Office for Nuclear Regulation

An agency of HSE

ASSESSMENT REPORT

Civil Nuclear Reactors Programme

NNB GenCo: Hinkley Point C Pre-Construction Safety Report 2012 – Assessment Report for Work Stream Fault Studies

Assessment Report: ONR-CNRP-AR-13-053
Revision 0
Version 2
March 2014

COPYRIGHT

EXECUTIVE SUMMARY

This assessment report reviews that portion of the Hinkley Point C Pre-Construction Safety Report 2012 (HPC PCSR 2012) that falls within the scope of the fault studies – design basis – work stream. Most of this material lies in HPC PCSR 2012 Chapters 9 and 14. The licensee, NNB Generation Company Limited (NNB GenCo), submitted HPC PCSR 2012 to the Office for Nuclear Regulation (ONR) to provide the site-specific baseline safety justification to support the construction of a twin UK EPR™ power station at Hinkley Point C (HPC).

A final version of the Generic Design Assessment (GDA) pre-construction safety report (PCSR) issued in November 2012 formed the basis for issue by ONR on 13 December 2012 of a Design Acceptance Confirmation (DAC) for the UK EPR™ design. The GDA PCSR addressed only the key elements of the design of a single UK EPR™ unit (the generic features on 'the nuclear island') and excluded ancillary installations that a potential purchaser of the design could choose after taking the site location into account. Certain matters were also deemed to be outside the scope of the GDA PCSR.

In contrast, HPC PCSR 2012 addresses the whole Hinkley Point C licensed site comprising the proposed twin UK EPR™ units and all ancillary installations. Some matters that were outside the scope of GDA PCSR are also addressed in HPC PCSR 2012. As the generic features were addressed in the GDA process, my focus is on site-specific documentation that has not been formally assessed by ONR previously. The remaining, generic documentation has been copied into HPC PCSR 2012 from an earlier March 2011 GDA PCSR which was superseded by the November 2012 GDA PCSR report.

It is important to note that HPC PCSR 2012 alone is not sufficient to inform a future ONR decision on whether to permission start of construction at HPC. NNB GenCo intends to submit a major revision to HPC PCSR 2012 before seeking consent for nuclear island construction which will fully integrate the final GDA PCSR and will be supported by other documentation.

The licensee has reported that no new design basis analysis (DBA) work has been undertaken in support of HPC PCSR 2012. The basis of the DBA reported in HPC PCSR 2012 is that from the consolidated GDA PCSR 2011. These aspects of HPC PCSR 2012 were therefore considered by ONR as part of GDA and have not been reconsidered within this assessment. This assessment has instead considered whether the DBA analysis for the generic EPR considered at GDA is applicable to the HPC site, including the particular equipment provided for power generation and for the ultimate heat sink. NNB GenCo has provided claims and arguments within the head document of HPC PCSR 2012 that the design basis analysis provided is applicable. However at the current time, NNB GenCo has provided insufficient evidence to support these arguments in the system description documentation. In particular, the description of the support systems provides details of the configuration of these systems and the measures taken to ensure suitable resilience. However, there is not sufficient information at present on the safety functions of the systems, their failure modes and the effects of loss of system availability. This information is needed to justify the level of safety classification given to the system and the measures required to ensure adequate reliability. A number of regulatory issues have been identified and shared with NNB GenCo to help in the development of a suitable safety case.

The information on the turbine and steam dump systems is presented as part of the site-specific case and is currently at a preliminary design level and will need significantly more information when the design becomes more mature.

In my opinion, HPC PCSR 2012 does not provide a sufficient safety justification for the HPC site outside of the scope of GDA. Rather, it provides a description of the proposed plant and details the outcome of site-specific design decisions. Evidence of a systematic design process will be needed.

The rational behind the selection of design options is often missing or insufficiently detailed to substantiate the decision. This is particularly true in the area of support systems and heat sink. However, I note that NNB GenCo is currently undertaking a major review of these systems, partly in the context of GDA assessment findings relating to their adequacy and partly in the context of findings relating to safety system classification.

To conclude, I am broadly satisfied with the licensee's claims and arguments that the GDA DBA can be applicable to the HPC site. However, insufficient evidence has been presented on the basis of the design decision-making. Ultimately, NNB GenCo will be required to provide ONR with the evidence that DBA claimed in the PCSR is still valid for the HPC site or to provide a HPC-specific DBA safety justification. NNB GenCo should ensure that this information is available within the next issue of the HPC PCSR and that a HPC site-specific fault schedule is available to support the next issue of the HPC safety report.

LIST OF ABBREVIATIONS

AF	Assessment Finding
AR	Assessment Report
BMS	(ONR) How2 Business Management System
BOP	Balance of Plant
CFI	Circulating Water Filtration System
CRF	Circulating Water System
CVCS	Coolant Volume Control System
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
DEL/DER	Safety Chilled Water System
DVL/DWL	Safeguard Building Ventilation System
DWN	Ventilation system for the Nuclear Auxiliary Building
DWK	Ventilation system for the Fuel Building
EBA	Containment Purge ventilation system
EVB	Containment sweep ventilation system
EVU	Containment Heat Removal System
EVR	Containment cooling and Ventilation System
GDA	Generic Design Assessment
HEPA	High Efficiency Particulate Air (filter)
HPB	Hinkley Point B
HPC	Hinkley Point C
HPC PCSR 2012	Hinkley Point C Pre-Construction Safety Report 2012
HVAC	Heating Ventilation and Air Conditioning
HSE	Health and Safety Executive
IEF	Initiating Event Frequency
ILW	Intermediate-Level Waste
ISFS	Interim Spent Fuel Store
LC	Licence Condition
LHSI	Low Head Safety Injection
LOCA	Loss Of Coolant Accidents
LOOP	Loss of Off-site Power
MSLB)	Main Steam-line Break
ONR	Office for Nuclear Regulation (an agency of HSE)

LIST OF ABBREVIATIONS

NNB GenCo	EDF Energy Nuclear New Build Generating Company Ltd
PCC	Plant Condition Categories
PCSR	Pre-Construction Safety Report
PSA	Probabilistic Safety Analysis
RBS	Reactor Boration System
RIS	Reactor Injection System
RRA	Decay Heat Removal System
RRC-A	Risk Reduction Category A
RRI	Component Cooling Water System
SAP	Safety Assessment Principle(s) (HSE)
SoDA	Statement of Design Acceptability
SFP	Spent Fuel Pool
SEC	Essential Service Water System
SEN	Auxiliary Raw Water Cooling System
SRU	Ultimate Cooling Water System
SSC	System, Structure and Component
TAG	Technical Assessment Guide(s) (ONR)

TABLE OF CONTENTS

Tables

1 INTRODUCTION

1.1 Background

1 This report presents the findings of the fault studies – design basis – assessment of EDF Energy Nuclear New Build Generating Company Ltd's (NNB GenCo) 2012 version of the pre-construction safety report (PCSR) for the Hinkley Point C (HPC) site, hereafter referred to as HPC PCSR 2012 (Ref. 1). NNB GenCo, the nuclear site licence holder for the HPC site, has plans to build a twin UK EPR™ unit power station at the HPC site. NNB GenCo has prepared HPC PCSR 2012, to provide the baseline safety justification to support entry to the construction phase of this project.

2 Assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) How2 Business Management System process 'Produce assessments' (Ref. 2). The ONR safety assessment principles (SAP), Ref. 3, together with supporting technical assessment guides (TAG), Ref. 14, have been used as the basis for this assessment.

3 This assessment largely builds upon the assessment work that was done during the Health and Safety Executive's (HSE) assessment of the UK EPR™ design as part of the Generic Design Assessment (GDA) process. The GDA Step 4 assessment was carried out on the November 2009 version of the PCSR (Ref. 4) and supporting documentation provided by EDF and AREVA during GDA Step 4. The 2011 version of the PCSR (Ref. 5) has been assessed in GDA but it is only the November 2009 version of the PCSR (Ref. 4) that has been formally subject to assessment. EDF and AREVA have also provided updates (Ref. 6) to the March 2011 PCSR (Ref. 5) for Chapter 14 on design basis faults, Chapter 15 on probabilistic safety analysis (PSA) and Chapter 16 on risk reduction and severe accident analysis to support the closure of the GDA issues raised as part of Step 4 of the GDA process.

4 The GDA issues raised as part of Step 4 have now been closed out and the GDA findings are being tracked to ensure that they are appropriately resolved. The UK EPR™ design was awarded a Design Acceptance Confirmation (DAC) by ONR (Ref. 7) and a Statement of Design Acceptability (SoDA) by the Environment Agency (Ref. 8) in December 2012. Note that this date was after the production of HPC PCSR 2012 (Ref. 1).

5 This assessment report (AR) has been written to support a summary assessment report that addresses whether HPC PCSR 2012 (Ref. 1) demonstrates suitable progress towards meeting ONR's requirement for an adequate pre-construction safety report.

1.2 Scope

6 The scope of this report covers the fault studies' work stream. Most of the licensee's material relating to fault studies lies in HPC PCSR 2012 Chapter 14 (design basis assessment). However, it is necessary also to assess chapters describing systems which may contribute to safety in order to confirm that the safety functions are clearly defined, that the system has been appropriately classified and that the design has taken appropriate account of the claims made on it in the fault studies analysis. A number of systems have undergone further design work since GDA and these aspects have been assessed. Chapters considered include Chapter 9 'Auxiliary Systems' and Chapter 10 'Steam and Power Conversion Systems'.

7 A final version of the GDA PCSR issued in November 2012 (Refs 5 and 6) formed the basis for issue by ONR on 13 December 2012 of a DAC for the UK EPR™ design. The

GDA PCSR addressed only the key elements of the design of a single UK EPR™ unit (the generic features on 'the nuclear island') and excluded ancillary installations that a potential purchaser of the design could choose after taking the site location into account. Certain matters were also deemed to be outside the scope of the GDA PCSR.

8 In contrast, HPC PCSR 2012 (Ref. 1) addresses the whole HPC licensed site comprising the proposed twin UK EPR™ units and all ancillary installations. Some matters that were outside the scope of GDA PCSR are addressed in HPC PCSR 2012 (Ref. 1). As the generic features were addressed in the GDA process, attention has been concentrated here on site-specific documentation that has not been formally assessed by ONR previously. The remaining, generic documentation has been copied into HPC PCSR 2012 from an earlier March 2011 GDA PCSR (Ref. 5) but this has now been superseded by the November 2012 GDA report. The generic documentation has only been revisited if recent developments have materially affected the case being made.

9 It is important to note that HPC PCSR 2012 (Ref. 1) alone is not sufficient to inform a future ONR decision on whether to permission construction of HPC and NNB GenCo intends to submit other supporting documentation. Note also that HPC PCSR 2012 (Ref. 1) will be superseded by a further site-specific revision intended to fully reflect the final GDA PCSR and other design changes from Flammanville 3 which is the reference design for HPC. It should also be noted the approach to safety function categorisation and safety system classification agreed during GDA (Ref. 23) is not fully reflected in HPC PCSR 2012 which largely uses the approach employed on Flammanville 3. The integration of the methodology and design changes agreed during GDA should be demonstrated in the next revision of the HPC PCSR.

10 The fault studies GDA Step 4 assessment focused on the design basis analysis of the UK EPR™ which has been sub-divided into a number of individual fault areas. These assessments cover faults where the integrity of the primary circuit is maintained (such as steamline break faults, loss of feed faults, loss of flow faults, and reactivity faults), and loss of coolant accidents (LOCA), where the integrity of the primary circuit is lost due to a break occurring somewhere on the primary circuit. Faults occurring during shutdown conditions or faults occurring away from the reactor in the spent fuel pool were also considered during GDA Step 4. A major area of assessment in GDA Step 4 was a review of the validation of the computer codes which play a significant part in these analyses.

11 This assessment will not cover the same areas of the previous Step 4 GDA assessment, but instead consider the changes from the GDA design or safety case: new information including new site-specific information; areas out of scope of GDA; and recent operational experience and standards development. Also to confirm that the GDA design is being implemented correctly, the outcome of work on assessment findings, additional fault analysis to support the reference design, operating rules, operating methods and instructions are examined.

1.3 Methodology

12 The methodology for the assessment follows the requirements of the ONR BMS step 1.4.1 'Produce assessments', in particular the 'Guidance on mechanics of assessment' (Ref. 2).

2 ASSESSMENT STRATEGY

13 The licensee's submission (Ref. 1) claims to provide the baseline safety justification for the construction and operation of twin UK EPR™ units at HPC and the safety justification to support entry to the construction phase of this project.

2.1 Standards and criteria

14 The relevant standards and criteria adopted within this assessment are principally the safety assessment principles (SAP) (Ref. 3), internal ONR technical assessment guides (TAG) (Ref. 14), relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and relevant TAGs are detailed within this section. National and international standards and guidance will be referenced where appropriate within the assessment report. Relevant good practice, where applicable, has also been cited within the body of the assessment.

2.2 Safety assessment principles

15 The primary source of standards (although not exclusively) for this assessment is the SAPs on general fault analysis, design basis accidents, and supporting guidance (FA.1–24). These cover identification of initiating faults, the potential consequences of fault sequences, and the analysis of fault sequences to determine requirements for safety systems, as well as specification of limits and conditions for safe operation. The design for reliability guidance (EDR.1–4) has been used to assess the documentation against the need to demonstrate the required tolerance to potential system failure commensurate with the system's intended functions. A more detailed list of the key SAPs employed during this assessment is provided within Table 1 of this report.

16 The requirement to reduce risk as low as reasonably practical is interpreted in this context in TAG NS-TAST-GD-005 and the relevant requirements for a satisfactory safety case are detailed in NS- NS-TAST-GD-051 (Ref. 14).

2.3 Integration with other assessment topics

17 This assessment has been focused primarily within the fault studies specialism. The assessment of the fuel and core design, which is a technical area that is closely related to fault studies, is not reported here. As a result, the justification of the fuel safety limits during accident conditions, including assessment of the critical heat flux correlations needed to demonstrate fuel integrity during many of the fault transients, are not discussed in this report.

18 The design basis thermal hydraulic analysis of the containment building during fault conditions, such as a large break loss of coolant accident or a main steam line break and assessment of the probabilistic safety analysis (PSA) are also reported separately.

19 Faults initiated by external hazards and the implications of internally-generated hazards (such as fire) are also treated as separate topics, as is the detailed mechanical design of safety systems.

3 LICENSEE'S SAFETY CASE

3.1 Summary

20 The intent here is to identify the key elements of the submissions in order to clarify the basis of the assessment. Nothing in this section is to be understood as a comment on the validity of the submission, nor should it be regarded as a comprehensive summary. Any detail quoted here should be verified in the original references before it is used for any other purpose.

3.1.1 Design basis analysis

21 The head document of HPC PCSR 2012 Section 14 summarises the contents of HPC PCSR 2012 Chapter 14 sub-chapters, which are the same as those of the March 2011 GDA PCSR, hereafter referred to as the consolidated GDA PCSR 2011 (Ref. 5). At this time, no HPC site-specific design basis analysis (DBA) is presented for HPC PCSR 2012 (Ref. 1). Instead, the licensee provides statements which it claims substantiates that the consolidated GDA PCSR 2011 DBA is representative of future HPC site-specific DBA, including its applicability to a twin-reactor site.

22 The plant characteristics of the UK EPR™ reference design used in the DBA are presented in consolidated GDA PCSR 2011 (Ref. 5). For the purposes of HPC PCSR 2012, the UK EPR™ design characteristics in Sub-chapter 14.1 of consolidated GDA PCSR 2011 are considered applicable by NNB GenCo to those that will be used in HPC site-specific DBA given that HPC design is closely based on the UK EPR™ reference design.

23 The licensee claims that Sub-chapter 14.0 of consolidated GDA PCSR 2011 (Ref. 5) is applicable to HPC based on the following arguments:

- The categories of DBA faults identified in consolidated GDA PCSR 2011 are applicable to HPC. However, the details of specific DBA faults may change or new faults could be added in future submissions as a result of: HPC PSA development; GDA issues; and GDA assessment findings resolution.
- HPC site-specific DBA will be performed using the same assessment methodology as described in Chapter 14.0 of consolidated GDA PCSR 2011 (Ref. 5). This means that it will be performed on a conservative basis, with the application of the single failure criterion, consideration of coincident loss of off-site power with the same assumptions on preventative maintenance. DBA faults involving the nuclear island spent fuel pool will be analysed using the methodology and assumptions stated in Sub-chapter 14.0, Section 2.10 of Ref. 1.
- The consequences of HPC site-specific DBA will be assessed against the same acceptance criteria as used for the GDA PCSR. However, in many cases this will be with slightly different limiting conditions of operation, reflecting the development of the plant operating rules. The results of equivalent HPC DBA faults, and hence margins to the acceptance criteria, may differ from those of equivalent DBA faults in the GDA PCSR. The extent of divergence will in certain cases depend on the exact fuel management strategy selected for HPC. While in the absence of HPC site-specific DBA the variation of these margins cannot yet be defined, the consequences of HPC site-specific DBA faults will remain within the acceptance criteria defined in the GDA PCSR.
- No new HPC site-specific DBA faults have so far been identified as a result of HPC being a twin-reactor site. The HPC fault list will be reviewed and any changes to the

fault schedule that are specific to HPC will be included in the DBA. The potential number of new design basis fault initiators as a result of HPC being a twin-reactor site is judged to be small given the relative independence of the two reactor units. Any new initiators will arise as a result of faults involving the shared services between the two reactors.

- HPC being a twin-reactor site will not impact on the DBA modelling assumptions or assessment methodologies for DBA faults involving an internal initiating event on a single unit as identified in consolidated GDA PCSR 2011 (Ref. 5). The potential consequences of DBA faults, whose initiating event affects both reactors on the HPC site, are addressed under Sub-chapter 14.6 of HPC PCSR 2012 (Ref. 1).
- There is confidence that the consolidated GDA PCSR 2011 (Ref. 5) analysis of design basis faults with conventional island initiators is applicable, and that the assumptions for the faults already identified will not be challenged by proposed or future HPC conventional island system designs. This is on the basis that:
  - Such faults, with conventional island initiators, are treated generically in consolidated GDA PCSR 2011 (Ref. 5) since the conventional island system designs are site-specific. In most cases, the conservative analysis assumptions with respect to plant availability mean that the acceptability of the fault consequences is independent of conventional island system design or responses.
  - Where conventional island systems / components perform a safety function claimed in PCSR 2011, the safety classifications of equivalent HPC-specific conventional island systems / components will be the same or higher.
  - The means by which the PCC faults are analysed are largely independent of the initiating event frequency (IEF). As long as the HPC-specific IEF of each PCC fault is consistent with the frequency band to which it is assigned in consolidated GDA PCSR 2011 (Ref. 5), then the analysis is applicable. If a fault is found to fall into a different PCC due to its site-specific frequency, it will be reassessed accordingly.

24 Faults affecting inventory in the interim spent fuel store (ISFS) and interim intermediate-level waste (ILW) store have not yet been assessed by NNB GenCo because of the early stage of design. A fault schedule for these buildings is not yet available.

25 The list of PCC faults covers faults affecting the core and the spent fuel pool. The GDA fault schedule also includes a representation of faults in the conventional island and balance of plant (BOP). However, they are included as losses of function only (black box) rather than specific faults and associated frequencies. The list has been identified systematically for initiating events within the nuclear island. For initiating events arising outside the nuclear island, it is based on loss of functional capability of services to the nuclear island.

3.1.2 Fault and protection schedule

26 No HPC site-specific fault and protection schedule has been produced for submission in HPC PCSR 2012. The current fault schedule included within consolidated GDA PCSR 2011 (Ref. 5) does not adequately represent faults specific to HPC or those which could come from the conventional island / BOP.

27 NNB GenCo claims that, for the purposes of HPC PCSR 2012 (Ref. 1), the content of the GDA fault and protection schedule, which covers all the considered PCC faults including

those specific to the nuclear island fuel storage pool, is applicable to HPC. The GDA fault schedule also includes representation of faults in the conventional island and BOP. This is on the basis of the following:

- The principles by which the PCC event list was developed will remain the same for HPC.
- The principles used for justification of the comprehensiveness of fault protection in consolidated GDA PCSR 2011 (Ref. 5) are applicable to HPC.
- The level of protection that will be provided by the HPC control and instrumentation (C&I) systems against the faults considered in consolidated GDA PCSR 2011 (Ref. 5) will be at least as comprehensive as that presented in the consolidated GDA PCSR 2011 fault and protection schedule.
- The as low as reasonably practicable (ALARP) discussions on the adequacy of the UK EPR™ design are applicable for HPC.

28 Therefore, the licensee claims that the fault and protection schedule presented for HPC PCSR 2012 (Ref. 1) is the same as that for consolidated GDA PCSR 2011 (Ref. 5).

29 During GDA, EDF / AREVA claimed the list of initiating faults would be complete when appropriate information became available (in particular detail design information and site-specific information). NNB GenCo proposes an approach to reorganising the structure of the safety report for internal faults: keeping the 'historical' list of design basis (PCC) faults; complemented by the fault and protection schedule. This ensures the completeness of the approach.

30 Generally, it has been indicated to ONR that NNB GenCo is not planning to modify the list of PCC events from GDA, but that additional design basis events with associated design basis analyses will be covered in the frame of the HPC fault and protection schedule.

31 NNB GenCo has now provided ONR with the specification of the HPC fault and protection schedule (Ref. 10). NNB GenCo stated that the HPC fault and protection schedule will form a key part of the next issue of the HPC PCSR. NNB GenCo has recognised that it is a fundamental requirement for the UK that we have a fault schedule that is applicable to HPC and that can be adequately demonstrated to be complete.

32 NNB GenCo has stated that the current GDA fault schedule format is an appropriate starting point, but NNB GenCo's preference for format would be to ultimately adopt something similar to that used for Hinkley Point B, as these have been recently updated and are considered to be more user-friendly. NNB GenCo states that the fault and protection schedule is a safety-report lifecycle deliverable and the format can therefore develop through the project. NNB GenCo has reported that the initial draft of the fault and protection schedule for the reactor building has provided a very good basis for informing the development of the format to be adopted. Examples from the initial draft of the fault and protection schedule for the reactor building has been shown to ONR during a level 4 regulatory interaction (Ref. 11) to inform ONR inspectors on progress on the HPC fault schedule development.

33 NNB GenCo has now made some strategic options / choices regarding the overall content of the HPC fault and protection schedule:

- Which claimed lines of protection to include – the Responsible Designer has proposed main line, backup line and severe accident line and this is considered by NNB GenCo to be a good approach.

- Inclusion of Systems, Structure and Components (SSC) classification (needs to recognise the classification workstream has to reach sufficient maturity). It is currently expected that this should converge for around 80% of SSCs by the end of 2013. This significantly reduces the potential risk of large amounts of work having to be updated as the classifications of SSCs are finalised.
- Hazards are not going to be integrated into the HPC fault and protection schedule in the short term (that is, not in 2013), due to the difference in format and large volume of underpinning work, but consideration will be given to doing so later, if it is judged appropriate. Ultimately the UK expectation is for full integration, if possible. The hazards fault schedule is in the process of being developed further and initial outputs from this work will need to be reviewed to inform the development of such an integration approach. It is expected that this specific aspect shall be reassessed by NNB GenCo in 2014.

3.1.3 Acceptance criteria

34 Safety criteria are defined in terms of radiological limits. In addition to safety criteria, it is convenient for practical purposes to introduce some decoupling criteria, which may be applied to the thermal hydraulic and neutronic calculations. This allows the thermal hydraulic and neutronic calculations to be decoupled and carried out separately from the radiological calculations.

35 A number of criteria are given, which require no fuel failures in normal operation and frequent faults and a limit of 10% fuel failures in less frequent faults. Specific structural integrity criteria are given for LOCA and rapid transients.

36 HPC PCSR 2012 (Ref. 1) reports that DBA is performed on a conservative basis so that the safety systems are designed with appropriate design margins. Where no UK EPR™ specific GDA DBA has been performed alternative statements are presented, the consequences of which are demonstrated to be bounding or to provide sufficient information for inferring results for any UK EPR™ specific analyses. Consequences have been calculated using a conservative methodology. A study referenced in HPC PCSR 2012 shows that the consequence analysis is representative for the HPC site (this study has not been considered as part of this assessment).

3.1.4 Equipment qualification

37 The purpose of qualification is to demonstrate that the equipment can fulfil its required function during normal operation and accident conditions. In practice, achievement of this objective is demonstrated by examining the consequences of a limited number of operating conditions:

- design basis fault conditions
- severe accident situations

38 Although they are excluded from the conventional list of design basis accidents, breaks equivalent to the double-ended guillotine rupture of a main reactor coolant pipe (2A-LOCA) and to the double-ended guillotine rupture of a steam line in the containment (2A-MSLB) are used for the qualification of equipment.

39 Depending on their safety role and the conditions for which the equipment is required to operate, qualification requirements are drawn up and incorporated into the equipment design via design functional requirements documentation and where necessary technical specifications.

40 The qualification procedure takes account of the effects of ageing and seismic loads.

41 Each safety function identified in the summary of functional requirement analyses is broken down into elementary functions for the equipment located in the buildings whose environmental conditions are affected by the accident.

42 The elementary functions are the abilities to change state when required. Typically, for a valve, the elementary functions are opening, closing, adjustment, maintaining open and maintaining closed. For a motorised item such as a pump or a fan, the elementary functions are start-up, shutdown, maintaining in operation and maintaining shutdown. The equipment that constitutes the ultimate barrier to fission-product release has a requirement related to leak tightness.

43 The equipment which has qualification requirements for operation in special conditions (for example high-energy water jets) is also identified. The length of time the equipment must fulfil its function in accidents is defined as: short-term, medium-term or long-term.

3.1.5 Adequacy of ultimate heat sink

44 Operation experience on failures of the ultimate heat sink was not addressed for GDA on the basis that this aspect of the design was site-specific. HPC PCSR 2012 includes a substantial amount of design information, although some aspects of the design are still to be finalised. The design is detailed in Chapter 9 of the PCSR with further detail in Refs 12, 13 and 15. Systems significant to this function include:

- circulating water filtration system (CFI);
- essential service water system (SEC);
- auxiliary raw water cooling system (SEN);
- circulating water system (CRF);
- intake coarse filtration and trash removal system and filter debris recovery pit (SEF); and
- ultimate cooling water system (SRU).

45 Selected claims for these systems are detailed below.

3.1.5.1 Circulating water filtration system (CFI)

46 The main pumping station of the CFI comprises of four separate trains of class 1 systems, which acts to remove debris from the sea water and direct it to various systems required for providing sea water cooling. The screens and chains are controlled to respond to the level of debris deposited and diverse spray systems help to clear the filter panels.

47 In addition to providing redundancy and diversity in the main intakes, there is provision to take water from the discharge pond if the filters in the CFI system are not available. In this case, a grid removes large debris.

48 The configuration selected resulted from an ALARP optioneering study. The primary driver for the number of intake heads is vulnerability to ship collision and aircraft crash and to a lesser degree clogging. The option of having two water intakes provides a reasonable level of redundancy, and contributes protection against the aircraft crash and ship collision hazards, provided that there is an adequate separation between the intakes. However, NNB GenCo argues that the majority of events challenging the integrity of the

sea water systems are caused by clogging of the intakes. It argues that the two deep sea water intakes designed for HPC are likely to be far less sensitive to clogging hazards.

49 NNB GenCo reports that it has taken account of operational experience feedback by providing band screens in addition to drum screens and by improving the provision of pressure-measurement instrumentation downstream of the screens, including early warning in the main control room of level transients.

50 Although the system is essentially automated, manual function is available.

3.1.5.2 Essential service water system (SEC)

51 The essential service water system (SEC) cools the heat exchangers of the component cooling water system (RRI) using sea water from the heat sink (downstream of CFI filtering).

52 The SEC is safety classified as class 1. The single failure criterion has been applied in order to ensure a sufficient level of redundancy.

53 To ensure the continuous flow rate of sufficiently cool filtered water to the RRI / SEC heat exchangers, the SEC system consists of four independent trains: two taking from the central drum screens and two from the chains. However, each SEC pump can be aligned to any filter via a common header which is normally closed.

54 The SEC system is designed so that, in all operating configurations, the loss of one or two trains does not compromise the cooling of the nuclear auxiliaries and particularly the safeguard auxiliaries.

55 Loss of essential service water, results in loss of the component cooling water system (RRI), which:

- removes decay heat from the primary circuit via the safety injection system / residual heat removal system (RIS/RRA) in normal shutdown and accidental scenarios;
- removes decay heat from the fuel pool cooling system;
- removes heat from trains 2 and 3 (refrigeration units) of the safety chilled water system (DEL); and
- indirectly maintains the primary circuit inventory by cooling the thermal barriers of the primary coolant pumps to ensure the integrity of the pump seals.

56 Detailed characteristics of the SEC [ESWS] circuit and equipment will be provided at a later stage.

3.1.5.3 Ultimate cooling water system (SRU).

57 The ultimate cooling water system will remove heat from the following:

- the containment, via the containment heat removal system (EVU) in some infrequent faults and severe accidents; and
- the fuel building pool via the third train of the fuel pool cooling system (PTR) for certain accidents involving loss of cooling to the spent fuel storage pools.

58 The SRU system is classified as safety class 3. It contains two 50% trains which are both necessary to supply the cooling needs of the EVU in the first 15 days after an event. It is designed to provide support to continued heat removal in design basis faults and severe accidents.

59 Normally, train 1 is in standby with valves closed. These are operated manually. The trains can be manually aligned to either of two screens.

60 Each train includes a pump supplied from a switchboard backed up by a main emergency diesel generator and an ultimate diesel generator.

61 Loss of the ultimate cooling water system results in loss of cooling to the containment building. In some infrequent faults this leads to an increase in containment pressure and to loss of backup cooling to the pond.

62 As a class 3 system, the SRU is not subject to the analysis of all internal and external hazards, but hazards are considered on a case by case basis. In particular, the design of the SRU must take account of the hazards that may lead to loss of the pumping station (particularly situations involving clogging).

63 Detailed characteristics of the SRU circuit and equipment will be provided at a later stage.

3.1.5.4 The circulating water system (CRF)

64 NNB GenCo claims that the circulating water system is not directly safety-related. However, automatic tripping of the CRF pump is required in the following situations:

- In the event of a significant level difference between upstream and downstream sections of the sea water filtration system drum screen or low water levels downstream, tripping of the CRF pumps protects the filtration devices and recovers sufficient margin for operation of the essential service water system.
- In the event of high water levels in the turbine hall condenser pit and/or the SEC pit, tripping of the CRF pumps protects from a flooding in the turbine hall due to a break of CRF pipes.

3.1.6 Adequacy of steam and power conversion systems

65 The HPC PCSR 2012 reference design for steam and power conversion systems is discussed in Chapter 10 of the PCSR as well as Hinkley Point C specific System Design Manuals. The following system safety cases have been written or extensively revised for HPC PCSR 2012:

- Sub-chapter 10.2 '*Turbine Generator Set'* is absent from consolidated GDA PCSR 2011 and contains a brief description of the system.
- Sub-chapter 10.4 '*Other Features of the Steam and Power Conversion Systems'* has been modified to insert information on systems not covered by consolidated GDA PCSR 2011 and some of the feed-water plant systems and the safety requirements and the design features on each system have been addressed.
- Sub-chapter 10.6 '*Main Feed water System'* describes the role it plays in maintaining appropriate primary circuit cooling during normal and accident conditions; limiting primary circuit overcooling.

3.1.6.1 The turbogenerator

66 The topics of turbine protection and fire countermeasures are addressed at the claims level in Chapter 10.2 Subsection 4.1 of Ref. 1.

67 Measures are taken to protect the turbine with redundant fault detection and trip circuits which trigger the fast closure of the steam inlet and feed-water extraction valves.

68 NNB GenCo claims probabilistic analysis demonstrates that the frequencies of turbine-generated missiles are ALARP.

69 In respect of control, the duration of the turbine run up to synchronising and rate of loading after synchronising, is dependent upon the length of the shutdown prior to start-up. Outside start-up periods, load increases are limited to:

- 10% full power instantaneously, from initial power of between 15% full power and 90% full power; and
- 5% per minute, from initial power greater than or equal to 15% full power.

70 The PCSR does not explain the reasoning.

3.1.6.2 Other features of the steam and power conversion systems

71 This topic includes the main condenser and systems associated with feed-water supply and steam systems which bypass the turbine. NNB GenCo argues that the condenser system is not the subject of direct safety claims.

72 The turbine bypass system is described in Chapter 10.4 Subsection 3 of Ref. 1. It is used to dump steam directly to the condenser during part-power operation. This allows design steam conditions to be maintained in the steam generators and primary plant.

73 The turbine bypass to the condenser accommodates the discharge of excess steam from the nuclear steam supply system during transient conditions (house load operation, large load decrease, turbine trip, and so on)**.** It is therefore designed to handle approximately 60% of the nominal steam flow produced by the reactor.

74 The condenser turbine bypass system fulfils the following functions:

- automatic heat up and cool down operations between safety injection and reactor heat removal system (RIS/RRA) connection and the hot shutdown state;
- controlling the average coolant temperature (complementing the rod control system) between 0% and 25% full power;
- control of the secondary pressure during starting up and synchronising the turbine to the grid by directing the steam to the condenser; and
- removing the excess steam to the condenser during significant operating transients, both normal and accidental, without causing the atmospheric relief valves to open and without resulting in automatic reactor shutdown.

75 The PCSR (Ref. 1) claims that there are no specific nuclear safety claims on the turbine by-pass system. Therefore, the turbine by-pass system is not safety classified.

3.1.7 Heating, ventilation and air conditioning (HVAC) systems

76 Heating, ventilation and air conditioning (HVAC) systems are described in Chapter 9.4 of Ref. 1. The UK EPR™ has a particularly complex HVAC system, designed with the intention of minimising radiological releases in normal operation and faults.

77 The ventilation systems play a direct role in supporting the third basic safety function; containment of radioactive substances. The systems reduce radioactive discharges into the environment in design basis events.

78 The purposes of the ventilation systems are to:

- maintain ambient conditions within acceptable limits for staff and equipment;

- protect staff and equipment against specific risks from the inside of the buildings (for example suffocation, explosion and fire); and
- monitor and limit radioactive discharges during normal operation and in accident conditions.

79 The ventilation and cooling systems are organised into three groups:

- systems or parts of systems which contribute to reducing radioactive discharges;
- systems that maintain the ambient conditions required for the safety and habitability of the main control room; and
- the support cooling systems for the safety classified ventilation systems.

80 Filtration of the extraction flow uses high efficiency particulate air (HEPA) filters and, if necessary, iodine filters. The decontamination factor requirements are defined. Discharge is to the vent stack.

81 The ventilation systems have been safety classified as F1 based on a French system and the design of F1-classified systems must meet the single-failure criterion. Also F1 components must be powered by the main emergency diesel generators.

82 The following safety-related components of the HVAC system can be powered by the ultimate emergency diesel generators:

- elements contributing to the containment of radioactivity during severe accidents; and
- supporting systems.

83 Elements of the ventilation and cooling systems must be qualified to accomplish their safety function under the ambient conditions anticipated for the duty. In the event of fire, fire dampers or fire-proof ducts are required to isolate the affected compartment.

84 Explosion-proof dampers are installed in air-intakes and air exhaust in buildings when it is necessary.

85 Areas presenting a risk of explosive atmosphere – for example battery rooms – are ventilated with a minimum air change rate or have specific provisions for hydrogen mitigation. Measures are taken to avoid local accumulation of an explosive atmosphere. If there is a risk of an explosive atmosphere being produced (for example due to failure of the ventilation system), an alarm is sent to the control room.

86 The fans are non-overloading direct-drive types (the motor power is sufficient over the entire power curve of the fan).

87 Local electrical heaters are installed in several rooms to maintain ambient conditions during the low temperature periods and more particularly to avoid boron precipitation in pipework relating to the supply of primary coolant.

3.1.7.1 Ventilation systems for the nuclear auxiliary building and the fuel building (DWN and DWK)

88 The DWN ventilation system for the nuclear auxiliary building and its extension, the DWK ventilation system for the fuel building operate continuously. They are designed for the following purposes:

- keep the ambient conditions within limits prescribed for correct operation of equipment and/or staff;

- ensure during normal operation that contamination is not spread by ventilation flows;
- reduce the concentration of aerosols and radioactive gases in the atmosphere;
- keep a negative pressure in the nuclear auxiliary building and the fuel building compared to ambient;
- isolate the air intake and the extraction from the nuclear auxiliary building in the event of an earthquake; and
- during shutdown, supply air to the containment sweep ventilation system (EBA).

89 The air supply is continuous and distributed to:

- the nuclear auxiliary building; and
- the fuel building.

90 The extraction is taken from:

- the nuclear auxiliary building;
- the fuel building; and
- the entire controlled area of the four safeguard buildings.

91 The DWN fan flow rate is adjusted by a variable fan speed to maintain the required vacuum inside the nuclear auxiliary building. No air is recirculated, but because of the potential for the presence of airborne contamination, the extract flow is filtered and discharged via the stack.

92 The system flow rates are increased during outages when the relevant rooms are open to atmosphere.

93 The nuclear auxiliary building ventilation system feeds a number of purge systems considered in more detail later in the assessment.

94 The system is classified as class 2. The DWN and DWK systems are not required to meet the single failure criteria. Only the dampers of the safety-classified DWK system meet the single failure criterion and therefore have redundancy.

95 NNB GenCo has provided information on the configuration of the system, its functional requirements and the ambient conditions that must be maintained. They advise that the flow rates remain to be confirmed by detailed studies. This is likely to include revision to take account of revised assumptions on ambient conditions applicable during the plant operating life.

96 Local cooling units are installed to maintain temperature in accordance with equipment requirements in key areas.

97 The chilled water for the local cooling units is provided by the DEL system in the primary coolant injection and boric acid makeup pumps rooms and by the DER system in other rooms.

98 The heater units in the boron rooms and RBS pump rooms are backed up by power from the main diesel generators. However, systems are not provided with power in the event of station blackout.

99 If radioactive iodine is detected in the air, the extraction from the affected cells is processed by iodine filtering. A maximum of four cells can be switched automatically to iodine filtration, but only three if the high capacity EBA system is in use (during outages).

100 In fault conditions, air supply to potentially contaminated zones is isolated and extraction directed to iodine filters. These are automatically isolated in the event of fire in the units.

101 In the case of low air temperatures, there is automatic protection to stop air supplies.

3.1.7.2 Containment cooling and ventilation system (EVR)

102 The containment cooling and ventilation system (EVR) is required to maintain conditions suitable for staff access and to work in the reactor building and the ambient conditions suitable for equipment and structures. Details of its system function are provided in Ref. 32.

103 A significant fraction of this system operates by closed-circuit cooling; rejecting heat to chilled water.

104 To enable access during power operation and to reduce the risk of radiological effects on staff, the containment is divided into two separate areas:

- a service area, which is accessible during plant operation; and
- an equipment compartment, which contains the primary circuit.

105 The service area system operates in combination with the containment sweep ventilation system (EVB), which is used to purge the atmosphere prior to outages.

106 The PCSR (Ref. 1) argues that it is not possible for leakage of activity between the plant areas of the containment and the service area.

3.1.7.3 Containment purge (EBA)

107 The EBA system makes a contribution to limiting radioactive release to the environment in normal operation by its filtering function and in faults, by closing down to isolate the containment building. It also acts to limit releases for faults occurring when containment is not intact.

108 Whenever necessary during normal plant operation, the low capacity EBA [CSVS] operates in open-circuit mini-purging mode to ventilate the service area of the reactor building; this enables the following:

- reduction in the activity of the atmosphere in the service area due to the presence of noble gases and tritium;
- fresh air supply for the atmosphere in the service area;
- creation of positive gage pressure in the stairways, to maintain their availability in the event of fire; and
- ensuring dynamic containment between the two areas of the reactor building by extraction of the air from the equipment and filtering compartment.

109 The high capacity EBA is used during outages for the following purposes:

- to reduce the concentration of fission or activation products in the reactor building atmosphere to allow access as soon as possible at cold shutdown; and
- to keep the ambient temperature and relative humidity acceptable for staff working in the reactor building during cold shutdown periods.

110 Air supply and conditioning for the EBA subsystem is provided by the DWN system (see Section 3.1.7.1).

111 In the event of a fuel handling accident in the reactor building, or a LOCA from the decay heat removal system, with an open equipment hatch the EBA system limits releases as follows:

- The containment isolation valves are closed.
- The air supply in front of the equipment hatch is isolated.
- The extraction of the low capacity EBA ensures dynamic containment of the reactor building by ensuring that net flow through openings is always inward. The air is filtered through a HEPA filter and iodine filter before discharge to the stack.

112 These functions are provided with redundancy to meet single-failure requirements. More generally, this system is required to close, to enable isolation of containment when required.

3.1.7.4 Ventilation System for the uncontrolled area in the safeguard building (DVL)

113 The DVL system is designed to remove heat released by operating equipment (lighting and heat from equipment, with the exception of the main motors which are cooled separately).

114 The DVL ventilation system is a support system for C&I equipment, for the electrical switchboards and mechanical equipment. It maintains acceptable temperatures inside the non-controlled portions of the safeguard buildings for proper operation of equipment and personnel access.

115 The DVL system performs significant safety functions and hence must be designed to accommodate single failures. This includes diversity of heat sink between water and air cooling.

116 As a result of GDA, significant enhancements to this system are planned. These will ensure that the system can meet the requirements for safety class 1. Preliminary information on these changes has been provided to ONR and a detailed justification will be provided in the next revision of the HPC PCSR.

3.1.8 Spent fuel pool resilience modifications

117 As a result of discussions during GDA, the fuel storage pond has been examined to ensure the resilience of the systems to potential accident conditions and a number of modifications / studies proposed. These include:

- CSNE0004UK – qualification of the performance of fuel building instrumentation adding this to the severe accident C&I scheme.
- CCSE0047UK – establishment of passive automatic opening of the spent fuel cooling hall to the nuclear auxiliary building to improve protection to over-pressurisation of the spent fuel pool hall.
- CCSE0048UK – a system to avoid explosive hydrogen concentrations in the spent fuel pond area.
- CCSE0023UK – provision of an external connection to allow re-supply of water to the spent fuel pool via the raw water system.

118 In addition, work is underway to examine the vulnerability to fuel transfer tube leakage and the temporary isolation of penetrations in the refuelling cavity, including procedures for this.

4 ONR ASSESSMENT

119 I have examined the HPC PCSR 2012 head document to determine areas for targeted sampling. This review has excluded consideration of fuel handling, severe accidents and containment response, which will be done by others. The primary focus of this assessment is Chapter 9; Chapter 10 and Chapter 14 of HPC PCSR 2012 (Ref. 1).

120 This assessment has been carried out in accordance with ONR HOW2 BMS policy (Ref. 2).

4.1 Assessment

4.1.1 Design basis analysis

121 Within the head document of HPC PCSR 2012 (Ref. 1), Chapter 14, NNB GenCo claims that the analysis performed for and reported in the consolidated GDA PCSR 2011 (Ref. 5) is applicable and appropriate for HPC. Therefore, no HPC site-specific DBA is presented within HPC PCSR 2012 (Ref. 1). Instead, the licensee provides statements within the head document which it claims substantiates that the consolidated GDA PCSR 2011 DBA is representative of future HPC site-specific DBA, including its applicability to a twin-reactor site.

122 HPC PCSR 2012 (Ref. 1) states that no new HPC site-specific DBA faults have so far been identified as a result of HPC being a twin-reactor site. HPC PCSR 2012 further states that the HPC fault list will be reviewed and any changes to the fault schedule that are specific to HPC will be included in the DBA. Plans for the development of the HPC fault schedule have been provided by NNB GenCo and are considered below. However, it is noted that an initial draft of a HPC reactor building fault schedule will not be available until the end of 2014, with the remaining plant areas following at a later date.

123 NNB GenCo claims that HPC being a twin-reactor site will not impact on the DBA modelling assumptions or assessment methodologies and that there are no new HPC site-specific DBA faults as a result of HPC being a twin-reactor site. The primary argument supporting this claim appears to be the independence of the two EPR units. NNB GenCo has provided a document, UK EPR™ Hinkley Point Project: identification and review of the safety implications of a twin-reactor design for Hinkley Point C (Ref. 9). This document provides a qualitative assessment of the hazards specifically associated with the HPC twin-unit configuration and determines whether the twin-unit configuration significantly changes the risk to nuclear safety associated with the generic site presented in the GDA PCSR (Ref. 5).

124 The key findings of this report (Ref. 9) concludes that, based on the level of design currently available, it is expected that there will be no significant increase in level of risk per unit, compared with the GDA baseline. Also, there may be some specific advantages to safety that can be realised as a result of a twin-unit configuration with the units sharing some services and facilities. The information provided in this report demonstrates that NNB GenCo is progressing the development of a twin unit justification in an appropriate manner. However, it remains my opinion that NNB GenCo's fault studies specialists should be actively monitoring the development of the interfaces, interconnections and shared services to ensure that the DBA faults for the twin-reactor HPC site comply with the assumptions made within GDA.

125 It has been stated in HPC PCSR 2012 (Ref. 1) that conservative analysis assumptions with respect to plant availability mean that the acceptability of the fault consequences is independent of conventional island system design or responses and that where

conventional island systems / components perform a safety function in the GDA reference design, the safety classification of equivalent HPC-specific conventional island systems / components will be the same or higher. These arguments support the claim that the GDA PCSR will bound the HPC site-specific design basis analysis. Evidence supporting these arguments will have to be provided to ONR before these claims can be assessed in more detail. This will be the subject of future technical meetings with NNB GenCo.

126 I note that HPC PCSR 2012 (Ref. 1) stated that the HPC site-specific DBA will be performed using the same assessment methodology as GDA, with the same acceptance criteria. The methodology was assessed as part of GDA and found to be fundamentally acceptable. However it is worth noting that a number of GDA assessment findings (AF) relate to methodology, and in particular the validation. I consider that it would be appropriate for NNB GenCo to develop plans to address all methodology related AFs before confirming that the assessment methodology will be the same as that used in GDA.

127 I further note that site-specific aspects of the design (such as assumptions on grid stability and turbine dynamic response) will need to be accounted for appropriately in the limiting conditions of operation assumed as a basis for design basis fault analysis.

4.1.2 Fault and protection schedule

128 The head document of HPC PCSR 2012 (Ref. 1) notes that no HPC site-specific fault and protection schedule has been produced for submission within HPC PCSR 2012. NNB GenCo has stated that for the purposes of HPC PCSR 2012, the content of the GDA fault and protection schedule is applicable to HPC. ONR's GDA assessment finding AF-UKEPR-FS-29 states:

"The fault schedule shall be updated as part of each major safety submission to reflect the design basis safety case at the time of the submission. The updated fault schedule shall be reported within each submission."

HPC PCSR 2012 does not appear to have considered ONR's finding AF-UKEPR-FS-29. Considering that this is one of the findings required prior to first nuclear safety-related concrete, it is not viewed as ideal that the fault schedule has not been updated as part of this submission.

129 Further, a regulatory action (Action #1110) was placed on NNB GenCo by ONR:

"NNB to provide a programme to ONR, on how NNB will systematically demonstrate that the HPC list of DBA PCC faults is complete, with respect to initiating faults, and that the associated fault frequencies are appropriate"

Action #1110 is still ongoing. However in response to this action, NNB GenCo has now supplied ONR with HPC specification for fault schedule development (Ref. 10). This document provides a specification for the HPC fault and protection schedule. From initial assessment, I consider that this document makes the right kind of commitments to address Action #1110. However, it lacks some of the detail that ONR was expecting (and that ONR would require) to progress this action. In general, this document provides commitments about the content of the fault schedule, but limited information on the methodology. Further information on the methodology has also been provided to ONR at a recent level 4 regulatory meeting in November 2013 (Ref. 11); this information has gone some way to addressing regulatory Action #1110.

130 Ref. 10 explains that NNB GenCo has considered Sizewell B's and the most recent Hinkley Point B's (HPB) nuclear power plants fault schedule format and methodology and will adapt HPB's methodology for HPC. This allows ONR inspectors to have an idea of NNB GenCo's high-level plans, but ultimately ONR requires detail on how this is to be implemented.

131 Ultimately, the HPC fault and protection schedule also needs to cover all sources of radioactivity, including those originating from the:

- fuel route (partly covered by GDA but requires further development);
- interim fuel storage facility; and
- intermediate-level waste store.

132 Development of these fault schedules is the subject of regular interaction between ONR and the licensee.

4.1.3 Acceptance criteria

133 I have reviewed the acceptance criteria detailed in Chapter 14.2.1 of Ref. 1 against the following HSE SAPs, in particular: ERC.1, FA.7 and NT.1 (Target 4).

134 It is my view that the approach described in Ref. 1 needs to be updated to reflect the final outcome of GDA. Firstly, if it is reasonably practicable to reduce fuel failures and consequential radiological releases, then NNB GenCo should do so, irrespective of the frequency of the fault. ONR's expectation for design basis faults is that barriers to the release of radiation should remain intact where reasonably practicable. This is the case for example in rod ejection faults, where selection of a suitable rod cluster control assembly insertion limit can potentially prevent fuel failure; see ONR's assessment finding (AF-UKEPR-FS-16).

135 On a more detailed level, the decoupling criteria given are a reasonable representation of the criteria defined for GDA, but omit the requirement to set limits on cladding embrittlement for fuel pins in intact circuit faults. These are required to demonstrate that the fuel retains its structural integrity in such faults.

136 In the case of less frequent faults within the design basis, I note that NNB GenCo is proposing to ensure that the likelihood of fuel failure must be sufficiently low to ensure that the radiological risk from any one fault does not make a disproportionately large contribution to the risk of the plant (as assessed against SAP NT.1, Target 8). I welcome this as a necessary, but not sufficient, condition for acceptability. It does not override the need for conservative deterministic fault analysis.

4.1.4 Equipment qualification

137 Analysis of the qualification of equipment operating envelope is an important part of specifications for their use. This includes specification of instrumentation and equipment required to ensure containment integrity in severe accidents.

138 I have considered the overall approach in the context of SAP EQU.1: *Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.* (This includes fault and severe accident conditions as required).

139 The standard assumption for normal operating conditions is a maximum ambient temperature for safety-related equipment of 50 ºC. The minimum temperature is -35 ºC for a short period.

140 To achieve a suitable operating environment, in these ambient temperatures, requires HVAC. Chillers are assumed to be capable of supporting this given an external air temperature of 47 ºC and diesels are assumed to operate at air temperatures below 44 ºC. This is subject to review as part of the redesign of the HVAC system and an internal ambient value of 50 ºC is under consideration in the context of work to address GDA assessment findings.

141 I note that this discussion is informed by assessments of the likely consequences of global warming over the projected operating life of the station and I regard this as a commendable approach.

142 In the case of faults, I note that the main steam line break and the double-ended guillotine fracture of the primary-circuit cold leg are used to define limiting conditions. I note that this is despite the fact that NNB GenCo has made break-preclusion arguments. I judge that this approach is consistent with good practice.

143 The duration of the fault considered is assumed to be limited for equipment qualification purposes. The medium-term / long-term limit is fixed at 24 hours. I consider this to be too short for some cases and NNB GenCo should confirm that there are no cliff edges in terms of risk in the first few days after the event. This will be raised with NNB GenCo as a level 4 regulatory issue (see Table 2) and I will pursue this as part of my ongoing assessment of the developing safety case.

144 I also note that the steam temperature assumed is limited to the saturation temperature postulated for the containment. This neglects pressuriser steam-space LOCAs, or conditions in the immediate path of a jet of primary coolant resulting from a breach. Steam-space discharges could be considerably hotter than specified and consequential damage can be anticipated. This should be explained in the head document. This will be raised with NNB GenCo as a level 4 regulatory issue and I will pursue this as part of my ongoing assessment of the developing safety case.

145 The topic of equipment qualification is generally iterative, in that requirements need to take account of what equipment can achieve. I regard the current position as interim and will revisit this topic later in permissioning.

4.1.5 Adequacy of ultimate heat sink

146 I examined the PCSR documentation in order to find a clear statement of the contribution of the systems to high-level safety functions and hence to their classification. In general, I found adequate description of the systems and arguments presented on the resilience of the proposed systems, but only limited information justifying design decisions. I have discussed this with NNB GenCo and it advises me that it is in the process of preparing documentation describing the primary and support systems required for particular safety functions. I expect this documentation as part of the next revision of the HPC PCSR and will consider it as part of my assessment.

147 Although the heat sink design was out of scope for GDA, some high-level assessment was made as part of GDA and I note that it was overall supportive of the design concepts. I examined the systems to ensure that they met the requirement of SAP EDR.2: *It should be demonstrated that the required level of reliability for their intended safety function has been achieved*.

148 In assessment of these systems, I have interpreted the NNB class definitions from Ref. 23 as follows:

- Class 1 – any safety feature that forms a principal means of fulfilling a principal role in ensuring nuclear safety.
- Class 2 – any safety feature that makes a significant contribution to fulfilling a principal role in ensuring nuclear safety, or forms a principal means of ensuring a safety function which makes a significant contribution to nuclear safety.
- Class 3 – any safety feature that contributes to a function which makes a significant contribution to nuclear safety, or fulfils another safety function.

149 I have chosen to examine the following systems:

- circulating water filtration system (CFI) because it is required by all sea water systems;
- essential service water system (SEC) because it supports a range of safety equipment;
- ultimate cooling water system (SRU) because it has important functions in severe accidents and in providing diverse heat-removal functions; and
- circulating water system (CRF) because it places major demands on the performance of the intake system.

4.1.5.1 Circulating water filtration system (CFI)

150 The CFI system plays an important role in meeting the decay heat removal safety function and I am encouraged to note that NNB GenCo has given the major parts of this system a class 1 safety classification (Ref. 12).

151 An ALARP study of the options for the design of the inlets is reported in Ref. 12. The option of: two intake heads, two intake tunnels, and two linking tunnels has been selected as the ALARP solution because it provides adequate redundancy and segregation without being disproportionately expensive. I note that an option of air cooling the safety systems was discounted on cost and novelty grounds. I accept that this would be to some degree novel, but Sizewell B has a reserve ultimate heat sink supporting the decay heat removal system and I therefore expect adequate measures to address the potential for loss of primary heat sink. I do however note that once-through feed systems can be used for decay heat removal if provided with adequate support systems. In conclusion, I expect the CFI system to be designed for a high degree of reliability.

152 The detail of the hazards considered are assessed in the external hazards topic area (Ref. 20). However, I note that a wide range of external and internal hazards are considered and automatic protection has been provided to ensure the integrity of essential service water supplies.

153 Loss of water level is monitored by both level sensors and head-loss sensors of diverse types. These systems feed information to both the protection system and the safety automation system. The implementation of these systems and the reliability claims will be assessed in the C&I topic area (Ref 21), but I support the need for diversity in monitoring and trip systems in this area.

154 On detection of low water levels in the seawater headers, the main condenser and conventional auxiliary cooling water systems are tripped to protect the essential service water system. NNB GenCo argues that the reduced pressure loss across the system will free some of the debris. It will also reduce the rate of fouling and help preserve a net positive suction head for sustained functioning of the sea water pumps.

155 Should common mode failure of the screens occur, there is the potential to realign one of the two essential service water system and one of the ultimate cooling water system pumps to draw water from the outflow. This is achieved by closing a sluice gate. This is a fairly low probability event, but based upon experience, can not be discounted.

156 Numerical reliability figures for this system derived in Ref. 13 are assessed in the PSA topic area (Ref. 25). These will need to show a satisfactory level of reliability, but subject to this requirement, I consider the level of redundancy and diversity provided for the filtering systems appropriate in the context of my understanding of relevant good practice.

4.1.5.2 Essential service water system (SEC)

157 The essential service water system is required to cool the fuel pool in all reactor states and to provide the heat sink for the reactor primary circuit in shutdown and post-trip states (via the residual heat removal system) when cooling via the steam generators is insufficient or unavailable.

158 In the event of loss of the essential service water system at-power, the secondary circuit is cooled by the emergency feed water system with steam dumped via the main steam relief trains or the steam generator safety valves.

159 In the case of steam release to atmosphere, the EFWS tanks contain sufficient water supplies for a small number of days of initial post-trip cooling; after which several further days of make-up supply are available from the fire fighting water supply system. Since main coolant pump seal injection flow is lost in this event, primary circuit integrity is assured by deploying all four primary seals (Ref. 12). I have asked for further information on this topic and will require a detailed justification for the qualification of this system in the event of loss of thermal barrier cooling. Failing the sustained operation of these seals, the system would need to be depressurised and water injected into the primary circuit using the low head safety injection (LHSI) system. I have asked for further information on the ability to maintain adequate shutdown margin in cases when the EBS is not available. I intend to progress this is a topic as resolution plans for existing assessment findings are agreed.

160 In outages where the primary circuit is open, make-up to the primary circuit is supplied by low head safety injection (trains 1 and 4) from the in-containment refuelling water storage tank; with the LHSI pumps being cooled by a diverse air cooled system through the chilled water system provided in one of the four trains of the ultimate cooling system.

161 NNB GenCo recognises that the SEC system is safety class 1 and requires tolerability of single failures (Ref. 12). The system consists of four trains with dedicated electrical supplies, backed up by main diesels. There is some ability to manually reconfigure the pipework. I concur with these decisions, but have not examined the consequence of the current level of electrical diversity and I will require responses to my outstanding questions on this topic. Details of the system design will be provided for the next revision of the HPC PCSR and further assessment will be made at that stage. This will be raised with NNB GenCo as a level 4 regulatory issue (see Table 2) and I will pursue this as part of my ongoing assessment of the developing safety case.

4.1.5.3 Ultimate cooling water system (SRU).

162 This system is the principal means of ensuring heat is removed from the containment building in the event of a release of energy and activity from the primary circuit into the containment building. It is also claimed as a diverse system for heat removal from the spent fuel pool. I therefore believe that it plays a significant role in ensuring a principal

safety function. My expectation is therefore that it would be categorised as class 2 rather than 3. I also expect that the system would be included in analysis of hazard resistance to ensure that it was adequately robust to be available in the case of a severe accident. I note that further details of the justification of classification will be available for the next revision of the HPC PCSR and further detail of the system design. I will consider this issue further when the information becomes available.

4.1.5.4 The circulating water system (CRF)

163 NNB GenCo claims that the circulating water system is not directly safety-related except that it may be necessary to trip the system in order to preserve the safety function of other systems reliant on the sea water intakes (Ref. 19).

164 I judge that this reasoning is sound on the basis that in the event of loss of condenser function, the reactor will trip and decay heat removal does not require the main condensers.

165 NNB GenCo has recognised that in the event of screen blockage, the main circulating water system pumps can place significant load on the screens and also main flow can empty the intakes in a short time. Provision is made to trip the system. I note that NNB GenCo intends to utilise diverse instrumentation as part of this protection.

166 I judge that the functional requirements have been appropriately considered. The details of these provisions will be examined during the assessment of the next revision of the HPC PCSR.

4.1.6 Adequacy of steam and power conversion systems

167 The turbogenerator plant was excluded from the generic design assessment on the basis that the generator unit needs to meet the local requirements of the electricity supply grid and that utilities usually make commercial decisions on the supply of turbines. Information on the turbine has now been introduced to HPC PCSR 2012.

168 Again, I examined the text for clear statements on the safety function of the equipment and a demonstration of adequate reliability as required by SAP ERD.2. In this area, my focus has been on hazards introduced by the potential for the turbine and its associated control systems to malfunction.

4.1.6.1 The turbogenerator

169 While the principle role of the turbogenerator is to transform thermal energy contained in the steam produced from the steam turbines into electrical power, there are three hazards associated with the turbine:

- it can fail in such a way as to generate damaging missiles;
- turbine lubricant and generator hydrogen cooling introduce the potential for fires in the turbine building; and
- the control of the turbine can introduce changes in steam demand that can potentially lead to damaging reactor power transients.

This needs to be reflected in the safety classification of the system and I propose to examine this aspect when NNB GenCo has finished its review of classification.

170 NNB GenCo does recognise these hazards and the claims made in respect to turbine-induced hazards are generally appropriate, but for a suitable and sufficient safety case, these need to be supplemented by supporting evidence and arguments.

171 The issue of fire protection and turbine fragmentation are assessed in the internal hazard topic area and I have not examined them.

172 In the case of power control, I view the specification of turbine controller performance as insufficient; however, Chapter 10.2 of Ref. 1 places some constraints on the turbine governor.

173 The difference between initial power raise after refuelling and subsequent power operation is recognised. Excluding initial start-up, Step changes in power (when operating at part power) are limited to 10% of rated power and a limit is placed on the rate of rise of 5% per minute. However, no information is provided on the automatic response of the turbine to changes in the frequency of the electricity supply grid. I therefore requested more information and this was supplied in a level 4 meeting (Ref. 15).

174 NNB GenCo advises that the turbine response to reductions in grid frequency will be to maintain a constant demanded power level, while the response to increasing grid frequency will be to reduce demanded power. However, the specification was subject to ongoing negotiations with the relevant authorities. In principle this seems acceptable, although further detail is required.

175 In conclusion, I will expect the fault studies to take account of plant operating conditions at the limit of the operating envelope that could reasonably be foreseen in combination with the fault. NNB GenCo is aware of this requirement and has advised that it plans to address it when the turbine design is finalised. This will be raised with NNB GenCo as a level 4 regulatory issue (see Table 2) and I will pursue this as part of my ongoing assessment of the developing safety case.

4.1.6.2 Turbine bypass system

176 I judge from the functional requirements identified for this system, that the system has an important part to play in cooling the plant post trip without releasing steam direct to atmosphere. It also has the capacity to make large changes to steam demand and hence reactor power levels, so that spurious operation could be a significant fault.

177 Experience at Sizewell B and elsewhere demonstrates that failures of the control system on the steam turbine bypass system can lead to rapid increase in steam demand from the steam generators – sufficient to require action of the protection system to limit consequential increases in reactor power. It follows that safety claims need to be made on this system. This should be recognised by NNB GenCo. This will be raised with NNB GenCo as a level 4 regulatory issue (see Table 2) and I will pursue this as part of my ongoing assessment of the developing safety case.

4.1.7 Heating, ventilation and air conditioning systems

178 The EPR has particularly complex HVAC systems, designed with the intention of minimising radiological releases in normal operation and faults. My assessment has focused on the following systems which I judge to be most significant in the context of fault studies:

- Air is conditioned, supplied to the reactor building and extracted by the nuclear auxiliary building ventilation system (DWN).
- Air supply, extraction and cooling within containment are maintained by the continuous containment ventilation system (EVR).

- Contamination levels in containment are controlled by the containment purge system (EBA) and specific filtering of activity in the vessel pit is provided by the internal filtering system (EVF).
- Ventilation of uncontrolled plant areas of the safeguard building is provided by the safeguards building ventilation system (DVL).
- The main control room is ventilated by a dedicated system. This is claimed to provide filtered ventilation and to have adequate redundancy and diversity of support systems. This has not been sampled because it has already been considered in some detail in GDA, which led to an assessment finding requiring NNB GenCo to review the system. The latter is also true of the diesel building ventilation system.

179 The general requirements of the HVAC systems are considered below, followed by consideration of specific systems. Consideration of the requirements for resistance to explosions has not been assessed. This will be covered in the internal and external hazards assessments (Ref. 20 and 22). A set of ambient conditions is established for plant depending on its thermal inertia. Detailed assessment of the values selected is considered in the external hazards assessment (Ref. 20).

180 The description provided in HPC PCSR 2012 (Ref. 1) shows that consideration has been given to a range of potential faults in the system and in particular, consideration is given to isolation of activity in the event of a release into various rooms within the reactor building.

181 Ref. 1 gives the functional requirements for the maintenance of ambient conditions in a number of rooms. However, these are general requirements and the functional requirements for particular systems are given only for selected systems (for example the boron storage criteria are explained). The information is in the form of limiting temperatures and does not include establishment of grace times in which mitigation of non-compliance would be required. I consider that this is needed to ensure consistency between design of the HVAC and that of the systems supported. This will be raised with NNB GenCo as a level 4 regulatory issue (see Table 2) and I will pursue this as part of my ongoing assessment of the developing safety case.

182 Environmental conditions for equipment required to maintain safety functions, in the event of loss of electrical supplies, was an issue during GDA and a number of findings are outstanding. These continue to be the subject of design work and will need to be addressed in the PCSR in due course. I have omitted these topics from assessment of HPC PCSR 2012 and this will be raised with NNB GenCo as a level 4 regulatory issue and will be progressed in technical meetings with NNB GenCo.

4.1.7.1 Ventilation systems for the nuclear auxiliary building and the fuel building (DWN and DWK)

183 The DWN system is described in Ref. 30 which gives an adequate description of the function of the system and its resilience to failures in related systems. The DWK system is described in Ref. 27.

184 The ventilation system for the nuclear auxiliary building DWN and its extension, the ventilation system for the fuel building DWK provide ventilation to areas of safety significance and have a role in limiting the spread of contamination. I therefore examined the safety case documentation to determine whether it detailed the failure modes and effects so that I could judge whether the categorisation and classification was adequately

justified and whether the design of the system included features intended to provide adequate resilience in accordance with the requirements of SAP EDR.2.

185 The system includes provision to address potential hazards arising from fire and earthquake. These are considered in the internal and external hazards topic areas (Ref. 20 and 22).

186 Operation in normal and fault conditions is considered and provision is made for adverse weather in the form of rain shields, filters and heat exchangers. Intakes are constructed from materials selected to avoid corrosion in the expected climatic conditions.

187 Isolation dampers and fans are arranged in such a way as to provide some tolerance to single failures, although this does not extend as far as providing full diversity and I note that common headers and discharge ducting to the stack is employed. Fans are of direct-drive electric designs to ensure robust operation.

188 The system comprises three heater trains of 33% capacity and four fans each of 50% capacity. The thermal flow rates and heat exchange rates will be confirmed by detailed studies.

189 The fans are shut down on loss of off-site power. The ventilation system for the nuclear auxiliary building DWN system power supply is not backed up, except for the heating (ensuring the minimum ambient temperature) which is backed up by power from the main diesel generators. In particular, the heating in the rooms containing 7000 ppm borated water for the primary coolant boration system has a powered backup.

190 Local air conditioning in selected rooms is powered by the main diesel generators. No provision is made for loss of main diesels. The significance of this is difficult to determine from the existing documentation.

191 The equipment provides significant resilience, but the loss of HVAC functions can be foreseen in accident conditions. The PCSR does not provide a suitable justification that essential safety functions will be maintained should a sustained station blackout event occur and this is the subject of a number of findings which were raised during GDA. This observation will be progressed in the context of the relevant regulatory issue (see Table 2).

192 I judge that the documentation for DWN generally lacks a clear link between the equipment and the detailed safety-case claims. However, NNB GenCo has advised me that this is being developed as part of an initiative on safety classification. I accept this. This system will need more detailed review when additional design information is available as part of the next revision of the HPC PCSR.

193 In the case of DWK, I note that the system will be modified to mitigate potential over-pressure events in the fuel building and the documentation will need to reflect this. This will be raised with NNB GenCo as a level 4 regulatory issue and will be progressed in technical meetings with NNB GenCo.

4.1.7.2 Containment cooling and ventilation system (EVR)

194 NNB GenCo advises that the cooling of the reactor pit is classified as safety category F2, which is the French equivalent to UK safety class 3 (Ref. 32), but the remainder of the system is not classified. This will need to be clarified in the UK context.

195 The PCSR states that the ventilation of the reactor vessel pit is responsible for removing heat from the control-rod drive mechanisms. The heat sink can be provided by either the component cooling water system (RRI) or the chilled water system (DER). There are two

trains, with segregated electrical supplies. The fans for the reactor pit have some backup electrical supplies in the event of station blackout. The reason for the requirement to cool the reactor vessel pit is not clearly presented.

196 The service area cooling is provided by local units supported by the chilled water system (DER). The coolers in the core instrumentation room have two times 100% capacity.

197 Of the support systems, the PCSR states that only the main fans, the reactor vessel pit fans and the RRI system are backed by main diesels. In the event of loss of main diesels, this system will not be available.

198 Details are given on the functional requirements of these systems, but the consequences of their failure are not detailed. NNB GenCo advises that the only safety function of the EVR is the cooling of the reactor pit during loss of power events.

199 For both divisions of the EVR system, NNB GenCo demonstrates that the system has some resilience to failures of support systems, but the consequences of failure of the EVR are not explained in detail. More information is needed on the consequences of failure of these systems. This will be raised with NNB GenCo as a level 4 regulatory issue (see Table 2) and I will pursue this as part of my ongoing assessment of the developing safety case.

200 Given that the focus of the design of the system of rupture foils and dampers, connecting containment rooms, is to ensure a high reliability of mixing in faults, I am sceptical about the claim that leakage between the equipment area and the service area can not occur, but the significance of the claim is not clear.

201 Overall, the PCSR (Ref. 1) provides an adequate description of the system, but not its detailed safety function. This will be assessed when the next revision of the HPC PCSR is received.

4.1.7.3 Containment purge (EBA)

202 NNB GenCo has classified the containment isolation and the low-flow filtering as of high safety significance. This is reasonable. However, the high-flow EBA is not safety classified (Ref. 31). This will need to be reviewed in the context of UK classification requirements.

203 The approach is to provide effective filtering of releases during normal operation and, so far as is reasonably practicable, containment to mitigate faults as part of defence-in-depth. This is a well-established practice and the containment isolation function is designed to be resistant to single failures.

204 The safety classification of the low-flow EBA appears to recognise its role in helping to mitigate faults occurring with the reactor containment open. The iodine filtering trains are redundant (2×100%) for this mode of operation. The system classification will need to be reviewed in line with UK expectations. This is covered in an existing GDA Step 4 assessment finding.

205 Some detail is given of the proposed practices for purging the containment prior to entry into the containment during outages. The principles appear to be sound, but the success criteria for these processes are addressed in the radiological protection topic area (Ref. 26).

206 The system is not backed up in the event of loss of 11 kV supplies. However, mechanisms for closing internal containment isolation valves are backed up.

207 Overall, in my view, the information provided is adequate for this stage of the project.

208 Also provided is a system to remove iodine particulate from containment and to purge the reactor building equipment space of the containment (EVF). This is designed for normal operation and is not claimed as a safety system, except that the associated fire dampers need to act to prevent the spread of fire in the reactor building. This appears to provide a degree of diversity for the purge function in normal conditions. I note and welcome this, but have not chosen to sample this system in detail on the basis that I judge that it is probably adequate for its limited role in faults and can be examined when more information is available in the next issue of the PCSR.

4.1.7.4 Safeguard building ventilation system (DVL and DWL)

209 The DVL system is designed to remove heat released by operating equipment (main motors are cooled separately). In particular, it is a support system for instrumentation and control equipment, for the electrical switchboards and mechanical equipment (Ref. 28). This function includes supplying the contamination-controlled part of the system (DWL). The system ensures that the maximum authorised temperatures are not exceeded.

210 As a result of assessment during GDA, the need to introduce increased diversity into the safeguard building ventilation system (DVL) was recognised and I met with NNB GenCo to review progress. A number of options for increasing the plant protection by modifying support systems were reviewed. The preferred design option for enhancement to the safeguards building ventilation system (DVL) is to add a new diverse class 1 safety system: DVLnew.

211 A number of design options have been considered, but the optimum is considered to be a two-division system each with two times 100% capability, powered by 400 V supplies, with dedicated transformers on separate divisions of the 11 kV supplies. The system will be designed to meet the requirements of projected global warming over the period of the plant life. NNB GenCo stated that discussions with suppliers were underway in order to provide equipment diversity where practical.

212 I am generally content with progress in this area. NNB GenCo has advised that the design has been analysed for the at-power condition, but not yet for shutdown conditions. The plan is to include some of the detail of the design in the basic design reference documentation. This will be subject to further review as part of my assessment of the next revision of the HPC PCSR.

4.1.8 Spent fuel pool resilience modifications

213 During the GDA Step 4, ONR required an enhanced safety case in support of the spent fuel pool and associated fuel handling areas / compartments (Ref. 24). From the robustness analysis, EDF and AREVA identified a number of generic and site-specific design changes. ONR is advised that work is progressing on developing these design changes and that generally no particular difficulties are anticipated in meeting ONR's expectations. This will be examined as part of my assessment of the next revision of the HPC PCSR.

214 The exception to this is the work to provide secondary containment around the fuel transfer tube. Assessment finding AF-UKEPR-FS-81 requires NNB GenCo to develop a safety case to demonstrate that the required reliability for the fuel transfer tube itself and the related watertight rooms can be achieved.

215 NNB GenCo advised that its suppliers were not confident of providing a seal at the interface between the fuel and the reactor building and therefore NNB GenCo proposes

to reduce the number of welds present in the fuel transfer tube and to argue that failure of this tube would be sufficiently improbable that mitigation measures do not need to be considered.

216 Based on the information available to date, I have advised NNB GenCo that it has not demonstrated that all reasonably practicable measures have been taken. Discussions are continuing on the resolution of this finding.

4.1.9 GDA assessment findings

217 During ONR's GDA assessment process, ONR raised 120 assessment findings in the area of fault studies, of which 24 are required before first nuclear island safety-related concrete; these are: AF-UKEPR-FS-29 and AF-UKEPR-FS-93 to 116. Currently NNB GenCo has only provided ONR with draft resolution plans for a small number of these GDA findings.

218 ONR is considering the draft resolution plans which it has been provided to-date and is in regular discussion with NNB GenCo on how all GDA AFs will be resolved. These AFs were developed by ONR's fault studies GDA assessment team through detailed assessment of safety documentation provided during GDA Step 4. This assessment considered consolidated GDA PCSR 2011 (Ref. 5). As the design basis analysis section of HPC PCSR 2012 (Ref. 1) is based on the sub-sections provided for the consolidated GDA PCSR 2011, it is my opinion that all GDA AFs raised as part of the GDA assessment process remain applicable to the HPC project and HPC PCSR 2012.

5 CONCLUSIONS AND RECOMENDATIONS

5.1 Conclusions

219 This report presents the findings of my fault studies assessment of NNB GenCo's pre-construction safety report 2012 for the Hinkley point C site (HPC PCSR 2012 (Ref. 1)).

220 The licensee has reported that no new design basis analysis work has been undertaken in support of HPC PCSR 2012. The basis of the DBA reported in HPC PCSR 2012 is that from the consolidated GDA PCSR 2011 (Ref. 5). These aspects of HPC PCSR 2012 were therefore considered by ONR as part of GDA and have not been reconsidered within this assessment. This assessment has instead considered whether the DBA analysis for the generic EPR considered at GDA is applicable to the HPC site, including the particular equipment provided for power generation and for the ultimate heat sink. A number of issues have arisen which will require resolution and these are summarised in Table 2.

221 NNB GenCo has provided claims and arguments within the head document of HPC PCSR 2012 that the DBA provided is applicable. However, at the current time NNB GenCo has provided insufficient evidence to support these arguments in the system description documentation. In particular, the description of the support systems provides details of the configuration of these systems and the measures taken to ensure suitable resilience. However, there is insufficient information at present on the safety functions of the systems; their failure modes and the effects of loss of system availability. This information is needed to justify the level of safety classification given to the system and the measures required to ensure adequate reliability.

222 The information on the turbine and steam dump systems is currently at a preliminary design level and will need significantly more information when the design becomes more mature.

223 In my opinion, HPC PCSR 2012 does not provide a sufficient safety justification for the HPC site outside of the scope of GDA. Rather, it provides a description of the proposed plant and details the outcome of site-specific design decisions. Evidence of a systematic design process will be needed. The rational behind the selection of design options is often missing or insufficiently detailed to substantiate the decision. This is particularly true in the area of support systems and the heat sink. However, I note that NNB GenCo is currently undertaking a major review of these systems, partly in the context of GDA findings relating to their adequacy and partly in the context of findings relating to safety system classification.

224 To conclude, I am broadly satisfied with the licensee's claims and arguments that the GDA DBA can be applicable to the HPC site. However, insufficient evidence has been presented on the basis of the design decision-making. Ultimately, NNB GenCo will be required to provide ONR with the evidence that DBA claimed in the PCSR is still valid for the HPC site or to provide a HPC-specific DBA safety justification. NNB GenCo should ensure that this information is available within the next issue of the HPC PCSR and that a HPC site-specific fault schedule is available to support the next issue of the HPC safety report. On the basis of the absence of satisfactory levels of information, particularly for systems outside the nuclear island, HPC PSCR 2012 is judged to be below the expected standard (IIS Rating 4).

5.2 Recommendations

225 With the exception of a number of issues raised within ONR's issues database (see Table 2), no other recommendations have arisen following my assessment of HPC PCSR 2012.

6 REFERENCES

1 NNB GenCo 2012 version of the Pre-construction Safety Report (PCSR) for the Hinkley Point C site. Submitted under cover of letter ONR-HPC-20337N, 06 December 2012. TRIM Ref. 2013/16143 and as detailed in UK EPR Master Submission List TRIM Ref. 2013/23292.

2 ONR How2 Business Management System, www.hse.gov.uk/nuclear/operational/assessment/index.htm.

Guidance on Production of Reports, AST/003 Revision 7, September 2013.
"Guidance on mechanics of assessment", Nuclear Safety Permission Step 1.4.1, TRIM 2013/204124.

3 Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf

4 UK EPR Pre-construction Safety Report – November 2009 Submission. Submitted under cover of letter EPR00226N. 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Master Submission List. November 2009. TRIM Ref. 2011/46364.

5 UK EPR Pre-construction Safety Report – March 2011 Submission. Submitted under cover of letter EPR00844N. 31 March 2011. TRIM Ref. 2011/200260 and as detailed in UK EPR Master Submission List. March 2011. TRIM Ref. 2011/200786.

6 PCSR Sub-Chapter 14.4 Update – Analyses of the PCC-3 events UKEPR-0002-144 Issue 08, November 2012, TRIM Ref. 2012/462138
PCSR Sub-Chapter 15.1 Update – Level 1 PSA UKEPR-0002-151 Issue 05, November 2012, TRIM Ref. 2012/439082
PCSR Sub-Chapter 16.3 Update – Practically Eliminated Situations UKEPR-0002-163 Issue 04, November 2012, TRIM Ref. 2012/460008
PCSR Sub-Chapter 16.4 Update – Specific Studies UKEPR-0002-166 Issue 04, November 2012, TRIM Ref. 2012/467463.

7 HSE Design Acceptance Confirmation (DAC): www.hse.gov.uk/newreactors/reports/step-four/close-out/epr70475n.pdf

8 EA Statement of Design Acceptability (SoDA): https://brand.environment-agency.gov.uk/skeleton/MyStore/km5l4

9 HPC-NNBOSL-UO-000-RET-000020 -UK EPR Hinkley Point Project: Identification and Review of the safety implications of a twin reactor design for Hinkley Point C, April 2012, Trim Ref. 2013/430795.

10 Hinkley Point C - Specification of the Fault and Protection Schedule - HPC-NNBOSL-XX-000-SPE-000012 Version 1.0, TRIM Ref 2013/464146.

11 Intervention Report ONR-NNB-IR-13-089, Level 4 Fault Studies Meeting, 19 November 2013, TRIM Ref. 2013/298479.

12 HPC PCSR2 - Heat Sink Summary Document, HPC-NNBOSL-U0-000-RET-000011 V2, January 2012, TRIM Ref 2013/18532.

13 Hinkley Point C Pumping Station Reliability Study – Evaluation of the LUHS Initiating Event Frequency, ECEF1103011, July 2012, TRIM Ref 2013/22230.

14 ONR Technical Assessment Guides:
http://www.hse.gov.uk/nuclear/operational/tech_asst_guides/index.htm

"ONR guidance on the demonstration of ALARP", NS-TAST-GD-005 Revision 5, ONR, May 2013.

"The Purpose, Scope, And Content Of Safety Cases", NS- NS-TAST-GD-051 Revision 3, ONR, July 2013.

15 Intervention Report ONR-CNRP-IR-13-038, Level 4 Fault Studies Meeting, 24 July 2013, TRIM Ref. 2013/298479.

16 Not used.

17 Hinkley Point C Pre-Construction Safety Report Response to the March 2011 Accident at Fukushima, HPC-NNBOSL-U0-000-RES-000050 Version 3.0 May 2013, TRIM Ref 2013/16198.

18 Not used.

19 CRF: Circulating Water System Part 2: System Operation, ETDOSF100224 A, (2010) TRIM Ref. 2013/393557.

20 NNB GenCo PCSR 2012 - Assessment Report – External Hazards, ONR-CNRP-AR-13-88, (2013) TRIM Ref. 2013/463256.

21 NNB GenCo PCSR 2012 - Assessment Report – C&I, ONR-CNRP-AR-13-103, (2013) TRIM Ref. 2013/4133.

22 NNB GenCo PCSR 2012 - Assessment Report – Internal Hazards ONR-CNRP-AR-13-88, (2013) TRIM Ref. 2014/6412.

23 PCSR – Sub-chapter 3.2 – Classification of structures, equipment and systems, UKEPR-0002-032 Issue 03, (2011) TRIM Ref. 2013/17155.

24 GDA Close-out for the EDF and AREVA UK EPR™ Reactor, GDA Issue GI-UKEPR-FS-03 Revision 2 Spent Fuel Pool Safety Case (2013) TRIM Ref. 2013/115947.

25 NNB GenCo PCSR 2012 - Assessment Report – PSA ONR-CNRP-AR-13-084 (2013) TRIM Ref. 2013/459661.

26 NNB GenCo PCSR 2012 - Assessment Report - Radioactive Waste & Discharges / Decommissioning, ONR-CNRP-AR-13-94 (2013) TRIM Ref. 2014/6705.

27 DWK Fuel Building Ventilation System, P2 System Operation 17DWK20 P2-SFLEFMF2006164D1 Issue D1 (2008) TRIM Ref. 2013/439039.

28 DVL Safeguards Building Non-Controlled Area Ventilation System, P2 - System Operation 17DVL20 EZL2007EN0077 F (2008) TRIM Ref. 2013/439028.

29 DWL Safeguards Building Non-Controlled Area Ventilation System P2 - System Operation, P2 - System Operation DWL SFLEZL030008 G (2008) TRIM Ref. 2013/439029.

30 DWN Nuclear Auxiliary Building Ventilation System P2 - System Operation DWN EZL2006EN0093 E (2008) TRIM Ref. 2013/439030.

31 EBA Containment Sweep Ventilation Plant System P2 System Operation P2-EYTS2007FR0131B1 (2009) TRIM Ref. 2013/439031.

32 EVR [CCVS] System Design Manual Part 2 System Operation, P2-EYTS2007FR0132 BPREL1, TRIM Ref. 2013/439033.

Table 1: Safety assessment principles considered during the assessment

SAP Number	SAP Title	Notes
Fault Analysis		
FA.1 to FA.3	General	The accident analyses performed by NNB GenCo will be assessed against the general fault analysis SAPs.
FA.4 to FA.9	Design basis	The design basis analyses performed by NNB GenCo are assessed against these SAPs. Examples of the faults to be considered are cooldown faults, heat-up faults, flow reduction faults, reactivity faults, increase in coolant faults, loss of coolant faults, ATWT faults, spent fuel pond faults, and shutdown faults.
FA.10 to FA.14	PSA	The thermal hydraulic analysis supporting the PSA success criteria will be assessed against the relevant parts of these SAPs.
FA.15 to FA.16	Severe accidents	The severe accident analysis performed by NNB GenCo in support of the twin EPR unit at HPC will be assessed against these SAPs.
FA.17 to FA.24	Validity of data and models	The validity of the computer codes and methods use to justify the fault performance of the twin EPR unit at HPC will be assessed against these SAPs.
Numerical Targets		
Target 4	Design basis fault sequences	The methodologies used by NNB GenCo to calculate the radiological consequences of design basis faults will be assess to allow a meaningful comparison against SAP Target 4.

Table 1: Safety assessment principles considered during the assessment

SAP Number	SAP Title	Notes
Engineering Principles		
EKP.3 and EKP.5	Key principles	The severe accident analysis will be assessed against the defence-in-depth SAP EK.3 and against the ALARP hierarchy identified in SAP EK.5.
EDR.1 to EDR.4	Design for reliability	These SAPs are reviewed as part of the design basis assessment under SAPs FA.4 to FA.9 discussed above. In particular, the safety case will be examined to determine redundancy and diversity of the protection provided to ensure that support systems adequately perform their safety function.
ESS.2, ESS.4, ESS.6 to ESS.9	Safety systems	The reactor protection system will be assessed against SAPs ESS.2, 4, 6, 7, 8 and 9.
ERC.1 to ERC.4	Reactor core	The nuclear design of the reactor core will be assessed against the relevant parts of these SAPs.

Issue No	Issue title	Issue	Level	Completion / review date
2039	Extending equipment qualification durations beyond 24 hours	Before first nuclear island concrete, the licensee shall consider the impact of extending equipment qualification durations beyond 24 hours for appropriate accident conditions.	4	Nuclear island safety related concrete
2040	LOCA from steam spaces in equipment qualification.	Before first nuclear island concrete, the licensee shall address the impact of small primary system LOCA from steam spaces in the relevant PCSR chapter on equipment qualification.	4	Nuclear island safety related concrete
2041	Sustained functioning of the reactor coolant pump static seals in the event of loss of the thermal barrier cooling.	Before first nuclear island concrete, the licensee shall provide further justification for measures to mitigate the loss of essential services water system. In particular, demonstration of sustained functioning of the reactor coolant pump static seals in the event of loss of the thermal barrier cooling.	4	Nuclear island safety related concrete
2042	Turbine design to prevent faults or to protect against them	Before first nuclear island concrete, the licensee shall provide further arguments and evidence to demonstrate that the turbine design is adequate to prevent faults or to protect against them. In particular, NNB GenCo should further develop the design of the turbine controller and demonstrate that the resulting limiting conditions of operation are tolerable in normal operation and anticipated faults.	4	Nuclear island safety related concrete

Issue No	Issue title	Issue	Level	Completion / review date
2043	Steam bypass requirements	The licensee shall, prior to the next revision of the HPC PCSR, identify a comprehensive set of cases where the steam bypass system either contributes to mitigation of radiological releases, or is required to act correctly to prevent faults. Then on this basis provide a suitable safety case to demonstrate that the design reduces risk to as low as reasonably practicable.	4	Nuclear island safety related concrete