Office for Nuclear Regulation

Civil Nuclear Reactor Build - Generic Design Assessment

Step 2 Assessment of the Fault Studies of Hitachi GE's UK Advanced Boiling Water Reactor (UK ABWR)

Assessment Report ONR-GDA-AR-14-005
Revision 0
28 August 2014

Published 08/14

EXECUTIVE SUMMARY

This report presents the results of my assessment of the preliminary fault studies safety case for Hitachi General Electric Nuclear Energy Ltd (Hitachi-GE) UK Advanced Boiling Water Reactor (UK ABWR), undertaken as part of Step 2 of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA).

The GDA process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments getting increasingly detailed as the project progresses. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including review of key nuclear safety, nuclear security and environmental safety claims with the aim of identifying any fundamental safety or security shortfalls that could prevent the proposed design from being acceptable in Great Britain. Therefore during GDA Step 2 my work has focused on the assessment of the key claims in the fault studies technical area to judge whether they are complete and reasonable in the light of our current understanding of reactor technology.

For fault studies, "safety claim" for Step 2 of GDA is interpreted as being:

- Design basis analysis (DBA) has shown that the engineering design of the UK ABWR is fault tolerant and has effective safety measures.
- Initiating faults included within the DBA are identified, with a commitment to extend the list of faults as appropriate to meet UK expectations.
- DBA fault sequences are established for the initiating faults within the design basis.
- DBA has shown that all considered fault sequences clearly meet identified and justified acceptance criteria, including ONR's design basis radiological consequence targets.

The standards I have used to judge the adequacy of the claims in the area of fault studies have been primarily ONR's Safety Assessment Principles (SAPs), in particular SAPs FA.1 to FA.9.

My GDA Step 2 assessment work has involved continuous engagement with the RP (Hitachi-GE) in the form of technical exchange workshops and progress meetings. In addition, my understanding of the ABWR technology, and, therefore, my assessment, has benefited from a visit to Kashiwazaki-Kariwa 6 & 7 nuclear power plants (undertaken just before the formal commencement of GDA Step 2).

My assessment has been based on the sections of the RP's Preliminary Safety Report (PSR) relevant to fault studies. In addition to making positive assertions against safety claims described above for design basis reactor faults, the PSR also states that future analysis will demonstrate the robustness of the UK ABWR design to very unlikely 'beyond design basis' faults and faults occurring in the spent fuel pool.

During my GDA Step 2 assessment of the UK ABWR aspects of the safety case related to fault studies I have identified the following areas of strength:

- The RP has demonstrated that its approach to analysing design basis faults is consistent with UK and international relevant good practice.
- The RP proposes to use established computer codes to model design basis fault sequences. The suitability of these codes has previously been accepted for licensing boiling water reactors by nuclear regulators in Japan and USA.

- Analysis of the design basis faults considered as part of licensing of Japanese ABWRs shows that acceptance criteria (which limit the radiological consequences resulting from a fault) are consistently met.
- The RP has set out proposals for summarising its safety case in a thorough and logical ‘fault schedule’.

During my GDA Step 2 assessment of the aspects of the UK ABWR safety case related to fault studies I have identified the following areas that require follow-up:

- The RP needs to extend the list of design basis events it considers in its safety case. It needs to include faults occurring during low power operation and shutdown, faults associated with essential services and support systems (for example electrical power supplies and cooling water systems), frequent events with a coincident common cause failure of a major safety system, and faults associated with fuel route operations. To ensure that these gaps in my expectations are addressed in a systematic manner and to provide additional guidance to the RP, I have raised five Regulatory Observations on these topics. The RP’s responses to these Regulatory Observations will be a major assessment task for ONR in the subsequent steps of GDA.
- The RP needs to submit to ONR UK ABWR specific analysis for the complete list of design basis events, using the codes and methods it has described in the PSR. This analysis, along with supporting information to demonstrate the validity of the methods employed, will be a major assessment task for ONR in the subsequent steps of GDA.
- The RP has proposed to complement the safety provisions of the ‘standard’ ABWR reactor design with a segregated back-up building. The design and the safety functions to be delivered by this building still need to be established. Consideration of the design and the safety claims on the back-up building will be a key assessment task for ONR in the subsequent steps of GDA.

In relation to my interactions with the RP’s subject matter experts in the fault studies topic area, I have found them to be very knowledgeable and effective. They have been responsive to my specific regulatory expectations in the fault studies topic area, notably with respect to my expectations for analysis and design provisions which represent relevant good practice in Great Britain.

Overall, I see no reason from my assessment of the preliminary fault studies safety case why the UK ABWR should not proceed to Step 3 of the GDA process.

LIST OF ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
ALARP	As Low As Reasonably Practicable
BMS	Business Management System
C&I	Control and Instrumentation
CCF	Common Cause Failure
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
DSA	Deterministic Safety Analysis
EA	Environment Agency
GDA	Generic Design Assessment
Hitachi-GE	Hitachi General Electric Nuclear Energy Ltd
IAEA	International Atomic Energy Agency
J-ABWR	Japanese ABWR
NRA	Nuclear Regulation Authority (of Japan)
NRC	Nuclear Regulatory Commission (US)
ONR	Office for Nuclear Regulation
PCSR	Pre-construction Safety Report
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
SAA	Severe Accident Analysis
SAP	Safety Assessment Principle(s)
SME	Subject Matter Expert
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Table(s)

1 INTRODUCTION

1.1 Background

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments getting increasingly detailed as the project progresses. Hitachi General Electric Nuclear Energy Ltd (Hitachi-GE) is the RP for the GDA of the UK Advanced Boiling Water Reactor (UK ABWR).

2. During Step 1 of GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams and made arrangements for the GDA of its ABWR design. Also, during Step 1, the RP prepared submissions to be evaluated by ONR and the Environment Agency (EA) during Step 2.

3. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including review of key nuclear safety, nuclear security and environmental safety claims with the aim of identifying any fundamental safety or security shortfalls that could prevent the proposed design from being acceptable in Great Britain.

4. To facilitate Step 2 of GDA, the RP submitted its UK ABWR Preliminary Safety Report (PSR) to ONR. This report presents the results of my assessment of the fault studies aspects of this PSR (principally Refs. 1, 2, 3 and 4).

1.2 Methodology

5. My assessment has been undertaken in accordance with the requirements of the ONR How2 Business Management System (BMS) procedure PI/FWD (Ref. 5). The ONR Safety Assessment Principles (SAPs) (Ref. 6), together with supporting Technical Assessment Guides (TAG) (Ref. 7) have been used as the basis for this assessment.

6. My assessment has followed my GDA Step 2 Assessment Plan for Fault Studies (Ref. 8) prepared in December 2013 (and revised in April 2014) and shared with Hitachi-GE to maximise openness and transparency. All the key assessment tasks identified in Ref. 8 have been undertaken, although the timing of some of the interactions with Hitachi-GE has not been in accordance with the dates originally envisaged in the plan.

2 ASSESSMENT STRATEGY

7. This section presents my strategy for the GDA Step 2 assessment of the fault studies of the UK ABWR. It also includes the scope of the assessment and the standards and criteria that I have applied.

2.1 Scope of the Step 2 Fault Studies Assessment

8. ONR's SAPs (Ref. 6) (see Section 2.2) require the risks arising from nuclear facilities during fault conditions to be assessed using three techniques: design basis analysis (DBA), probabilistic safety analysis (PSA), and severe accident analysis (SAA). This GDA Step 2 fault studies assessment for the UK ABWR focuses on DBA, with the adequacy of the RP's PSA and SAA assessed elsewhere (Ref. 9).

9. The purpose of DBA is to provide a robust demonstration of the fault tolerance of a nuclear facility and the effectiveness of its safety measures. Its principal aims are to guide the engineering requirements of the design, including modifications, and to determine limits to safe operation, so that safety functions can be delivered reliably during all modes of operation and under reasonably foreseeable faults. In DBA, any uncertainties in the fault progression and consequence analyses are addressed by the use of appropriate conservatism.

10. An integral part of DBA for a reactor is undertaking of transient analysis of fault sequences using computer models of the reactor design in question. This is a major component of the work required to demonstrate the adequacy of the design and the suitability and sufficiency of the safety measures. The results of these computer models (usually predictions of physical parameters e.g. temperatures, masses of steam/water losses, radioactive releases, etc.) are assessed against deterministic targets. This type of modelling of fault sequences, which includes declared conservatisms and comparisons against defined targets, is often called deterministic safety analysis (DSA).

11. The objective of my GDA Step 2 fault studies assessment for the UK ABWR was to review and judge whether the claims made by the RP related to DBA that underpin the safety aspects of the UK ABWR are complete and reasonable in the light of our current understanding of reactor technology.

12. For fault studies, "safety claim" for Step 2 of GDA is interpreted as being:

- DBA has shown that the engineering design of the UK ABWR is fault tolerant and has effective safety measures.
- Initiating faults included within the DBA are identified, with a commitment to extend the list of faults as appropriate to meet UK requirements.
- DBA fault sequences are established for the initiating faults within the design basis.
- DBA has shown that all considered fault sequences clearly meet identified and justified acceptance criteria, including ONR's design basis radiological consequence targets.

13. My fault studies assessment of the DBA safety claims has not been restricted to faults associated with the reactor operating at full power. The scope of this assessment includes all operating modes and operations of the reactor (including low power and shutdown operations) and fuel route operations (including the safe storage of spent fuel in the spent fuel pool, refuelling operations, the import and export of fuel into the spent fuel pool). The RP's DBA safety case for the UK ABWR will eventually need to address faults across the whole facility which have the potential for radiological consequences (for example, the radiological waste treatment and storage systems) however this

assessment of the high level claims has been targeted at the larger hazards contained within the reactor and the fuel route systems.

14. SAP FA.5 (Ref. 6) clearly defines the criteria for faults to be considered within the design basis. It is not expected that the onerous requirements of DBA are applied to faults with a very low initiating event frequency (less than 1 $x10^{-5}$ per year). However, it is considered relevant good practice, both in the UK and internationally, to consider 'beyond design basis' faults on a best-estimate basis (i.e. excluding the conservatisms normally included with the DBA) and demonstrate the effectiveness of the available safety measures for these very unlikely events. This assessment has therefore looked at how the RP identifies beyond design basis events and how it intends to analyse them.

15. In addition to assessing the adequacy of the submissions provided by the RP specifically for GDA Step 2, I have also evaluated whether the claims related to fault studies are supported by a body of technical documentation sufficient (or a programme of work to develop such documentation) to allow me to proceed with GDA work beyond Step 2. As part of Step 2, I have not undertaken a detailed assessment of any supporting transient analysis (or DSA) for either the design basis or beyond design basis faults. However, gaining an appreciation of the availability and documentation of this analysis has been vital to reaching a judgement on the ability to proceed to Step 3.

16. Finally, during Step 2, I have undertaken preparatory work for my Step 3 assessment, notably:

- Developed a strategy for using technical support contractors for DBA on the UK ABWR design.
- Considered how ONR can best utilise the fault studies assessment work that has already been undertaken on the ABWR design by organisations such as the US Nuclear Regulatory Commission (NRC).
- Raised five Regulatory Observations to be addressed by the RP during Step 3 in areas where additional analyses[1] of the UK ABWR are necessary to demonstrate the robustness of the design.

2.2 Standards and Criteria

17. The goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety, security and environmental case. For this purpose, within ONR, assessment is undertaken in line with the requirements of the How2 BMS document PI/FWD (Ref. 5). Appendix 1 of Ref. 5 sets down the process of assessment within ONR; Appendix 2 explains the process associated with sampling of safety case documentation.

18. In addition, the SAPs (Ref. 6) constitute the regulatory principles against which duty holders' safety cases are judged, and, therefore, they are the basis for ONR's nuclear safety assessment and therefore have been used for GDA Step 2 assessment of the UK ABWR. The SAPs 2006 Edition (Revision 1 January 2008) were benchmarked against the International Atomic Energy Agency (IAEA) standards (as they existed in 2004). The SAPs are currently being reviewed but no significant changes are anticipated which could alter this Step 2 assessment of the fault studies claims made in the UK ABWR PSR.

19. Furthermore, ONR is a member of the Western European Regulators Nuclear Association (WENRA). WENRA have developed reference levels, which represent good practices for existing nuclear power plants, and safety objectives for new reactors.

---

[1] *Additional to that provided in the Step 2 submission or indicated by Hitachi-GE as to be provided at the start of Step 3.*

20. ONR's TAGs provide further guidance on how the relevant SAPs, IAEA standards and WENRA reference levels should be applied in ONR assessments.

21. How these different types of guidance have been applied in this Step 2 fault studies assessment of the safety claims for the UK ABWR is summarised in the following sub-sections.

2.2.1 Safety Assessment Principles

22. The key SAPs (Ref. 6) applied within my fault studies assessment are:

- Fault Analysis SAPs FA.1 to FA.9;
- Severe Accidents SAPs FA.15 and FA.16;
- Engineering SAPs EKP.2 to EKP.5, ECS.1, ECS.2, EDR.1 to EDR.4, ESS.2, ESS.4, ESS.6 to ESS.9, ESS.11, ERC.1 to ERC.3, EHT.1 to EHT.4;
- Computer codes and calculation methods SAPs FA.17 to FA.24; and
- Numerical Target for DBA consequences T4.

23. Details have how these SAPs have been applied are given in Section 4 and in Table 1.

2.2.2 Technical Assessment Guides

24. The following TAGs are directly relevant to the assessment of fault sequences on nuclear reactors:

- NS-TAST-GD-034: Transient Analysis for DBAs in Nuclear Reactors, Revision 2, June 2013 (Ref. 7).
- NS-TAST-GD-042: Validation of Computer Codes and Calculation Methods, Revision 2, June 2013 (Ref. 7).

25. My detailed assessments of the transient analyses undertaken (or planned) by the RP for the UK ABWR will be Step 3 and 4 activities. My Step 2 assessment of the fault studies safety claims has largely remained at the higher level set out in the SAPs identified above. Therefore, these TAGs have not been used during Step 2 but they will be used extensively in future Steps.

2.2.3 International Standards and Guidance

26. The following IAEA standards and WENRA guidance have relevance for any assessment of fault studies claims made on a boiling water reactor:

- Relevant IAEA standards (Ref. 10) are:
  - International Atomic Energy Agency (IAEA) Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements (SSR) 2/1, IAEA 2012; and
  - International Atomic Energy Agency (IAEA) Safety Standards Series – General Safety Requirements (GSR) Part 4: Safety Assessment for Facilities and Activities IAEA 2007.
- Relevant WENRA references (Ref. 11) are:
  - Reactor Safety Reference Levels (January 2008).

27. These standards set expectations for the performance of DSA to demonstrate the robustness of reactor designs which are directly applicable to a fault studies assessment. My Step 2 fault studies assessment has principally been undertaken against the SAPs

but Table 1 demonstrates how these ONR expectations are consistent with the international standards.

2.3 Use of Technical Support Contractors

28. During Step 2 I have developed specifications for three packages of work to be undertaken by technical support contractors and started to develop a strategy for Steps 3 and 4 of GDA to perform independent confirmatory analysis of a carefully selected sample of fault sequences. However, none of the outputs of the three specified work packages provide an input to the conclusions of my Step 2 fault studies assessment.

- Package 1 is for the development of a computer model of the thermal hydraulic and system response of the UK ABWR in fault conditions, independent of the models used by the RP. Work on this model has started in Step 2 so that it will be available for use during Steps 3 and 4 of GDA.
- Package 2 is an independent expert review of the completeness of the list of design basis initiating events identified by the RP for the UK ABWR. This work has been specified in Step 2 so that it can commence promptly at the start of Step 3. It will use the Pre-Construction Safety Report (PCSR) to be delivered by the RP at the start of the Step 3 as its key reference.
- Package 3 is a review of the publically available documentation of the US NRC certification of the US ABWR design developed by GE Nuclear Energy. It is anticipated that the US NRC assessment of the US ABWR will contain many insights and assurances which will be of value to the ONR assessment of the UK ABWR. However, it is over 20 years old and was not produced to support the ONR assessment of the UK ABWR at the present day. Although this review will be complete by the end of Step 2, it is being undertaken to inform the Step 3 and 4 application of the (Package 1) UK ABWR computer model.

29. I have also held discussions with the RP to explore the practicalities of obtaining the necessary UK ABWR design information to facilitate independent analyses. The availability of such information is fundamental to successful delivery of the technical support contractor strategy.

30. More details of my strategy for using technical support contractors will be set out in my fault studies Assessment Plan for Step 3 of GDA.

2.4 Integration with Other Assessment Topics

31. Early in GDA I recognised that there would be a need to consult with other assessors (including EA's assessors) as part of the fault studies assessment process. Similarly, other assessors will seek input from my assessment of the fault studies for the UK ABWR. These interactions are important to ensure the prevention of assessment gaps and duplications and therefore, they are key to the success of the project. Thus, I made every effort to identify, up front, as many potential interactions as possible between the fault studies and other technical areas, with the understanding that this position would evolve throughout the UK ABWR GDA.

32. Also, it should be noted that the interactions between the fault studies and some technical areas need to be formalised since aspects of the assessment in those areas constitute formal inputs to the fault studies assessment, and vice versa. These are:

- The assessment of the RP's UK ABWR SAA has been led by the PSA topic area. However, I have been actively involved in this assessment of the claims and planning for assessment in future Steps. Fault studies specialists will take the lead on the more detailed review of the computer modelling of severe accident phenomena and the engineered systems designed to mitigate the consequences in the event of common cause failure of design basis systems.

- There are direct interactions and interdependencies with ONR's fuel and core technical assessment. The RP demonstrates the robustness of the UK ABWR design to fault conditions by showing that acceptance criteria on the performance of fuel are met. These acceptance criteria are being considered by ONR's fuel and core assessor. In addition, the fuel and core technical assessment considers the core loadings, fuel cycles, and fuel performance correlations assumed in the fault studies DSA.
- The fault studies and PSA specialists have worked together to gain confidence in the RP's list of initiating events, with additional support provided by control and instrumentation (C&I) and electrical engineering inspectors.

33. In addition to the above, during GDA Step 2 there have been interactions between fault studies and the rest of the technical areas, i.e. engineering disciplines and human factors on safety claims made on structures, systems and components (SSCs). Although these interactions, which are expected to continue thorough GDA, are mostly of an informal nature, they are essential to ensure consistency across the technical assessment areas.

3 REQUESTING PARTY'S SAFETY CASE

34. The scope of an assessment of the fault conditions that can occur on a nuclear power plant is potentially very wide ranging and extensive. For Step 2, I have focussed my assessment on what I judge to be the most significant areas of the (preliminary) safety case:

- reactor faults;
- spent fuel pool and fuel route faults;
- analysis codes;
- categorisation and classification of SSCs;
- the fault schedule;
- UK ABWR balance of plant;
- beyond design basis faults; and
- considerations in the light of the Fukushima accident.

35. The primary reference supplied by the RP for ONR's Step 2 assessment of the UK ABWR is the PSR. The main section within the PSR for most of the areas above is:

- Hitachi-GE UK ABWR (Generic Design Assessment): Fault studies to discuss deterministic analysis, PSA and fault schedule development (Ref. 1).

36. Ref.1 gives information on the strategy to be followed for developing a UK ABWR specific DBA safety case. To better illustrate this strategy, the methodologies and results from safety analyses of the similar (but not identical) Japanese ABWR (J-ABWR) built and operated in Japan have been provided by the RP to supplement the UK ABWR PSR (Ref. 12). However, DBA (including transient analysis) for the UK ABWR will not be provided until the start of Step 3 via the PCSR.

37. The preliminary safety case for the spent fuel pool and the RP's proposals for a SSC categorisation and classification scheme are reported elsewhere in the PSR:

- Hitachi-GE UK ABWR (Generic Design Assessment): Initial Safety Case report on Spent fuel pool (Ref. 2);
- Hitachi-GE UK ABWR (Generic Design Assessment): Categorisation and Classification of Systems, Structures and Components (Ref. 4).

38. In addition to these references, useful background information (and indeed some fault studies related claims) are set out in:

- Hitachi-GE ABWR General Description (Ref. 3).

39. A summary of Hitachi-GE's preliminary safety case in the area of fault studies, as set out in references identified above, is given in the following sub-sections.

3.1 Reactor Faults

40. In its Step 2 submissions to ONR, the RP has stated that a systematic approach to plant safety has been applied to the UK ABWR for (reactor) fault assessment (Ref. 1). DSAs (i.e. the modelling of reactor fault transients with some clearly declared assumptions and uncertainties included) have been undertaken on the similar J-ABWR which have shown that the consequences of the considered fault sequences meet the acceptance criteria published by the Nuclear Safety Commission of Japan (Ref. 12). The PSR submission (Ref. 1) states that new analyses will be undertaken for the UK ABWR for all operating modes and configurations (including partial power and shutdown states) and the results compared against new acceptance criteria identified for the UK. However, examples of

existing J-ABWR analyses have been supplied to ONR to provide confidence that the analysis methods followed by the RP (and acceptance criteria applied) will be consistent with UK and international relevant good practice.

41. For Japanese plants, the RP splits its identified reactor faults into anticipated operational occurrences and design basis accidents. This is consistent with IAEA terminology and is similar to the UK practice of categorising faults within the design basis as frequent or infrequent faults. The submission also provides a comparison of the initiating events considered by the RP in accordance with normal Japanese practice and those suggested by the IAEA safety guide NS-G-1.2 (now superseded by Ref. 10 but it is still considered by the RP to be a suitable benchmark). The RP states that its practice is almost identical to that recommended by the IAEA (Ref. 1). However, it has committed to undertake a failure modes and effects analysis to identify a definitive list of initiating events for the UK ABWR.

3.2 Spent Fuel Pool and Fuel Route Faults

42. The RP's submission (Ref. 2) identifies some indicative design basis faults for the spent fuel pool and gives a commitment to provide a fuller list with a more comprehensive safety case in the PCSR to be delivered for Step 3. However, the submission introduces some key claims for the spent fuel pool:

- The fuel storage system and the fuel handling system are designed to prevent criticality by a geometrically safe arrangement or other appropriate means. The design is such that sub-criticality is ensured under all envisaged conditions even when the fuel assemblies are stored at the maximum storage capacity.
- The fuel pond cooling system is designed to maintain the spent fuel pool water temperature below a maximum allowable temperature, even when an active component within it, or related systems, fails.
- If the fuel pond cooling system fails, there are sufficient time margins before spent fuel pool water boils for alternative means of cooling or water injection to be initiated, such that fuel is not uncovered.
- If boiling does occur, the amount of radioactivity transferred to the environment will be small, even without credit being taken for the filtered ventilation system.
- There are multiple means of providing alternative cooling.

3.3 Analysis Codes

43. In its Step 2 submission to ONR (Ref. 1), the RP has provided a list of the computer codes used for DSA of the J-ABWR and stated what techniques it intends to employ to analyse the safety performance of the UK ABWR. For a significant portion of the identified reactor faults, the RP intends to utilise the same analysis codes as it used on the J-ABWR. However, in some areas it has stated the intention to use different codes.

44. The Step 2 PSR submission provides basic descriptions of these analysis codes. It states that majority of the codes are proprietary to the RP's American sister company (GE-Hitachi), the implication being that they have been designed for modelling ABWR faults. The other codes, although not developed specifically for the ABWR, are in general use for in BWR analysis by a range of organisations.

45. The RP has stated that more detailed descriptions of the computer codes planned to be used on the safety justification of the UK ABWR will be provided in the Step 3 PCSR. These more detailed descriptions will include the validation evidence for the analysis codes.

3.4 Classification and Categorisation of Systems, Structures and Components

46. The RP's submission (Ref. 4) proposes a three-tier approach (A to C) to the categorisation of safety functions, informed by SAP ECS.1. This has been allied with a three-tier approach (1 to 3) to classifying the SSCs which are required to deliver the identified safety functions, informed by SAP ECS.2.

47. Examples of safety functions and SSCs delivering them have been provided in the submission. A commitment is given to confirm the classifications applied to SSCs through the development of fault studies work during GDA.

3.5 Fault Schedule

48. The RP has prepared a fault schedule which summaries the initiating events identified for the UK ABWR and the protection systems and/or operator actions provided to safely manage such events should they occur. A single page of the fault schedule has been included within the Step 2 submission (Ref. 1) as an illustration of the format and approach to be adopted.

49. The RP has stated that the fault schedule will be re-assessed as the detail of the UK ABWR is determined. However, a comprehensive fault schedule will be included within the Step 3 PCSR. They have also stated that the fault schedule will consider faults occurring in all operating modes and configurations, as well as the spent fuel pool, radiological waste handling/storage facilities, and faults initiated as a result of internal and external hazards.

3.6 UK ABWR Balance of Plant

50. A significant feature of the UK ABWR design which is different from all the currently operating reactors in the UK is that it has a direct steam cycle system i.e. the water fed to the reactor is turned to steam and directed to the turbines without an intermediate secondary circuit.

51. During normal (power generating) operation, the generated steam contains radioactive Nitrogen-16 with a small amount of noble gas and iodine from any leaking fuel elements. As a result, the balance of plant (i.e. the steam lines from the reactor, the turbo-generator set, condensers and feedwater injection systems) has specific design features to deal with this hazard, notably additional shielding and an off-gas treatment system.

52. Faults initiating within the balance of plant have the potential to cause transients in the reactor core, while faults initiating in the reactor have the potential to cause significantly higher levels of radioactivity to be present in the balance of plant. As a result, a key safety feature of UK ABWR design is provision of fast acting valves which isolate the primary containment vessel (which contains the reactor) from the balance of plant.

53. The RP's preliminary safety case addresses such faults initiating in or affecting the balance of plant through its analysis of reactor faults (Ref. 1). It has also applied the approach to categorisation and classification to the balance of plant (Ref 4) and it has stated such faults will appear on the fault schedule.

3.7 Beyond Design Basis Faults

54. The RP's PSR submission (Ref. 1) identifies the requirement for beyond design basis faults to be considered within the UK ABWR safety case, and provides a definition for such events:

- the initiating event frequency is between 10^{-5} and 10^{-7} per year;
- the potential consequences are greater than 100 mSv (off-site) or 500 mSv (on-site);
- the core is significantly damaged by multi-systems failures cause by common cause failure or functional dependency; and
- the time margin to implement countermeasures for core damage prevention is small.

55. A preliminary list of potential fault sequence groups are identified for future analysis using realistic/best-estimate assumptions. However, no UK ABWR specific analysis of beyond design basis faults is provided within the PSR (Ref. 1).

3.8 Considerations in the Light of the Fukushima accident

56. Following the events at Fukushima in March 2011, the worldwide nuclear industry has put in place measures to ensure that the risks from nuclear facilities under extreme conditions are further reduced.

57. One of the key lessons from Fukushima is the importance of having a thorough and correctly defined design basis safety case. However, it is also now considered relevant good practice to consider the implications of design basis measures failing or very unlikely events/combinations of events occurring. While the fault studies sections of the PSR submission (Ref. 1) do not explicitly discuss learning from Fukushima, they do state that design basis faults, beyond design basis faults and severe accidents will be identified and analysed in future PCSR submissions.

58. ONR is aware of a number of physical modifications being made to the J-ABWR plants built in Japan. The RP has stated to ONR that similar capabilities will be provided on the UK ABWR, notably through the provision of a back-up building. This building will be segregated from the main reactor building and contain its own independent and diverse electrical and water supplies that can be used to deliver essential safety functions to the reactor and spent fuel pool following an extreme event.

59. No claims on the function and capability of the proposed back-up building are made in the fault studies sections of the PSR submission (Refs. 1 & 2). However, it is expected such claims will be set out in future PCSR submissions. It is noted that the electrical engineering sections of the PSR (Ref. 13) do start to introduce some claims on the back-up building but that is beyond the scope of the Step 2 fault studies assessment reported here.

4 ONR ASSESSMENT

60. Details of my GDA Step 2 fault studies assessment of the UK ABWR preliminary safety case are presented in the sub-sections below. Each sub-section summarises the assessment done in regard to different aspects of the fault studies submission, details any strengths identified in the design or safety case, as well as the items that require follow-up and the conclusions reached.

61. The assessment has followed the strategy described in Section 2 of this report. It has centred upon a review of the formal PSR submission supplied by the RP for Step 2. It has also involved continuous engagement with the RP's fault studies subject matter experts (SME), most significantly through two week-long technical exchange workshops (one in the UK and one in Japan) and a number of routine progress meetings held over video conference links. At these workshops and meetings, the RP has supplemented the PSR submission with presentations, which have provided additional details to the PSR and also previewed information to be supplied later in Step 3 as part of the PCSR.

62. Ahead of commencing my Step 2 assessment, I increased my familiarity with ABWR technology by visiting to Kashiwazaki-Kariwa 6 & 7 nuclear power plants.

63. During my GDA Step 2 assessment, the interactions with the RP's SMEs and my review of the PSR submission prompted me to raise six Regulatory Queries (Ref. 14) to provide further clarity on the background and claims specified for the UK ABWR fault studies area. The responses to these queries on matters of fact have aided my understanding and provided some additional context but have not directly affected my assessment of the high level claims made in the PSR. They have resulted in a number of 'lines of enquiry' which I will pursue further in Steps 3 and 4, notably on the design and required functionality of the residual heat removal system.

4.1 Reactor Faults

4.1.1 Assessment

64. The majority of fault studies information provided in the PSR submission (Ref. 1) is associated with reactor faults. Similarly, the majority of my fault studies assessment effort during Step 2 has focussed on reactor faults.

65. As I stated in my Step 2 Assessment Plan (Ref. 8), my major assessment objective for Step 2 was to review and gain confidence in the completeness of the list of UK ABWR design basis faults identified and considered by the RP, in accordance with SAP FA.5. In addition to considering the formally submitted documentation, I have also worked towards this objective by including the issue of the identification of initiating faults on the agendas of the two fault studies technical exchange workshops held during Step 2.

66. I have looked at the supplied information on the methodologies, analyses and results performed for fault sequences presented in the PSR. However, the detailed examination of these aspects will not be undertaken till Steps 3 and 4 when UK ABWR specific analyses are available (the PSR only supplies a selection of J-ABWR analyses provided for information).

4.1.2 Strengths

67. The PSR gives evidence that the RP has undertaken DBA on the reference plant (J-ABWR) and provides a commitment to develop this further for the UK ABWR. Although there are some differences between the UK ABWR and the J-ABWR, what is presented in the PSR gives me confidence that the new DBA undertaken specifically for the UK ABWR will be able to demonstrate that the reactor is robust against a wide range of faults.

68. The RP has used IAEA terminology and definitions to group design basis faults (anticipated operational occurrences and design basis accidents) and compared the results of transient analysis against (Japanese) acceptance criteria. While these groupings do not exactly match the usual frequency driven grouping approach used in the UK (i.e. frequent and infrequent faults), the approach is broadly similar. Also, while the applied acceptance criteria will need to be justified, they appear reasonable.

69. The PSR does not provide details on the assumptions to be made in the proposed UK ABWR specific transient analysis of design basis faults. However, the examples given of Japanese transient analysis appear to be consistent with the requirements of SAP FA.6; for the fault sequences assessed, consequential failures are considered (for example, the loss of the grid connection following a fault induced reactor trip) and single failures in safety equipment are assumed. The J-ABWR transient analysis shows that the appropriate acceptance criteria are met. Notably for the major faults of a loss of coolant accident and a main steam line break, the analyses suggest that the correct performance of the engineered safety systems will mean there will be no consequential fuel failures. It is therefore my expectation that future UK ABWR specific analyses will be able to successfully demonstrate similar results.

4.1.3 Items that Require Follow-up

70. The list of design basis faults provided in the PSR (based on the RP's normal practice in Japan) is broadly consistent with my expectations and the RP has presented a positive comparison with IAEA guidance. However, it is limited to single events on front line systems as initiators and to faults occurring from full power operations.

71. SAP FA.6 requires the analysis of fault sequences to consider the worst normally permitted configuration of equipment outages and the most onerous permitted operating states of the plant. Whilst it is often the case that faults from full power are the most limiting, equipment availabilities and safety system responses can change during low power and refuelling operations. There are welcomed commitments given in the PSR (Ref. 1) to undertake new analysis for the UK ABWR for all operating modes and configurations, however, it gives no previews of what the safety claims in the partial power or shutdown safety cases will be.

72. SAP EDR.2 requires that appropriate use should be made of diversity in the designs of SSCs important to safety. As a result, for frequent faults (initiating event frequency greater than 10^{-3} per year), it is relevant good practice in the UK to consider the failure of a major safety system (for example, a failure to actuate an emergency core cooling system) and show that an alternative system(s) can ensure appropriate acceptance criteria are met. This demonstration of diversity is not provided in the PSR submission but a commitment is given to provide it going forward. This will need to be monitored. One notable implication of this UK requirement is that frequent initiating events combined with an assumed failure of the reactor trip system (often called an 'anticipated transient without scram' fault) will need to be considered within the design basis.

73. SAP EDR.3 states that common cause failure (CCF) should be addressed explicitly. Again, by limiting itself to single event initiators, the RP has excluded a number of potentially complex or challenging events, which I would expect to see assessed within the design basis.

74. To ensure that these gaps in my expectations are addressed in a systematic manner and to provide additional guidance to the RP, I have raised four Regulatory Observations (Ref 15):

- RO-ABWR-0007: The RP is required to analyse spurious failures in the complex control and instrumentation systems which are used to both operate the UK

ABWR and protect it from fault conditions. Some failures in control and instrumentation systems may have benign consequences or result in a fault already considered by Hitachi-GE. However, the analysis of some faults may identify the need for new (and diverse) means of protection if the functionality of the control and instrumentation system with the initiating problem is compromised.

- RO-ABWR-0008: The RP is required to undertake design basis analysis of a range of major CCFs of key systems involved in the distribution of power within the generic UK ABWR site (i.e. switchboards and static conversion equipment).
- RO-ABWR-0009: The RP is required to review the resilience of the UK ABWR to loss of off-site power events (of different durations) and to loss of off-site power events coincident with CCFs of installed onsite safety classified electrical systems.
- RO-ABWR-0010: The RP is required to demonstrate that it has comprehensive design basis analyses of all initiating events occurring in UK ABWR support systems such as heating, ventilation and air conditioning (HVAC) systems, cooling chain systems and compressed gas systems. Partial failure of a system (e.g. failure of a single component or train) and total failure of a system due to a CCF are to be considered.

75. The RP is producing resolution plans for these Regulatory Observations requiring additional submissions to be supplied to ONR during Step 3. I will assess work undertaken by the RP in response to these Regulatory Observations during Steps 3 and 4 of GDA.

4.1.4 Conclusions

76. I am broadly satisfied with the RP's approach to reactor fault studies and the claims it has put forward in the PSR (based upon their existing analyses of similar faults on the J-ABWR). However, the RP still needs to deliver the considerable amount of additional UK ABWR specific analyses that it has identified, and it will be a significant part of my future assessment to review the RP's supporting arguments and evidence which underpin the claims it has already made.

77. The RP also needs to address the four Regulatory Observations summarised above in order to demonstrate that the engineering design of the UK ABWR is fault tolerant and has effective safety measures for all design basis events. Thorough and systematic responses to these Regulatory Observations during Step 3 have the potential to address the initial gaps I have observed in Hitachi-GE's initial submissions.

4.2 Spent Fuel Pool and Fuel Route Faults

4.2.1 Assessment

78. I have assessed the RP's PSR submission (Ref. 2) for the spent fuel pool and discussed the proposed safety case for this aspect of the UK ABWR with the RP at the two fault studies technical exchange workshops. I have also reviewed the general aspects of the design of the spent fuel pool provided in the ABWR General Description document (Ref. 3).

4.2.2 Strengths

79. The spent fuel pool PSR submission demonstrates that the RP appreciates that a systematic design basis safety case needs to be produced for this aspect of the facility. The RP has provided sensible examples of the types of initiating events that need to be considered and what safety functions will need to be delivered.

80. One aspect of the spent fuel pool design which is noted and welcomed is the spent fuel pool cooling and cleanup system. This system extracts water from the spent fuel pool via 'skimmer weirs" rather than from the main spent fuel pool directly. This engineering feature is likely to reduce the potential for a pipe break that could cause a catastrophic loss of pool water and therefore reduce the potential for a fault that could result in the fuel within the pool becoming uncovered.

4.2.3 Items that Require Follow-up

81. The spent fuel pool PSR submission (Ref. 2) is not a complete safety case; instead it is a document which sets out what a future safety case could contain. Every aspect of the safety case needs to be provided, starting with a definition of its scope. It needs to be clear which systems and facilities are to be considered, notably extending beyond the spent fuel pool to include refuelling operations and fuel import/export arrangements. Initiating events and fault sequences need to be systematically identified, protective safety systems need to be specified and appropriately designated a safety classification, and suitable acceptance criteria need to be established against which the performance of the safety systems can be judged.

82. Given the lack of maturity of the PSR submission and the size of the task to develop it to a complete safety case, I have raised a Regulatory Observation (RO-ABWR-0011, see Ref. 15) formally requesting the RP to address my expectations for a fuel route safety case (including the spent fuel pool).

83. Effectively removing the decay heat from the fuel is an important safety function in both normal operations and fault conditions, whether that function is being provided to fuel in the reactor or in the spent fuel pool. From the information that has been provided in the PSR submission (Ref. 2 & 3), it appears that the levels of engineered provision of spent fuel pool cooling falls short of relevant UK good practice in terms of redundancy and diversity. There are multiple means of delivering cooling to the spent fuel pool but many of these share the same piping intakes/returns and therefore are not independent of each other. This aspect of the design will need to be considered further during Step 3, informed by the safety claims identified in the RP's response to my Regulatory Observation RO-ABWR-0011.

84. Maintaining the fuel in the spent fuel pool in a sub-critical state is also a vital safety function. The RP has made a significant claim that the fuel storage system and fuel handling system will keep the fuel in a geometrically safe arrangement during both normal operations and fault conditions (see Section 3.2). This claim is welcomed but I will need to examine the supporting analysis during Steps 3 and 4.

4.2.4 Conclusions

85. The RP has provided a clear commitment to deliver a design basis safety case for the UK ABWR fuel route (including the spent fuel pool). To achieve this, it needs to address my Regulatory Observation (RO-ABWR-0011). My detailed assessment of the adequacy of the design and safety case for the fuel route will commence upon receipt of the deliverables from RO-ABWR-0011. I anticipate that the level of redundancy and diversity within the engineering design of the spent fuel pool cooling system will be an area of close scrutiny.

4.3 Analysis Codes

4.3.1 Assessment

86. The Step 2 PSR submission (Ref. 1) only provides limited amounts of information on the analysis codes the RP intends to use to assess UK ABWR fault sequences. The analysis codes are primarily in-house codes (i.e. Hitachi-GE or GE-Hitachi codes). Many of these

87. Some examples of the application of these codes were provided at the second fault studies technical exchange workshop held in Step 2. However, while this information complemented the formal PSR submission and did not reveal any major concerns, I will not commence my detailed assessment of the analysis codes until Step 3.

4.3.2 Strengths

88. The RP has clearly stated within its PSR submission (Ref. 1) which analysis codes it intends to employ during GDA of the UK ABWR. A basic description of each code has been provided in the PSR submission (Ref. 1) along with some sample analyses of faults using Japanese practises (i.e. J-ABWR analysis). This level of detail is sufficient for my Step 2 assessment.

4.3.3 Items that Require Follow-up

89. The detailed assessment of the analysis codes used by the RP to model UK ABWR fault sequences will be a major objective of my Steps 3 and 4 work scope. It appears that many of the existing analysis methodologies were developed and received regulatory approval more than 20 years ago. A lot more detailed information will be required on their verification and validation, their heritage, maintenance, documentation and any formal approval of their application received from other regulators so that I can assess their compliance with the expectations set out in SAPs FA.17 to FA.24. Crucially, the RP will need to demonstrate why the available evidence is applicable to the UK ABWR, which is expected to have a number of design differences to the original reference Japanese plant. The RP will also need to demonstrate that its proposed codes and methodologies represent relevant good practice given that different and more advanced computer codes may offer greater modelling capability and sophistication.

90. In addition to pursuing in the work described in the above paragraph in Steps 3 and 4, I intend to undertake some independent confirmatory analysis of a carefully selected sample of UK ABWR fault sequences. For this, I will commission a technical support contractor to use a state-of-the-art systems code to perform UK ABWR fault analysis (see Section 2.3). The comparisons of this independent work against the conclusions reached by the RP using its own codes will inform the level of confidence I attribute to Hitachi-GE's codes and methods.

4.3.4 Conclusions

91. It was not my intent to perform detailed assessment of fault studies analysis codes as part of my Step 2 assessment. At this point of my assessment, I have confidence that the codes appear to be appropriate for the analysis of the UK ABWR (based on their use and acceptance internationally).

92. Detailed assessment of these analysis methods will be undertaken by ONR, supported by technical support contractors, within Steps 3 and 4 of GDA.

4.4 Categorisation and Classification of Systems, Structures and Components

4.4.1 Assessment

93. The RP's PSR submission (Ref. 4) provides definitions for its three tier categorisation and classification scheme, and gives some examples of how these definitions are likely to be applied to safety functions and the SSCs delivering those safety functions.

94. During Step 2, I have reviewed these definitions and examples, as well as the means by which the RP plan to capture these allocations in the fault schedule. However, as the RP has not yet supplied a full list of initiating events and declared which SSCs are being formally claimed to protect against these events (either as design basis protective measures or defence-in-depth safety systems), it has not been possible to assess in detail the application of the proposed categorisation and classification scheme.

4.4.2 Strengths

95. The proposed categorisation and classification process is consistent with the suggested schemes set out in SAPs ECS.1 and ECS.2. The RP has also explicitly discussed how the scheme will be applied not just to design basis events but also to “foreseeable” events (frequent events with unmitigated consequences beneath the basic safety level defined in Target 4 of the SAPs) and beyond design basis events. The scheme also considers the situation where a SSC is not the primary means of delivering a safety function.

4.4.3 Items that Require Follow-up

96. The proposed approach to categorisation and classification will need to be tested through its application to the full range of safety functions and SSCs in the subsequent steps of GDA. The populated fault schedule (see Section 4.5) will be a key document for considering the appropriateness and effectiveness of the scheme.

97. While the three-tiered system will result in a hierarchy of requirements for SSCs, I have not looked at what these requirements will be, for example what engineering standards will be applied to a Class 1 SSC, what maintenance requirements will be applied to a Class 2 SSC, or what testing requirements will be applied to a Class 3 SSC, etc. This will need to be a significant assessment activity in future GDA Steps, undertaken in close cooperation with colleagues in engineering disciplines.

98. It is important to note that the categorisation and classification scheme needs to be applied beyond the reactor to all the SSCs (with a role in nuclear safety) that are within the scope of the GDA. Notably, this includes the balance of plant (see below), fuel route operations (including but not restricted to the spent fuel pool), and radwaste treatment facilities. The extent of the safety case for these systems beyond the reactor is limited within the PSR submission, therefore I have not been able to assess during Step 2 how effective the proposed categorisation and classification scheme will be in these areas. As discussed in Section 4.2 above, I have identified some concerns with the adequacy of the spent fuel pool cooling engineering design which could be symptomatic of an inadequate approach to categorising safety functions beyond the reactor.

4.4.4 Conclusions

99. The proposed categorisation and classification process appears to be consistent with my expectations but its effectiveness and appropriateness will need to be assessed after it has been extensively applied to the fault sequences and SSCs identified for the UK ABWR.

4.5 Fault Schedule

4.5.1 Assessment

100. I have assessed the extract of the proposed fault schedule supplied in the PSR submission (Ref. 1) and have discussed the RP’s proposals with its SMEs in a number of meetings.

4.5.2 Strengths

101. The proposed format of the UK ABWR fault schedule set out by the RP in Step 2 clearly identifies the list of considered faults and the SSCs available to protect against those faults. Further information is also provided on the expected frequency of such faults (i.e. frequent, infrequent or beyond design basis faults), the operating states considered, assumptions made, whether the SSCs are passive, automatic or manually operated, and what their safety classification is. From my initial review of the format, and from all my subsequent interactions with the RP where it has used the fault schedule as a vehicle for explaining its developing safety cases, I have confidence in the approach being taken.

4.5.3 Items that Require Follow-up

102. The RP has provided successively more developed revisions of its fault schedule during Step 2, with the first 'fully populated' fault schedule to be submitted to ONR as part of the Step 3 PCSR[2]. Assessment of this comprehensive fault schedule will be a major part of my work in Step 3.

4.5.4 Conclusions

103. The format of the UK ABWR fault schedule, along with the RP's proposals for populating it are consistent with my expectations. While I have not assessed the scope or contents of a complete fault schedule as part of my Step 2 assessment, I am confident that the UK ABWR fault schedule will be a vital document for my and other ONR assessors' Step 3 assessments.

4.6 UK ABWR Balance of Plant

4.6.1 Assessment

104. In addition to reviewing the PSR submission (Refs. 1 and 3), as part of my Step 2 assessment, I attended with ONR colleagues a multi-disciplinary presentation from the RP on the UK ABWR balance of plant (Ref. 16).

105. This presentation established that faults initiating in the balance of plant which directly affect the reactor are not a special sub-class of faults. The RP has identified such faults as part of its wider analysis of reactor design basis faults (see Section 3.1.1), consistent with that approach, I will similarly consider balance of plant faults as an integral (as opposed to separate) part of my assessment of reactor faults.

106. As with the other reactor faults, my Step 2 assessment has been limited to a review of the high level claims made by the RP for balance of plant faults and I have not looked in detail at the supporting transient analysis at this stage.

4.6.2 Strengths

107. I am satisfied that faults initiating in the balance of plant are considered in both the UK ABWR design and the (preliminary) safety case. A significant safety feature of the design is the ability to rapidly isolate the primary containment vessel (containing the reactor) from the balance of plant. This claim is clearly established in the PSR submission (Ref. 1) and the supplied J-ABWR analysis illustrates how Hitachi-GE are likely to model such faults (notably main steam line faults) for the UK ABWR.

---

[2] The fault schedule will be a live document that will need to be regularly revised during GDA as the UK ABWR develops.

4.6.3 Items that Require Follow-up

108. Faults associated with the main steam lines and the feedwater system are significant reactor faults which I will be assessing in detail during Steps 3 and 4. I will be examining in detail the design basis safety case, the functional claims made, the SSC requirements and the supporting transient analysis which demonstrates the robustness of the UK ABWR design.

109. Despite not being directly connected to the reactor, faults associated with the off-gas system have the potential to result in radiological releases large enough for DBA to be necessary (as defined by SAP FA.5). During Step 3, I will be seeking evidence that the RP has identified and considered faults in the off-gas system in the PCSR, and summarised the protection against such faults in the fault schedule. I will use this information, along with discussions with colleagues in other technical disciplines, to determine whether it is appropriate to include the off-gas system in my assessment sample for Step 4.

4.6.4 Conclusions

110. Faults initiating in the balance of plant are considered in both the UK ABWR design and the (preliminary) safety case. I will consider these faults in more detail during Steps 3 and 4 as part of my wider assessment of reactor faults. In particular, I will need to look in the detail at transient analysis and engineering substantiation which demonstrates the effectiveness of the systems which isolate the primary containment vessel during fault conditions.

111. In addition, during Step 3, I will be looking to establish confidence in the RP’s consideration of off-gas treatment system faults within the design basis safety case.

4.7 Beyond Design Basis Faults

4.7.1 Assessment

112. The amount of detail provided in the PSR submission on beyond design basis faults is limited. However, the RP’s proposed methodology for identifying and analysing such faults was discussed with it at the two fault studies technical exchange meetings held during Step 2.

113. It has already been commented on that the RP’s initial approach to design basis faults was limited to the consideration of single event initiators (see Section 4.1). It has committed to demonstrating (within the design basis) that the UK ABWR can tolerate a frequent fault coincident with the failure of a major safety system. Through Regulatory Observations RO-ABWR-0007 to RO-ABWR-0010 (Ref. 15), Hitachi-GE are also considering major CCFs within key systems as part of the design basis safety case.

114. It was established at the first of the fault studies technical exchange meetings that a number of the fault sequences the RP had identified for analysing on a best-estimate basis as beyond design basis faults would instead require conservative analysis as part of the expanded DBA safety case. In the time between the first and second technical exchange meetings, the RP had reviewed its approach to identifying beyond design basis faults, recognising the broadening of the scope of its DBA. This resulted in a presentation at the second technical exchange meeting of a revised list of beyond design basis faults (i.e. changed from that originally set out in the PSR).

4.7.2 Strengths

115. The RP has demonstrated during Step 2 that it is aware of the implications of considering CCFs within the design basis on the list of events to be considered as beyond design

basis faults. In response to the interactions with ONR, it has reviewed the methodology for identifying beyond design basis faults and previewed a new approach which appears to be both systematic and rigorous.

116. During Step 2, they set out an acceptable programme to undertake new UK ABWR specific analyses of the newly identified beyond design basis faults. These analyses, largely to be undertaken during Step 3, will make realistic assumptions (i.e. exclude the conservatisms included within DBA) and will demonstrate compliance with more relaxed acceptance criteria (compared to those used for DBA). This is consistent with my expectations.

4.7.3 Items that Require Follow-up

117. While the RP's updated proposals for beyond design basis faults appear sensible, to date they have only been described to ONR in presentations. They need to be formally submitted to ONR through the PCSR and then supplemented by the extensive analysis work required to show that the identified acceptance criteria are met.

118. The definitions of a beyond design basis fault set out in the PSR (see Section 3.7) and the accompanying acceptance criteria appear to be broadly acceptable. However, it is noted that they are narrowly defined with respect to reactor faults. It is possible that beyond design basis faults could occur elsewhere on the UK ABWR plant (notably associated with the spent fuel pool) or in different operating modes. During Step 3, as work on both beyond design basis faults and the fuel route safety case progresses, I will challenge the RP on whether there are any additional events to consider.

4.7.4 Conclusions

119. As a result of expanding the DBA safety case to consider CCFs, it has been necessary for the RP to propose a new methodology for identifying candidate beyond design basis faults. This methodology appears to be broadly acceptable but it will need to be formally assessed during Step 3, along with the accompanying analyses of the considered fault sequences.

120. The way in which the RP has rapidly responded to my challenges in this and related areas with a systematic and well thought out revised approach is encouraging.

4.8 Considerations in the Light of the Fukushima Accident

4.8.1 Assessment

121. The scope and completeness of the DBA safety case, and the treatment of beyond design basis faults have been major parts of my Step 2 fault studies assessment and have been discussed above. ONR's assessment of the RP's claims with respect to severe accidents has been reported elsewhere (Ref. 9). Given the length of time that has elapsed since March 2011, it is my expectation that all of these components of fault studies (i.e. DBA, beyond design basis faults and SAA) should incorporate learning from Fukushima as a matter of relevant good practice.

122. The design of the back-up building and the safety claims placed on it are not described in the fault studies PSR submissions (Refs. 1 & 2). However, during a number of presentations during Step 2, Hitachi-GE have identified areas where key safety functions will be delivered by the back-up building.

4.8.2 Strengths

123. The provision of a segregated back-up building with independent and diverse electrical and water supplies will be a welcomed strengthening of the UK ABWR design.

4.8.3 Items that Require Follow-up

124. ONR is still waiting for specific details on the design and functionality of the back-up building. Crucially for the fault studies topic area, the RP has still to identify which fault sequences (whether they be classified as design basis, beyond design basis or severe accidents) will make claims on the functionality of the back-up building. It was originally envisaged that the back-up building would only be required during very unlikely extreme events, however, in a number of presentations to ONR during Step 2, the RP has indicated it will perform an important role to play in protecting against design basis faults, notably frequent faults with a CCF of a major safety system.

125. Establishing what claims are being made on the back-up building will be a major objective of my Step 3 and 4 assessments. I anticipate the fault schedule will be a vital tool for providing clarity on what these claims are and cascading this information beyond the fault studies topic area into the engineering disciplines.

4.8.4 Conclusions

126. It is my expectation that lessons learnt from Fukushima will be incorporated into all aspects of the UK ABWR safety case as a demonstration that relevant international good practice and operational experience is being taken into account.

127. The back-up building is a welcomed feature but it still needs to be established exactly what its capability will be and what safety claims are being placed on that capability. My interactions with the RP during Step 2, notably those associated with the development of the UK ABWR fault schedule, give me confidence that these claims will become much clearer at the start of Step 3.

4.9 Readiness for Step 3

128. The PSR supplied to ONR for Step 2 of GDA only provides an outline of the proposed safety case for fault studies, and in almost every area there is a commitment to undertake further work ahead of making new submissions to ONR in the form of a much more detailed PCSR and/or supporting topic reports.

129. As part of my interactions with the RP's SMEs during Step 2, I have discussed their programme for undertaking UK ABWR specific analyses of the fault sequences, populating the fault schedule, and addressing my five Regulatory Observations. The first formal submission of the PCSR is due at the start of Step 3 (September 2014) but during Step 2 I have been provided with early drafts of the sections related to fault studies. The RP's work programme is such that not all the identified work streams will be complete in time for incorporation into the first formal revision of the PCSR. However, my discussions with the SMEs (and preview I have had of the PCSR) gives me confidence that there will be sufficient information available at the start of Step 3 to commence my assessment of the arguments that underpin the high level claims considered in Step 2.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

130. The RP has provided a PSR for the UK ABWR to ONR for Step 2 of GDA. For my fault studies assessment, I have assessed the high level claims made in this submission against the expectations of the SAPs, targeting:

- reactor faults;
- spent fuel pool and fuel route faults;
- analysis codes;
- categorisation and classification of SSCs;
- the fault schedule;
- UK ABWR balance of plant;
- beyond design basis faults; and
- considerations in the light of the Fukushima accident.

131. In addition to reviewing the submitted PSR documentation, I have had continuous engagement with the RP in the form of technical exchange workshops and progress meetings. I have found the RP's SMEs to be very knowledgeable and effective. They have been responsive to my specific regulatory expectations in the fault studies topic area, notably with respect to my expectations for analysis and design provisions which represent relevant good practice in Great Britain.

132. Through this assessment I have identified the following areas of strength:

- The RP has demonstrated that its approach to analysing design basis faults is consistent with UK and international relevant good practice.
- The RP propose to use established computer codes to model design basis fault sequences. These codes have previously been accepted as being suitable for licensing boiling water reactors by nuclear regulators in Japan and USA.
- Analysis of the design basis faults considered as part of licensing of Japanese ABWRs shows that acceptance criteria (which limit the radiological consequences resulting from a fault) are consistently met.
- The RP has set out proposals for summarising its fault studies safety case in a thorough and logical fault schedule.

133. I have also identified a number of fault studies related matters in the PSR that require follow-up:

- The RP needs to extend the list of design basis events it considers in its fault studies safety case to include frequent events with a coincident common cause failure of a major safety system, faults occurring a low power operation and during shutdown, faults associated with essential services, and faults associated with fuel route operations. To ensure that these gaps in my expectations are addressed in a systematic manner and to provide additional guidance to the RP, I have raised five Regulatory Observations on these topics. Hitachi-GE's responses to these Regulatory Observations will be a major assessment task for ONR in the subsequent steps of GDA.
- The RP needs to submit to ONR UK ABWR specific analysis for the complete list of design basis events, using the codes and methods it has previewed in the PSR. This analysis, along with supporting information to demonstrate the validity

of the methods employed, will be a major assessment task for ONR in the subsequent steps of GDA.

- The RP has proposed to complement the safety provisions of the ‘standard’ ABWR reactor design with a segregated back-up building. The design and the safety functions to be delivered by this building still need to be established. Consideration of the design and the safety claims on the back-up building will be a key assessment task for ONR in the subsequent steps of GDA.

134. The RP has given me sufficient assurances that it understands the requirement to provide additional information to address these and other matters. As a result, I see no reason, on fault studies grounds, why the UK ABWR should not proceed to Step 3 of the GDA process.

5.2 Recommendations

135. My recommendations are as follows:

- Recommendation 1: The UK ABWR should proceed to Step 3 of the GDA process.
- Recommendation 2; All the important items identified in my Step 2 assessment report should be included for follow up in ONR’s fault studies GDA Step 3 Assessment Plan for the UK ABWR.

6 REFERENCES

1 Hitachi-GE UK ABWR (Generic Design Assessment): Fault Studies to discuss deterministic analysis, PSA and fault schedule development, GA91-9901-0009-00001 Rev B May 2014, Trim Ref. 2014/110645

2 Hitachi-GE UK ABWR (Generic Design Assessment): Initial Safety Case report on Spent fuel pool, GA91-9901-0003-00001 Rev B May 2014, Trim Ref. 2014/109378

3 Hitachi-GE ABWR General Description GA91-9901-0032-00001, November 2013, Trim Ref. 2013/442571

4 Hitachi-GE UK ABWR (Generic Design Assessment): Categorisation and Classification of Systems, Structures and Components, GA91-9901-0007-00001, XE-GD-0104, Rev A, November 2013, Trim Ref. 2013/449576

5 *ONR How2 Business Management System. BMS: Permissioning – Purpose and Scope of Permissioning.* PI/FWD – Issue 3. August 2011 www.onr.gov.uk/operational/assessment/forward.pdf.

6 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.onr.gov.uk/SAPS/index.htm.

7 *Technical Assessment Guides.*

NS-TAST-GD-034: Transient Analysis for DBAs in Nuclear Reactors, Revision 2, June 2013.

NS-TAST-GD-042: Validation of Computer Codes and Calculation Methods, Revision 2, June 2013.

www.onr.gov.uk/operational/tech_asst_guides/index.htm.

8 Generic Design Assessment of HGNE's Advanced Boiling Water Reactor (ABWR) - Step 2 Assessment Plan for Fault Studies ONR-GDA-AP-13-004 Revision 1**.** ONR April 2014. Trim Ref 2013/397166

9 ONR-GDA-AR-14-003 – Assessment Report - UK ABWR GDA - Step 2 Assessment Report - PSA – August 2014, Trim Ref. 2014/180670

10 *IAEA Standards and Guidance*.

International Atomic Energy Agency (IAEA) Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements (SSR) 2/1, IAEA 2012

International Atomic Energy Agency (IAEA) Safety Standards Series – General Safety Requirements (GSR) Part 4: Safety Assessment for Facilities and Activities IAEA 2007

International Atomic Energy Agency (IAEA) Safety Standards Series – Safety Guide: Safety Assessment and Verification for Nuclear Power Plants 2001 (This publication has been superseded by GSR Part 4 and SSG-2)

www.iaea.org.

11 Western European Nuclear Regulators Association Reactor Safety Reference Levels, January 2008

http://www.wenra.org/

12 Hitachi-GE UK ABWR (Generic Design Assessment): J-ABWR establishment permission application document Attachment 10 (Kashiwazaki-Kariwa Unit 6/7), GA91-9901-0047-00001 Rev 0 April 2014, Trim Ref. 2014/171391

13 Hitachi-GE UK ABWR (Generic Design Assessment): Preliminary Safety Report on Electrical Engineering , GA91-9901-0006-00001 Rev C, May 2014, Trim Ref. 2014/206378

14 Hitachi-GE UK ABWR - Schedule of Regulatory Queries raised during Step 2. ONR. TRIM Ref. 2014/271889

15 Hitachi-GE UK ABWR - Schedule of Regulatory Observations raised during Step 2. ONR. TRIM Ref. 2014/271901

16 ONR-GDA-CR-13-037 - Contact Report - Balance of Plant Workshop (BOP) - 18 February 2014, Trim Ref. 2014/105258

Table 1

Relevant Safety Assessment Principles Considered During the Assessment and Comparison with Relevant WENRA and IAEA Standards

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
FA-	**Fault analysis general**			
FA.1	Design basis analysis, PSA and severe accident analysis	The general fault analysis SAPs have been considered throughout the review of the PSR submission and the interactions with Hitachi-GE. In particular, extensive consideration has been given to how DBA is complemented by beyond design basis analysis, PSA and SAA.	E1	Requirement 42: Safety analysis of the plant design (SSR 2/1) Requirement 15: Deterministic and probabilistic approaches (GSR Part 4)
FA.2	Identification of initiating faults		E4	Requirement 2: Scope of the safety assessment (GSR Part 4) Requirement 16: Postulated initiating events (SSR 2/1)
FA.3	Fault sequences		E6	Requirement 4: Purpose of the safety assessment (GSR Part 4) Requirement 14: Scope of the safety analysis (GSR Part 4)
FA-	**Design Basis Analysis**			
FA.4	Fault tolerance	These SAPs set out ONR's expectations for DBA and are therefore considered continually in every fault studies interaction and assessment involving the UK ABWR.	-	Requirement 14: Design basis for items important to safety (SSR 2/1) Requirement 7: Assessment of safety functions (GSR Part 4)
FA.5	Initiating faults		E5	Requirement 16: Postulated initiating events (SSR 2/1) Requirement 14: Scope of the safety analysis (GSR Part 4)

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
FA.6	Faults sequences		E6, E8	Requirement 16: Postulated initiating events (SSR 2/1) Requirement 7: Assessment of safety functions (GSR Part 4)
FA.7	Consequences		E7	Requirement 15: Deterministic and probabilistic approaches (GSR Part 4) Requirement 9: Assessment of the provisions for radiation protection (GSR Part 4) Requirement 6: Assessment of the possible radiation risks (GSR Part 4)
FA.8	Linking of initiating faults, fault sequences and safety measures		E9	Requirement 7: Assessment of safety functions (GSR Part 4) Requirement 10: Assessment of engineering aspects (GSR Part 4)
FA.9	Further uses of DBA		H2.1, H5, H6	Requirement 22: Safety classification (SSR 2/1) Requirement 7: Assessment of safety functions (GSR Part 4) Requirement 10: Assessment of engineering aspects (GSR Part 4)
FA-	**Severe Accidents**			
FA.15	Fault sequences	During Step 2, the assessment of severe accidents has been reported separately from the fault studies report. However, the	LM3.3	Requirement 20: Design extension conditions (SSR 2/1)
FA.16	Use of severe accident analysis		LM1, LM2, LM3, R2	Requirement 20: Design extension

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
		scope of the SAA and how it interfaces with the DBA has been considered in this assessment. The severe accident SAPs set some of the expectations for the beyond design basis events considered in this assessment.		conditions (SSR 2/1) Requirement 7: Assessment of safety functions (GSR Part 4)
FA-	**Validity of data and methods**			
FA.17	Theoretical models	The detailed assessment of the computer codes and methodologies employed by Hitachi-GE is a task for Steps 3 and 4 of GDA. However, these SAPs have been considered as part of the readiness review for Step 3.	-	Requirement 18: Use of computer codes (GSR Part 4)
FA.18	Calculation methods		-	Requirement 18: Use of computer codes (GSR Part 4)
FA.19	Use of data		E8.1, E8.5	Requirement 18: Use of computer codes (GSR Part 4) Requirement 19: Use of operating experience data (GSR Part 4)
FA.20	Computer models		-	Requirement 18: Use of computer codes (GSR Part 4)
FA.21	Documentation		-	Requirement 20: Documentation of the safety assessment (GSR Part 4)
FA.22	Sensitivity studies		E8.7	Requirement 18: Use of computer codes (GSR Part 4) Requirement 17: Uncertainty and sensitivity analysis (GSR Part 4)
FA.23	Data collection		E11	Requirement 18: Use of computer codes

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
				(GSR Part 4) Requirement 19: Use of operating experience data (GSR Part 4)
FA.24	Update review		E11, N3	Requirement 24: Maintenance of the safety assessment (GSR Part 4) Requirement 2: Scope of the safety assessment (GSR Part 4)
NT1	**Numerical Targets**			
Target 4	Design basis fault sequences	A major objective of this Step 2 assessment was to come to a view on the completeness of the list of design basis faults. Target 4 is key to defining the "design basis region". The acceptance criteria proposed by Hitachi-GE for DBA (as a proxy for Target 4) have been assessed as part of Step 2 and will be looked at further in Step 3 and 4.	-	Requirement 16: Criteria for judging safety (GSR Part 4)
EKP-	**Engineering Key Principles**			
EKP.2	Fault tolerance	These principles are fundamental to fault studies and have been considered throughout the review of the PSR submission and the interactions with Hitachi-GE. These SAPs were particularly important to	-	Requirement 10: Assessment of engineering aspects (GSR Part 4)
EKP.3	Defence in depth		E2	Requirement 7: Application of defence in depth (SSR 2/1) Requirement 13: Assessment of defence in depth (GSR Part 4)

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
EKP.4	Safety function	come to a view on the adequacy of the proposed fault schedule.		
EKP.5	Safety measures		E9	Requirement 23: Reliability of items important to safety (SSR 2/1)
ECS-	**Safety Classification and Standards**			
ECS.1	Safety categorisation	These principles have been considered in the assessment of Hitachi-GE's categorisation and classification scheme, and to come to a view on the adequacy of the proposed fault schedule.	G2	Requirement 4: Fundamental safety functions (SSR 2/1)
ECS.2	Safety classification of structures, systems components		G2	Requirement 22: Safety classification (SSR 2/1) Requirement 27: Support service systems (SSR 2/1)
EDR-	**Engineering Design for Reliability**			
EDR.1	Failure to safety	These principles are fundamental to fault studies and have been considered throughout the review of the PSR submission and the interactions with Hitachi-GE.	E9.1	Requirement 26: Fail-safe design (SSR 2/1)
EDR.2	Redundancy, diversity and segregation		E8.2, E9.4	Requirement 21: Physical separation and independence of safety systems (SSR 2/1) Requirement 24: Common cause failures (SSR 2/1)
EDR.3	Common cause failure		E9.4	Requirement 24: Common cause failures (SSR 2/1) Requirement 27: Support service systems (SSR 2/1)

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
EDR.4	Single failure criterion		E8.2, E10.7	Requirement 25: Single failure criterion (SSR 2/1)
ESS-	**Safety Systems**			
ESS.2	Determination of safety system requirements	These principles have been considered at high level in this Step 2 assessment. They will become increasingly important in subsequent Steps when Hitachi-GE's transient analysis is examined in more detail.	-	Requirement 22: Safety classification (SSR 2/1) Requirement 23: Reliability of items important to safety (SSR 2/1)
ESS.4	Adequacy of initiating variables		-	Requirement 15: Design limits (SSR 2/1)
ESS.6	Adequacy of variables		-	Requirement 15: Design limits (SSR 2/1)
ESS.7	Diversity in the detection of fault sequences		E9.1, E9.2, E9.4, E9.5	-
ESS.8	Automatic initiation		E9.3	Requirement 7: Application of defence in depth (4.11 d) (SSR 2/1)
ESS.9	Time for human intervention		E9.3	Requirement 32: Design for optimal operator performance (SSR 2/1)
ERC-	**Reactor Core**			
ERC.1	Design and operation of reactors	These principles have been considered at high level in this Step 2 assessment. They will become increasingly important in subsequent Steps when Hitachi-GE's transient analysis is examined in more detail.	E3.1	Requirement 4: Fundamental safety functions (SSR 2/1)
ERC.2	Shutdown systems		E9.5	Requirement 46: Reactor shutdown (SSR 2/1)
ERC.3	Stability in normal operations		-	Requirement 45: Control of the reactor core (SSR 2/1)

SAP No.	SAP Title	Notes	WENRA Reference levels (Ref. 9)	IAEA Standard (Ref. 8)
EHT-	**Heat Transport Systems**			
EHT.1	Design	These principles have been considered at high level in this Step 2 assessment. They will become increasingly important in subsequent Steps when Hitachi-GE's transient analysis is examined in more detail.	E3.1, E9.7	Requirement 47: Design of reactor coolant systems (SSR 2/1) Requirement 70: Heat transport systems (SSR 2/1)
EHT.2	Coolant inventory and flow		E3.1, E9.7	Requirement 51: Removal of residual heat from the reactor core (SSR 2/1) Requirement 49: Inventory of reactor coolant (SSR 2/1)
EHT.3	Heat sinks		E3.1	Requirement 53: Heat transfer to an ultimate heat sink (SSR 2/1)
EHT.4	Failure of heat transport system		E9.7	Requirement 47: Design of reactor coolant systems (SSR 2/1) Requirement 48: Overpressure protection of the reactor coolant pressure boundary (SSR 2/1) Requirement 52: Emergency cooling of the reactor core (SSR 2/1)