminating in the CEGB issuing a formal response to the Review as report PWR R686 November 1982* (ref 2) which addresses the Inspectorate's concerns on a point by point basis.

3. This supplement is an updating of the position taking into account information received from the CEGB up to 20 December 1982 and should be read in conjunction with the Review and R686. For convenience the main paragraph numbering except for the Introduction and Conclusions is identical to that of the Review.

4. Attention is again drawn to the potentially confusing differences in terminology as noted in paragraph 11.2 of the Review. In this supplement the Inspectorate has used terms as defined in its Safety Assessment Principles (NII/S/2).

5. At this stage of the licensing process it is important for the Inspectorate to understand and agree the basis and principles to be employed especially in the case of novel systems such as the integrated protection system (IPS). The detailed implementation of these principles can then be considered on a longer timescale as the project proceeds.

6. The Inspectorate has taken note of the introductory sections 1 to 4 of R686 setting out the current position and the further information promised. This has been taken into account in the comment on each section and in the conclusions.

---

* R686 and many other supporting reports are NNC documents which are endorsed by the CEGB and constitute part of their safety case.

GENERAL

11.1 to 11.5 No further comment required.

GENERAL PROTECTION SYSTEM STRATEGY

11.6 In regard to the comment made in the Review, although the position has become clearer in some areas, the Inspectorate cannot be satisfied with the general design basis for the protection system until a satisfactory schedule and comprehensive specification for this system have been provided.

11.7 The position on protection system diversity remains as stated in the Review. The fault schedule in the PCSR, section 15.1.9, sets out the general intent on diversity but the insufficiency of analysis referred to in the Review has yet to be remedied in order to show that the systems meet the intent. Further discussions will be necessary on the CEGB's response on steam generator (SG) level measurements and systems dealing with anticipated transients without trip (ATWT) situations. In the latter case the transient analysis promised for frequent faults has not been received at the time of writing.

11.8 It is agreed that all aspects of the protection system and services need not be fixed at this stage in the design process. The aspect with which the Inspectorate was concerned in the Review was that a PCSR should establish how the principles in the CEGB's design safety guidelines, particulary reliability and diversity, are to be met by the protection initiation and service systems provided. The principles document and the analysis of reactor trip system reliability referred to by the CEGB have not been received by the Inspectorate at the time of writing.

11.9 The response in R686 contains a discussion of the overtemperature and overpower T trip functions of a non integrated protection system. This supports the Inspectorate's view that in some cases the fault studies are not relevant to the integrated protection system. The improved protection claimed should be supported by inclusion in the fault schedule of relevant faults such as control rod banks out of line and supporting fault studies. The Inspectorate

will examine this question further when the promised specification for the protection system and the relevant studies are available.

11.10 Whilst the CEGB's assumption, that any issues arising out of the generic review have been included in the Review, is correct in most cases, it is not universally correct. However, the issues from the generic review which are still outstanding have been discussed with the CEGB on 5 November 1982 and 4 January 1983 and the Inspectorate is satisfied that work is in hand by the CEGB which could provide solutions to its concerns.

GENERAL DESIGN BASIS

11.11 The Inspectorate notes the CEGB's agreement to provide comprehensive schedules for the protection system but considers the time scale of September 1983 to be late for such basic information. Without such a schedule responses to several other questions, eg cable segregation, are not sufficiently definitive.

11.12 The Inspectorate notes the CEGB's response and the definition of class 1E equipment. It will examine IEEE 323 for acceptability. The proposals for non 1E equipment go some way towards meeting the Inspectorate's concern but are not completely acceptable since the Inspectorate remains of the view that it is essential to classify that portion having a significant safety role (as exemplified by the NII designation "safety related instrumentation") in order to ensure proper control at all stages.

11.13 The Inspectorate notes that a comprenensive analysis of single failures is intended and will wish this to be carried out against its definition of "the single failure criterion" to allow exceptions to be considered in an orderly manner.

11.14 The Inspectorate considers the response in R686 to be inadequate since it may be interpreted as referring to a 10^{-4}/year event. It considers that the relevant parts of the protection system and safety related instrumentation should be qualified to hazard levels corresponding to a 10^{-6}/year event and consistent with the CEGB

design risk target for the station. Further information on to the studies to be undertaken and the level at which qualification will be carried out have been requested and should be agreed with the Inspectorate before a decision on licensing can be made.

11.15 On 20 December 1982 the Inspectorate only had issue A (draft) of report PWR/R684 (ref 3). This indicates an intent to provide four way segregation against fire for the whole of the primary protection system which is a significant improvement over the PCSR proposals. The schedule of systems within the primary and secondary protection system mentioned in 11.11 above is required before the full implications of this intent can be understood. Further, the Inspectorate is still not clear as to the CEGB's intentions on the routeing and segregation to be provided for safety related instrumentation. The Inspectorate is not yet satisfied as to the acceptability of the means of providing segregation. This topic will be considered further in Supplement 8 to the Review.

11.16 Further consideration of technical specifications (operating rules) must await the provisional statement promised for March 1983.

11.17 The Inspectorate has not yet been satisfied on the concerns set out in the Review relating to sensors and further discussion will be required. In particular it may be noted that:

(a) Sensor failure modes: the response in R686 is noted but no further analysis of failure modes has been provided.

(b) Use of common tappings: the information provided in the CEGB's response deals with certain aspects only and does not give the Inspectorate the required assurance that sensors claimed to be independent will have separate tapping points.

(c) Testing of sensors: the Inspectorate has not been convinced that it is not reasonably practicable to provide arrangements for testing sensors remotely.

11.18 The Inspectorate is now satisfied that the CEGB has established a satisfactory policy on valves as indicated in its report R690 Issue B (ref 4).

11.19 Though further information is to be provided, until it is received the position remains substantially as it was in the Review. Before a decision on licensing can be made an improvement in the case is required in relation to 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) It is noted that operation with less than four loops is not currently intended and this satisfies the Inspectorate's concern.

(b) The Inspectorate will examine the information promised on the instrument air system when it becomes available. It will also require similar information on all other relevant instrument supplies.

(c) The Inspectorate is still not satisfied that the preliminary analysis of common mode failure of transmitters (sensors) presented in the PCSR section 15.11.13 produces worse situations than would be caused by stuck or out of tolerance sensors.

(d) The response in R686 removes the ambiguity of statements in the PCSR and is acceptable. It allows the reactor coolant pump (RCP) speed trip to be claimed for 1, 2 or 3 RCP failure faults.

(e) The Inspectorate will examine the analysis of spurious actuation of protection actions promised when it becomes available.

(f) The Inspectorate accepts that control room indications is a subject which can be dealt with as the design proceeds. The maintenance strategy should however be agreed sufficiently in advance of operation.

PROTECTION INITIATING SYSTEM

11.21 and 11.22 No further comment required.

11.23

(a) No further comment required.

(b) The Inspectorate has been informed by the CEGB of several improvements to the integrated protection system (IPS) which overcome many of its earlier concerns. The Inspectorate can now agree that the implementation of micro-processor technology in the Westinghouse IPS is acceptable. However the Inspectorate is still awaiting reliability information which has been promised. It also awaits the results of the CEGB and NNC's assessment of the software.

(c) It is noted that the RCP speed trip is incorporated in the secondary protection system (SPS). The implications of the two zone fire segregation in that system have yet to be examined by the Inspectorate.

11.24

(a) The Inspectorate's concern regarding the use of by-passes has been satisfied by the provision of four group segregation of this system as noted in 11.15 above.

(b) The response given in R686 as to limitations on the use of the by-pass system is acceptable.

(c) The Inspectorate will examine the promised study of operational by-passes when it becomes available. No preliminary statement has been received at the date of writing.

(d) The Inspectorate is not yet convinced about the adequacy of the boron injection signal derivation. It has not been provided with a description of the hardware involved, the effects of failures nor the preliminary reliability assessment.

11.25 The Inspectorate's concern over lack of definition of certain primary protection system actions is not adequately addressed by the CEGB's response since it does not give sufficient detail as to how or where they will be provided or what specification they will meet. It will expect to see these actions included in the schedule and specification mentioned under 11.6 above.

11.26 Although further details of the secondary protection system are given, most of this was already in the PCSR as a statement of intent. The Inspectorate's position remains that there is as yet no information available on the hardware intent for the SPS. It is noted that a bypass system will now be provided which removes the concern on failed sensors.

11.27 No change in position from that stated in the Review.

11.28 Whilst a number of the Inspectorate's concerns have been overcome, particularly in regard to the integrated protection system as a result of the improvements that have been made, further information is still to be provided and will need to be assessed.

CONTROL AND PROTECTION

11.29

(a) If the response in R686 means that all control faults will be protected by means of sensors which are diverse and

independent from those causing the fault, it is acceptable: this will need to be confirmed by the CEGB. The control signal selection described is acceptable in principle and will be examined further as the system is developed.

(b) The CEGB response in R686 largely concerns protection cabling and does not indicate a clear and firm intent for the segregation of control cabling. The statement that these (non 1E) cables will be allocated to groups 5 and 6 with only electrical segregation may prove to be unacceptable because of the possibility of fires producing multiple control faults.

11.30 The Inspectorate's concern that fires and power supply failures could cause multiple control faults beyond the protection system design basis has been acknowledged but until it has details of the methodology proposed it cannot comment further. The Inspectorate considers that generally it would be better to place emphasis at the design stage on preventing unwanted consequences by segregation rather than analysing the complex effects of fires and other events on the existing arrangement.

INTERLOCKS

11.31 and 11.32 As a statement of intent for the design of protection interlocks the Inspectorate finds this response acceptable. However at the present time it has little information on these interlocks and further consideration can only be given when the promised information becomes available.

REACTOR TRIP SYSTEM

11.33 No comment required.

11.34 and 11.35 The Inspectorate has examined the two reports on control rod reliability referred to by the CEGB (ref 5 and ref 6) but, because of limitations set by common mode failure, has not been

persuaded to change the statement made in the Review, ie that the control rod system reliability should not be claimed to be better than 10^{-5} failures per demand.

It is noted that the CEGB intends to provide analysis or additional protection such that faults more frequent than 10^{-2} per annum are satisfactorily covered by the case for anticipated transients without trip (ATWT) argument which is claimed as an acceptable alternative to a diverse tripping system. This analysis has not been received at the time of writing.

11.36

a) See 11.34 and 11.35 above.

(b) The additional information on the logic of the boron initiation system has been noted but the Inspectorate currently has no details of the equipment involved nor evidence of adequate reliability particularly following single failures and this is required. Since the emergency boration system (EBS) is claimed as part of the protection provided for a number of ATWT faults the Inspectorate needs to be satisfied about its acceptability.

(c) The response that these systems will be scheduled as part of the protection and analysed for single failures is noted and is satisfactory as an intent. The Inspectorate will consider any exceptions claimed (see 11.13 above).

(d) The range of faults to be considered will now include failure of reactor coolant pumps and its consequent effect on the boron injection system. This is acceptable.

11.37

(a) The choice of the number of control rods (RCCAs) assumed to have failed to drop when deriving the system reliability is a complex one and the Inspectorate has insufficient information at present to reach a conclusion.

Table 1 appears to indicate that the EBS will now be claimed to augment the control rod system for primary protection as well as providing the alternative ATWT reactivity insertion. The Table also ignores the 10^{-5} limit which the Inspectorate would place on the control rod system. At present the Inspectorate is still of the view that two rod failures should be considered bearing in mind other possible mechanisms for reduction of shutdown reactivity margin such as covered in 11.37 (c) of the Review. (paragraph 38 of Supplement 2 to the Review (ref 8) also considers this issue).

(b) Subject to confirmatory evidence of the statements made by the CEGB, the margin of 50°C between the faulted condition and the temperature at which the control rod mechanism is qualified is acceptable.

(c) Whilst it is accepted that administrative procedures will make disconnection of RCCA's from their drive mechanism unlikely it is not in the Inspectorate's view so unlikely that it can be ignored. Further consideration of the consequences is therefore required.

11.38 Although the CEGB's argument in R686 is that a large margin will exist to departure from nucleate boiling (DNB), the Inspectorate is still of the opinion that the reactor should remain sub critical following any tripped fault. The CEGB's response indicates that this is not achieved for cooldown faults. However it is accepted that the faults considered in the PCSR under this heading have extreme pessimisms included and it would be acceptable if the requirement were met for any sequence of frequency greater than 10^{-7} per annum (see paragraph 38 of Supplement 2 to the Review).

11.39 Whilst the CEGB has made advances in the safety case for the reactor trip system, and further information has been promised, this is not yet sufficient to change the Inspectorate's general position from that stated in the Review.

PRESSURE PROTECTION

11.40 The response in R686 relates only to overpressure conditions when below full power temperature and the Inspectorate still considers that a more comprehensive analysis than is provided in the PCSR is required to justify that the protection provided against all overpressure conditions is to the same standard as that for reactor protection. However for the case of cold overpressurisation, the Inspectorate is able to accept figures 15.15/1 and 15.15/2 in the PCSR as an adequate indication of the envelope of allowable conditions and the analysis provided in R561 (ref 7) gives useful supporting information.

11.41

(a) Providing that the devices for testing the safety relief valves described are to be fitted the Inspectorate will be satisfied on this point.

(b) Subject to the promised confirmation, the response in R686 to the Inspectorate's concern about repressurisation of the reactor coolant system (RCS) by the seal injection flow would be acceptable.

(c) It is noted that the primary pressure relief system will withstand a single failure for all faults. Subject to the acceptability of the technical specifications covering these valves and the Inspectorate's acceptance of the boron injection system this would be acceptable.

(d) The Inspectorate accepts that the power operated relief valve (PORV) and block valve controls described will adequately reduce the frequency of small loss of coolant accidents (LOCAs) caused by PORV failures. They will also provide acceptable cold over-pressure protection to maintain the reactor coolant circuit within the envelope discussed in Section 11.40 above.

11.42 Some of the Inspectorate's concerns on pressure protection have now been adequately resolved. However a specification for the systems involved will need to be included in the protection system specification to be provided together with the analysis mentioned in 11.40 above.

REACTOR HEAT REMOVAL SYSTEMS

11.43 The Inspectorate is not yet satisfied that adequate diversity of heat removal is provided with the reactor at pressure since no justification has been given for the effectiveness of "bleed and feed". Further consideration will be required of mechanisms which could cause loss of heat removal via the steam generators and on the effectiveness of the bleed and feed procedure now claimed (see also paragraphs 19 and 20 of Supplement 2 to the Review (ref 8).

11.44

(a)(i) The Inspectorate is satisfied that the addition of a diverse interlock and an extra isolation valve make the probability of a LOCA via this route acceptably low.

(ii) It is considered that the reactor heat removal system (RHRS) can be designed to the required reliability but the Inspectorate will require the CEGB to confirm that the stresses induced by thermal transients on system initiation are properly taken into account in the system design in the manner indicated in R686.

(b) The Inspectorate is not yet satisfied that the arrangements proposed for interconnecting the spray and RHR systems are acceptable. The arrangement shown in figure 2 of R686 does not as it stands achieve the stated objective since with valve HV066A open, both pumps will preferentially inject into the cold legs instead of the containment spray.

It is noted that it is proposed to delete the hydrazine spray additive system but to date the Inspectorate has not received an adequate justification that this modification will not result in larger radioactivity releases post accident.

(c) The Inspectorate accepts the intent for maintenance of the RHRS set out in R686 and will consider this question further when the details of intended maintenance become available.

11.45 The Inspectorate has noted the arguments presented for not providing redundancy of the refuelling water storage tank (RWST) and associated pipework systems. It now considers that the single tank provided would be acceptable if redundant vents and outlet lines were to be provided.

11.46 No further comment required.

11.47 With regard to the response in R686 to the Inspectorate's concerns on causes of frequent LOCAs:-

(a) It is accepted that the provision of automatically controlled block valves will reduce the frequency of small LOCAs due to PORV failure to an acceptable level.

(b) The information provided in R686 and the programme of future work described in R685 (ref 9) relating to steam generator (SG) tube integrity goes some way towards satisfying the Inspectorate's concern. The proposed sensitivity study concerning coincidental failure of the high head safety injection (HHSI) will be an important input to the Inspectorate's further examination of this issue

(c) The Inspectorate still has reservations concerning the apparent relatively high frequency of RCP seal failures other than those caused by loss of seal cooling and awaits

the demonstration based on data sources promised by the CEGB. Two emergency charging system (ECS) pumps are now provided which removes the Inspectorate's main concern about this system. However, further examination will be required of other single failures which would cause the system to fail as part of the analysis referred to in 11.13 above.

11.48 Whilst advances have been made by the CEGB in reducing the frequency of certain forms of small LOCAs, as stated in paragraph 11.47 above the Inspectorate is not yet completely satisfied that the frequency of small LOCAs caused by steam generator tube failures and RCP seal failures reported on operating plants has been shown to be sufficiently low to be consistent with the protection provided.

11.49 No comment required.

11.50 The Inspectorate is pleased to note that a study will be undertaken to establish the required feasibility of maintenance post LOCA.

11.51 The Inspectorate will consider this question of blockage of containment sump screens by debris further when the promised analysis becomes available.

11.52 Whilst progress has been made towards satisfying the Inspectorate's concerns it will be apparent from the foregoing that some issues still remain to be resolved before a decision on licensing can be taken.

AUXILIARY FEED WATER SYSTEM

11.53 No comment required.

11.54 The Inspectorate has noted the response to its concern on the reliability of the auxiliary feedwater system but still considers that individual system target reliabilities can and should be stated for

the classes of faults identified. Notwithstanding the reference to redundancy and accepting that an averaged unavailability will be assumed in the fault analysis, it remains to be satisfied that the reliability of the auxiliary feedwater system (AFWS) will be acceptable during the time a pump is out of service.

11.55 The Inspectorate agrees that the testing described for the auxiliary feed water system is acceptable in principle.

11.56 The position on seismically qualified feed water storage is now clearer and the capacity indicated is considered acceptable provided the qualification is to the appropriate seismic level so as to be consistent with the CEGB's design risk target.

CONTAINMENT SYSTEMS

11.57 No comment required.

11.58

(a) The Inspectorate has noted the fuller description of the secondary containment in R686 and in ref 10. From a preliminary examination this is acceptable to the Inspectorate provided the specification for the primary containment is not relaxed. The means for preventing the spread of radioactivity between the areas requiring access will need to be examined.

(b) The concern on the reliability of personnel airlocks is satisfied by the improvements proposed to the design and by the provision of the secondary containment system to process any leakage.

(c) The Inspectorate will need to give further consideration to the case justifying the provision of single rather than double sump isolation valves when the CEGB's proposals become firmer as the design develops, but is of the view that an adequate solution can be found.

(d) The Inspectorate reserves its position on this question of sizing of the containment purge system until the additional data promised becomes available.

(e) The Inspectorate maintains the view expressed in the Review that it would be prudent to qualify the containment systems for degraded core situations. This has not been adequately covered by the CEGB's response which relates only to establishing potential margins.

(f) It is noted that consideration is being given to isolating the containment sump pump lines on high containment activity signals. However, the Inspectorate has not yet been convinced that complete containment isolation should not be initiated on a high radiation level signal which would give a more direct indication of the need to close the containment.

(g) The Inspectorate's response is dependent on its consideration of the proposed analysis referred to in 11.51 above.

SERVICES

11.59 No comment required.

11.60 The response that the contribution of the service systems will be included in the protection system schedule to be provided is noted and is acceptable (but see 11.11 above).

11.61 The Inspectorate's concern related to all services which supply the protection system whilst the response in 11.20(b) is acceptable only in regard to the instrument air system.

Electrical System

11.62 The response, that those parts of the electrical system which are required for the operations of safeguards equipment, and which

therefore contribute to the overall ability to mitigate the consequences of faults will be included in the protection system schedule to be provided, is noted and is acceptable (but see 11.11 above).

11.63 No comment required.

11.64 The Inspectorate now understands that the part of the system feeding the primary protection system is to be segregated against fire into four trains. This is acceptable subject to definition of which systems are within the primary protection system. The Inspectorate's concern on operational and reliability limitations in the case of two train systems has not yet been resolved since no additional information has been provided.

11.65 No change in the position from that stated in the Review.

11.66

(a) A draft report covering electrical systems reliability was received on the 15 October 1982 but the final report is not yet available at the time of writing. This draft report, whilst clarifying many aspects, does not give an adequate specification for the reliability required of the electrical systems nor does it give the diversity requirements. The Inspectorate awaits the promised information on voltage and frequency limitations of plant items before further assessment can be done.

(b) As noted in 11.64, the primary protection system is segregated against fire into 4 trains. However, the Inspectorate is still uncertain as to how far this segregation applies to the electrical systems particularly since they also feed the secondary protection system which is two-way segregated. Issue B of Report PWR/R684 which is referred to in the CEGB response in R686 was not received by the Inspectorate until 21 December 1982 and has not yet been assessed.

(c) The Inspectorate is still not clear about the CEGB's intentions for dealing with situations where electrical plant items are unavailable and awaits the further information promised.

(d) The CEGB's response that control supplies for grid switching will be independent of the diesel generators and station services is noted and subject to the air reservoirs being sized for 24 hours relevant duty, the proposal is acceptable.

11.67 Whilst the Inspectorate considers the proposals for the electrical system will prove to be acceptable, only limited progress has been made towards resolving the concerns expressed in the Review.

Instrument Air System

11.68 and 11.69 The response in 11.20(b) of R686 promises a full assessment of the instrument air system by May 1983 and this is awaited. It is still considered that the redundancy and segregation of the instrument air system in its present form could prove to be unaccceptable due to its susceptibility to common mode failures.

Essential Cooling Systems

11.70 No comment required.

11.71 The Inspectorate welcomes the undertaking to provide a detailed stress analysis to justify the post LOCA performance of the component cooling water and essential service water systems.

11.72 The Inspectorate notes the additional information given on the reserve ultimate heat sink (RUHS) pumped subsystem. A more complete specification and clarification of which fault sequences it is effective against is required before the Inspectorate can make a decision on this arrangement.

11.73 The design change to remove the essential seawater system components from the auxiliary building indicated by the CEGB's response overcomes the concern expressed in the Review.

SAFETY-RELATED INSTRUMENTATION

11.74 No comment required.

11.75

(a) As stated under 11.12 above the Inspectorate is not satisfied with the proposal not specifically to identify safety related instrumentation.

(b) The CEGB's response to 11.12 of R686 indicates a general intent to provide a specification which would be satisfactory if coupled with adequate identification as under (a) above.

(c) The CEGB's response in 11.12 of R686 falls short of an intent to provide evidence (by qualification) that such instrumentation will meet its performance specification.

11.76 The Inspectorate accepts the CEGB's commitment to provide instrumentation to monitor accident conditions beyond the design basis and will review this instrumentation at a later stage when the CEGB review is available.

11.77 No comment required.

11.78 The Inspectorate notes that the need for further analysis of reactor control common mode failure is accepted and will examine the analysis promised when it becomes available.

11.79 No change in the position from that stated in the Review.

11.80 The control signal selection described under 11.29(a) of R686 is acceptable in principle and will be examined in more detail as information becomes available.

11.81 and 11.82 First stage specifications for the main (ref 11) and emergency (ref 12) control rooms were received by the Inspectorate in August 1982. The Inspectorate has examined the specification for the

main control room in some detail and found shortcomings which have been communicated to the CEGB as the first stage in agreeing the principles to be applied in the design of the control rooms.

11.83 The position is essentially as stated in the Review. Further information has been provided and more is promised by the CEGB. This will be examined when received.

CONCLUSIONS

1 As will be apparent from the preceding commentary, progress has been made on a substantial number of items. This includes changes in the design which improve the safety of the plant and further information to support the safety case such as set out in R686.

2 In the case of the integrated protection system, whilst many of the Inspectorate's concerns have been resolved by changes to the system, others await further work which is promised. In particular the software assessment will not be available until further into 1983.

3 In a number of other areas the position remains as set out in the Review, mainly because further information or agreement on important principles is still awaited. It is disappointing that much of the information the Inspectorate had expected to receive by now is not yet available to it. For example, the Inspectorate is still finding it particularly difficult not having a schedule and specification for the complete protection system; this is basic information which it considers should have been provided in the PCSR and which will not be available until September 1983.

4 At this stage of the licensing process, the Inspectorate would not expect all details of the protection to be available. However it does expect that all elements of the system should be identified and a specification provided

together with clear statements of the principles to be applied on matters such as segregation, protection against hazards, qualification of components etc. There should also be adequate analysis to show that the system described is capable of meeting these basic requirements.

5 The Inspectorate sees no reason to change the view stated in the Review that an acceptable protection system can be provided but it expects to see the concerns it has expressed resolved to its satisfaction before a decision on licensing can be made.

HM NII, February 1983

REFERENCES

1 HSE. Sizewell B: A review by HM Nuclear Installations Inspectorate of the Pre-construction Safety Report for Health and Safety Executive HA3, (HMSO July 1982), NII 01.

2 R J Burton. Response to NII review of the PCSR July 1982 protection and essential systems. NNC report PWR/R686 issue B. November 1982.

3 M H Goldemund. Response to NII review of the PCSR July 1982 - safety aspects of fire protection. NNC draft report PWR/R684 issue A. November 1982.

4 D P Luckhurst. Response to NII review of the PCSR July 1982 - Reactor pressure circuit component integrity. NNC Report PWR/R690 Issue B. December 1982.

5 G K Roberts. Report entitled Westinghouse control rod drive mechanism failure to trip data. April 1982. (4874B:1).

6 M A Langton. Assessment of the reliability of the primary shutdown system. NNC report PWR/R680 Issue A October 1982.

7 S C Bubb. The Westinghouse Cold Overpressure Mitigating System in SNUPPS plants. NNC report PWR/R561 Issue A May 1982.

8 HSE. Sizewell B. A review by HM Nuclear Installations Inspectorate - Supplement 2 - safety analysis (NII 01 (Supp 2)).

9 J R Clarke and D J Shepherd. Response to NII review of the PCSR July 1982 - Steam generator tube integrity. NNC report PWR/R685 Issue B November 1982.

10 CEGB. Paper giving background information on the Secondary Containment System sent to the Inspectorate on 23 September 1982.

11 BBOO/RM/IRL/PS808946 First stage specification for the Sizewell B main control room and MCR equipment. NNC June 1982.

12 BBOO/RM/IRE/PS809263 First stage specification for the Sizewell B auxiliary shutdown room and ASR equipment. NNC June 1982.