Office for Nuclear Regulation

New Reactors Division

Step 4 Assessment of Fault Studies for the UK Advanced Boiling Water Reactor

Assessment Report: ONR-NR-AR-17-16
Revision 0
December 2017

EXECUTIVE SUMMARY

Hitachi-GE Nuclear Energy Ltd is the designer and Requesting Party for the United Kingdom Advanced Boiling Water Reactor (UK ABWR). Hitachi-GE commenced Generic Design Assessment (GDA) in 2013 and completed Step 4 in 2017.

This assessment report is my Step 4 assessment of the Hitachi-GE UK ABWR reactor design in the area of fault studies

The scope of the Step 4 assessment is to review the UK ABWR design basis and beyond design basis safety case and supporting analysis against the expectations of ONR's Safety Assessment Principles (SAPs) and relevant international guidance. Faults associated with the reactor in all operating modes have been considered, as well as fuel route faults and other facilities on the site containing or associated with radioactive hazards.

My assessment conclusions are:

- Through the generic pre-construction safety report (PCSR) and supporting references, Hitachi-GE has adequately demonstrated for GDA that the UK ABWR can be safely managed in fault conditions.
- The predicted mitigated radiological consequences for most design basis faults on the UK ABWR are very small. This is generally achieved by preventing fuel in the core or the spent fuel pool from failing in fault conditions, and by ensuring barriers which confine any radioactive material remain intact.
- Some faults are associated with a bypass of containment, or are managed through a deliberate release of radioactive steam. However, the predicted doses to workers and the public have been shown to be acceptably small.
- Hitachi-GE has demonstrated that events just outside the design basis or involving multiple failures of safety measures can be managed with the existing equipment such that significant fuel damage can be avoided and that cliff-edge escalations in fault severity will not occur.

My judgement is based upon the following factors:

- A review of the completeness of the list of initiating events identified by Hitachi-GE.
- A comparison of the level and safety classification of engineered protection for faults against UK relevant good practice.
- A detailed assessment of Hitachi-GE's transient analysis, considering the codes and methods used, the level of conservatism included, and the acceptability of the results against applicable acceptance criteria.
- A review of how Hitachi-GE has consolidated its analysis together as part of, and in support of, a wider safety case for the UK ABWR.

To conclude, I am satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for fault studies. I consider that from a fault studies view point, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to future permissions and permits beings secured.

Several assessment findings have been identified; these are for a future licensee to consider and take forward in their site-specific safety submissions. These matters do not undermine the generic safety submission and require licensee input/decision.

LIST OF ABBREVIATIONS

1D	One Dimensional
3D	Three Dimensional
10CFR50	Title 10 Code of Federal Regulations Part 50
ac	alternating current
ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
A-PPRM	Axial-Peaking Power Range Monitor
APR	Automatic Power Regulator System
APRM	Average Power Range Monitor
ARI	Alternative Rod Insertion
ATWS	Anticipated Transient Without Scram
ATWS-RPT	ATWS Recirculation Pump Trip
B/B	Backup Building
BDBA	Beyond Design Basis Analysis
BOC	Beginning of Cycle
BSL	Basic Safety Level
BSO	Basic Safety Objective
BWR	Boiling Water Reactor
C&I	Control & Instrumentation
CCF	Common Cause Failure
COPS	Containment Overpressure Protection System
CPR	Critical Power Ratio
CR	Control Rod
CST	Condensate Storage Tank
CUW	Reactor Water Clean-up System
D/W	Drywell
DAC	Design Acceptance Confirmation
DAG	Diverse Additional Generator
DBA	Design Basis Analysis
DBG	Double Blade Guide
DSP	Steam Dryer, Steam Separator Pit
EA	Environment Agency
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EHC	Turbine Electro-Hydraulic Control System

EOC	End of Cycle
FA	Fuel Assembly
FCVS	Filtered Containment Venting System
FDW	Feedwater System
FDWC	Feedwater Control System
FDWSTP	Feedwater Stop Function
FHM	Fuel Handling Machine
FLSR	Flooding System of Reactor Building
FLSS	Flooding System of Specific Safety Facility
FMCRD	Fine-Motion Control Rod Drive
FMEA	Failure Mode and Effect Analysis
FPC	Fuel Pool Cooling and Clean-up System
FP	Fire Protection System
FSF	Fundamental Safety Function
GDA	Generic Design Assessment
GRS	Gesellschaft für Anlagen und Reaktorsicherheit
HCU	Hydraulic Control Unit
HLSF	High Level Safety Function
HPCF	High Pressure Core Flooder
HVAC	Heating Ventilation and Air Conditioning System
HWBS	Hard-Wired Backup System
IAEA	The International Atomic Energy Agency
LCO	Limiting Condition for Operation
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
LPFL	Low Pressure Core Flooder System
LPRM	Local Power Range Monitor
MCPR	Minimum Critical Power Ratio
MDEP	Multi-national Design Evaluation Programme
MG	Motor-Generator
MOC	Middle of Cycle
MOP	Mechanical Over-Power
MOX	Mixed Oxide Fuel
MS	Main Steam
MSIV	Main Steam Isolation Valve
MSTR	Main Steam Tunnel Room
MSV	Main Stop Valve
MUWC	Make Up Water Condensate System

NRW	National Resources Wales
NSEDP	Nuclear Safety and Environmental Design Principles
OECD-NEA	Organisation for Economic Co-operation and Development - Nuclear Energy Agency
ONR	Office for Nuclear Regulation
P&ID	Piping and Instrumentation Diagram
PCI	Pellet Cladding Interaction
PCIS	Primary Containment Isolation System
PCSR	Pre-construction Safety Report
PCV	Primary Containment Vessel
PLC	Programmable Logic Controller
PSA	Probabilistic Safety Assessment
PST	Primary Source Term
PWR	Pressurised Water Reactor
R/B	Reactor Building
RBC	Reactor Building Overhead Crane
RBM	Rod Block Monitor
RCCV	Reinforced Concrete Containment Vessel
RCIC	Reactor Core Isolation Cooling
RCIS	Rod Control Information System
RCW	Reactor Building Cooling Water System
RDCF	Remote Depressurisation Control Facility
RFC	Recirculation Flow Control
RHR	Residual Heat Removal System
RI	Regulatory Issue
RIP	Reactor Internal Pump
RMI	Reflective Metallic Insulation
RO	Regulatory Observation
RPT	Recirculation Pump Trip
RPV	Reactor Pressure Vessel
RQ	Regulatory Query
RSW	Reactor Building Service Water
RUHS	Reserve Ultimate Heat Sink
S/P	Suppression Pool
SAPs	Safety Assessment Principles
SBO	Station Blackout
SCC	Stress Corrosion Cracking
SFC	Safety Functional Claim

SFP	Spent Fuel Pool
SGTS	Standby Gas Treatment System
SLCS	Standby Liquid Control System
SoDA	Statement of Design Acceptability
SPC	Safety Property Claim
SRNM	Start-up Range Neutron Monitor
SRV	Safety Relief Valve
SSC	System, Structure, (and) Component
SSLC	Safety System Logic and Control System
TAF	Top (of) Active Fuel
TAG	Technical Assessment Guide
TBV	Turbine Bypass Valve
TCV	Turbine Control Valve
TOP	Thermal Over-Power
TSC	Technical Support Contractor
UK	United Kingdom
UK ABWR	United Kingdom Advanced Boiling Water Reactor
US NRC	United States (of America) Nuclear Regulatory Commission
W/W	Wetwell
WENRA	Western European Nuclear Regulators' Association
ΔCPR	Change in Critical Power Ratio

TABLE OF CONTENTS

Annexes

1 INTRODUCTION

1. This assessment report details my Step 4 Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR reactor design in the area of fault studies.

1.1 GDA Background

2. Information on the GDA process is provided in a series of documents published on ONR's website (**http://www.onr.org.uk/new-reactors/index.htm**). The outcome from the GDA process sought by Requesting Parties such as Hitachi-GE is a Design Acceptance Confirmation (DAC) from ONR and a Statement of Design Acceptability (SoDA) from the Environment Agency (EA) and Natural Resources Wales (NRW).

3. The GDA of the UK ABWR has followed a step-wise approach in a claims-arguments-evidence hierarchy which commenced in 2013. Major technical interactions started in Step 2 with an examination of the main claims made by Hitachi-GE for the UK ABWR. In Step 3, the arguments which underpin those claims were examined. The reports in individual technical areas and accompanying summary reports are also published on ONR's website.

4. The objective of the Step 4 assessments is to undertake an in-depth assessment of the safety, security and environmental evidence. Through the review of information provided to ONR, the Step 4 process should confirm that Hitachi-GE:

   - has properly justified the higher-level claims and arguments;
   - has progressed the resolution of issues identified during Step 3; and
   - has provided sufficient detailed analysis to allow ONR to come to a judgment of whether a DAC can be issued.

5. The full range of items that might form part of the assessment is provided in ONR's 'GDA Guidance to Requesting Parties' (**http://www.onr.org.uk/new-reactors/ngn03.pdf**). These include:

   - consideration of issues identified in Step 3;
   - judging the design against the Safety Assessment Principles (SAPs) and whether the proposed design reduces risks to as low as is reasonably practicable (ALARP);
   - reviewing details of the Hitachi-GE design controls, procurement and quality control arrangements to secure compliance with the design intent;
   - establishing whether the system performance, safety classification, and reliability requirements are substantiated by the detailed engineering design;
   - assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final as-built design; and
   - resolution of identified nuclear safety and security issues, or identifying paths for resolution.

6. All of the regulatory issues (RIs) and regulatory observations (ROs) issued to Hitachi-GE during Steps 2 to 4 are also published on ONR's website, together with the corresponding Hitachi-GE resolution plan.

1.2 Scope

7. The intended assessment strategy for GDA Step 4 in the fault studies area was set out in an assessment plan (Ref. 1).

8. The objective of this GDA Step 4 fault studies assessment has been to review the deterministic safety case submitted by Hitachi-GE for initiating events or fault sequences determined to be within the design basis established for the UK ABWR. In

addition, it has considered the adequacy of Hitachi-GE's analysis to show that events, or combinations of events, just outside of the design basis do not result in an escalation to a severe accident with, for example, a significant degradation of the reactor core.

9. ONR's assessments of Hitachi-GE's probabilistic safety case for fault conditions and severe accidents have been reported separately.

10. The scope of this assessment is broad. It includes any initiating faults on the generic single-unit site identified by Hitachi-GE for GDA that have the potential to lead to a person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement. This is notable because the UK ABWR is a direct-cycle boiling water reactor (BWR) that has some inherent design features which are novel for the UK.

11. Despite this breadth of scope, the main focus of this assessment has been on the detailed design basis analysis (DBA) performed by Hitachi-GE on reactor faults, and to a slightly lesser extent, the spent fuel pool (SFP). This is a reflection of the magnitude of the hazard associated with these two locations and the complexity of the analysis undertaken by Hitachi-GE to support its DBA safety case. 'Non-reactor' faults occurring in facilities away from the reactor and SFP have been considered, but in a proportionate and targeted manner.

12. The fault studies GDA review has followed the step-wise approach in a claims-argument-evidence hierarchy, as set out in ONR's guidance. In the earlier Steps 2 and 3, the underpinning safety claims and arguments were assessed (Refs. 2 and 3). The Step 4 assessment has built upon those earlier assessments, looking in greater detail at the evidence that supports claims and arguments made by Hitachi-GE. This has involved the review of:

- documentation summarising the results of transient analysis and showing compliance to acceptance criteria;
- documentation demonstrating the adequacy of the verification and validation of computer codes; and
- documentation demonstrating that claims and arguments identified in fault studies are being cascaded and linked to other technical areas, safety case documentation, procedures, limits and conditions etc.

13. It should be noted that large portions of the safety claims and arguments identified in the fault studies safety case have been revised or added because of ONR's interactions with Hitachi-GE during Steps 2 and 3. As a result, part of the Step 4 assessment has included a review of the completeness of the fault studies related claims and arguments included in the final safety case submissions provided to ONR.

14. In addition to the technical information contained within submissions, this assessment has also considered the adequacy with which the multiple documents provided in the fault studies area are linked together to form a coherent safety case, and how they interface with and support the safety case documentation in other technical areas. Hitachi-GE's top-level report which summaries the totality of its safety case for the UK ABWR, and ties all the different topic areas together is the generic pre-construction safety report (PCSR). It is therefore a significant document for this assessment.

1.3 Method

15. This assessment has been undertaken consistent with internal guidance on the mechanics of assessment within ONR (Ref. 4).

2 ASSESSMENT STRATEGY

2.1 Standards and criteria

16. The SAPs (Ref. 5) constitute the regulatory principles against which dutyholders' safety cases are judged, and therefore are the basis for ONR's nuclear safety assessments, including the assessment detailed in this report. The SAPs are supplemented by Technical Assessment Guides (TAGs) which provide additional advice to ONR inspectors on assessing safety case submissions.

17. International guidance documents are also available which capture long-established relevant good practices for reactor design basis analysis.

18. Further details are provided in sub-sections below. Given the breadth of this assessment, extra discussion on the applicable SAPs and guidance is also given in specific contexts and applications throughout Section 4 as appropriate.

2.1.1 Safety Assessment Principles

19. The following SAPs have been at the forefront of the fault studies assessment described in this assessment report:

- Fault Analysis SAPs FA.1 to FA.9;
- Severe Accidents SAPs FA.15, FA.16 and FA.25;
- Engineering SAPs EKP.2 to EKP.5, ECS.1 to ECS.3, ECV.1, EDR.1 to EDR.4, EHA.3 to EHA.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 AV.1 to AV.8;
- Numerical Targets 4, 5, 6 and 8.

20. Based on experience, these SAPs were identified at the start of GDA Step 4 in the Assessment Plan (Ref. 1) and have informed both the interactions with Hitachi-GE during the step and assessment write-up presented in this report.

2.1.2 Technical Assessment Guides

21. TAGs provide additional guidance to ONR inspectors on the interpretation and application of the SAPs. The following TAGs have informed this fault studies assessment of Hitachi-GE submissions against the SAPs above:

- NS-TAST-GD-34 "Transient Analysis for DBAs in Nuclear Reactors" (Ref. 6)
- NS-TAST-GD-35 "The Limits and Conditions for Nuclear Plant Safety" (Ref. 7)
- NS-TAST-GD-03 "Safety Systems" (Ref. 8)
- NS-TAST-GD-35 "Radiological Analysis Fault Conditions" (Ref. 9)
- NS-TAST-GD-42 "Validation of Computer Codes and Calculational Methods" (Ref.10)
- NS-TAST-GD-19 "Essential Systems" (Ref. 11)
- NS-TAST-GD-94 "Categorisation of Safety Functions and Classification of Structures, Systems and Components (Ref. 12).

22. In addition to the underlying technical merit of Hitachi-GE's UK ABWR design and analysis, I have considered the adequacy with which the supplied documentation is aggregated together as a safety case. TAG NS-TAST-GD-051 (Ref.13) sets out some key expectations for safety cases against which I have compared Hitachi-GE's submissions:

- All references and supporting information should be identified and be easily accessible.

- There should be a clear trail from claims through the arguments to the evidence that fully supports the conclusions, together with commitments to any future actions.
- A safety case should accurately represent the current status of the facility in all physical, operational and managerial aspects.
- For new facilities or modifications, the safety case should accurately represent the design intent.
- There should be reference from the safety case to important supporting work, such as engineering substantiation. The safety case should be able to act as an entry point for accessing all relevant supporting information on which it is built.

2.1.3 National and international standards and guidance

23. There are both International Atomic Energy Agency (IAEA) standards (Ref. 14) and Western European Nuclear Regulators Association (WENRA) positions (Ref. 15) which are relevant to the fault studies assessment of the UK ABWR.

24. The latest version of the SAPs (Ref. 5) was benchmarked against the extant IAEA and WENRA guidance in 2014, including the specific SAPs identified above for this fault studies assessment. In addition, the assessment plan (Ref. 1) explicitly mapped the SAPs above to guidance set out in Refs 14 and 15. Therefore, the general approach adopted in this report has been to assess Hitachi-GE's submissions against the SAPs, and as a result it can be inferred that international guidance is being met.

25. Following the events at Fukushima, the guidance provided in the latest versions of Refs 14 and 15 includes enhanced discussion on the treatment of postulated accident conditions outside of the "traditional" design basis. Both IAEA and WENRA set expectations that 'design extension conditions' should be analysed with a graded or best-estimate approach (in contrast to the conservative, rule-based approach applied for design basis events). They recognise that there are two variants of design extension conditions:

- events which do not result in significant fuel degradation and core damage;
- events which do result in core damage.

26. The first variant is typically as a result of multiple failures and the objective of the analysis is to demonstrate that there is sufficient engineered provision to ensure that the event will not escalate to core damage. Ref. 14 states that analysis for the second variant should be about showing that the plant can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or large radioactive release is 'practically eliminated'.

27. This assessment report has considered the adequacy with which Hitachi-GE has considered the first variant of design extension conditions, ie the demonstration that multiple failures occurring with an initiating event frequency that is outside the design basis will not result in an escalation to core damage. ONR's review of severe accidents resulting in core damage is reported elsewhere (Ref. 16).

28. In addition to the high level guidance provided in Ref. 14 for nuclear power plant design, the IAEA has also published a specific safety guide on the requirements for deterministic safety analysis (Ref. 17). This provides recommendations on computer modelling of thermal hydraulic phenomena such as those considered by Hitachi-GE in its DBA and beyond design basis analysis (BDBA). However, its requirements are consistent (although slightly more detailed) with the expectations set out in the fault analysis series of SAPs.

29. The United States Nuclear Regulatory Commission (US NRC) has many years of experience in regulating BWRs, and its published requirements often represent relevant good practice. Its standard review plan for the review of light water reactor safety analysis reports (Ref. 18) and Part 50 of its Title 10 Code of Federal Regulations (10CFR50) (Ref. 19) include some very detailed, BWR-specific requirements for accident analysis. The UK ABWR has a design history which includes a lot of US involvement, and it has become apparent to me over the course of the GDA that many of Hitachi-GE's design choices and analysis methods are intended to meet US NRC's requirements.

2.2 Use of Technical Support Contractors (TSCs)

30. It is usual in GDA for ONR to use TSCs to provide additional capacity, to enable access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision making etc.

31. To supplement ONR's internal capability, two contracts were placed with Amec Foster Wheeler and Gesellschaft für Anlagen und Reaktorsicherheit (GRS) for fault studies specialists to work as an integral part of the GDA Step 4 assessment team under my supervision.

32. Independent of these contracts for embedded resource, two further contracts were placed with GRS for defined packages of work, with an output in the form of reports providing advice to ONR on the adequacy of specific aspects of Hitachi-GE's UK ABWR safety case:

- a review of the verification and validation evidence available to support the computer codes ODYN, LAMB, SAFER and SHEX used by Hitachi-GE (Ref. 20);
- independent confirmatory analysis on selected fault transients utilising the UK ABWR computer models developed by GRS under contract to ONR during Steps 2 and 3 (Refs. 21 to 27).

33. The review of the computer code verification and validation evidence has provided a significant input to the assessment of Hitachi-GE methods reported in Section 4.8.

34. The independent confirmatory analysis has been referenced on a case-by-case basis as part of the assessment of key design basis reactor transients in Section 4.3. It has also been referenced in Section 4.8 to inform my judgements on the general adequacy of Hitachi-GE's methods.

35. For both work packages, the final deliverables provided by GRS were supplied to Hitachi-GE for information and to allow it to make any comments on the factual accuracy of the TSC's work. It is important to note that the judgements reported in this assessment report are my own, informed by advice provided by GRS where indicated, and cognisant of any contrary opinions or caveats expressed by Hitachi-GE on this advice.

2.3 Integration with other assessment topics

36. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore be carried out in isolation as there are often safety issues of a multi-topic or cross-cutting nature. The nature of fault studies is that it interfaces with almost every topic, however the following areas are particularly notable:

- An objective for DBA and BDBA of reactor faults is to demonstrate that there is no, or at least very limited, consequential damage to fuel in the reactor core as

a result of the event in question. This is demonstrated by showing that a range of limits (referred to as 'acceptance criteria') are complied with. The technical basis and validity of the acceptance criteria related to fuel failure considered in this assessment report have been assessed in the fuel and core technical area. The basis for acceptance criteria on reactor coolant barrier has been assessed in the structural integrity area. The basis for acceptance criteria on the containment structure has been assessed in the civil engineering topic area.

- This assessment report has considered faults associated with the control and instrumentation (C&I) system used to move control rods (CRs) in and out of the reactor core. This aspect of the assessment has been undertaken in close cooperation with the C&I topic area (with regard to the failure mechanisms that can cause the event and the protection systems available to minimise the consequences) and the fuel and core topic area (with regard to the impact of the event on the fuel).
- There is always close cooperation between the fault studies and the probabilistic safety analysis (PSA) topic areas. Hitachi-GE has developed a common process for identifying initiating events considered in both the DBA and PSA, and therefore I have worked with PSA colleagues to consider the adequacy and completeness of the resulting list of events. In addition, the DBA reactor transient analysis considered in detail in this assessment report case has also been used to support aspects of the PSA. Therefore, comments on, for example, the validity of thermal hydraulic computer codes made in this report have relevance to the PSA assessment.
- There are claims within the UK ABWR DBA and BDBA safety case on venting the containment as a diverse means to remove heat. The effectiveness of this measure for ensuring relevant acceptance criteria are met has been considered in this report. However, the acceptability of containment venting in severe accidents, along with a judgement on whether venting in any circumstances is consistent with the objective of practically eliminating large or early releases, has been considered in the severe accidents topic area.
- The UK ABWR has design features to control and manage hydrogen generated in both normal operation and a range of fault scenarios. I have excluded the consideration of hydrogen from this report. Hydrogen generated in normal operation has been considered by the reactor chemistry and internal hazards topic areas. Hydrogen in fault conditions (DBA, BDBA and severe accidents) has been considered in the severe accidents topic area.
- The high level assessment of non-reactor faults has been undertaken in conjunction with PSA colleagues. The more detailed assessment of the engineering which delivers the key safety functions identified in the non-reactor safety case and the compliance with relevant good practice has been undertaken by radioactive waste management specialist colleagues.
- Internal and external hazards are potential initiators of design basis and beyond design basis events, and as such have been considered in this assessment. However, the completeness of the list of hazards considered by Hitachi-GE and the adequacy of barriers that protect against hazards (or limit their consequences) has been separately assessed by colleagues who specialise in internal and external hazards.
- This fault studies assessment has included a detailed examination of the fault schedule developed for the UK ABWR. The fault schedule, and more significantly, the design basis claims it summarises on key structures, systems and components (SSCs), have been relevant to the assessments performed by engineering colleagues (including but not limited to mechanical engineering, C&I, electrical engineering and structural integrity specialists).
- In this report, I have looked in detail at Hitachi-GE's approach to categorising safety functions and classifying SSCs. However, the codes, standards, procurement arrangements, testing and inspection requirements etc that follow from the applied SSC classification are matters for the engineering disciplines.

2.4 Out of scope items

37. As stated in Section 1, the scope of this fault studies assessment is broad, including most initiating faults on the generic single-unit site with the potential to result in significant radiological consequences.

38. The assessment of the fuel route includes cask handling operations within the reactor building. However, all fuel handling operations undertaken after the spent fuel has left the reactor building, including within the spent fuel interim store, are out of scope.

39. Any faults that are specific to a multi-unit site have been excluded from this assessment.

40. The assessed safety case considers all planned operating modes of the reactor, including reactor faults occurring at a range of reactor powers. However, during electricity generating operations, the reactor has been assumed to be normally at, or close to, rated power. Faults occurring during, or as a result of, load-following operations have been treated as out of scope and additional safety case arguments would need to be made if a future licensee planned to routinely operate in such a way.

41. The assessment assumes GE14 fuel will be used. Neither Hitachi-GE's safety case nor this assessment have considered mixed oxide (MOX) fuel.

42. An objective of this assessment has been to judge the adequacy with which Hitachi-GE has identified significant limits and conditions from its UK ABWR fault studies safety case. However, a detailed assessment of setpoints, technical specifications, operating procedures and emergency arrangements has not been performed.

3 REQUESTING PARTY'S SAFETY CASE

3.1 Safety Case Documentation and Structure

43. Hitachi-GE has identified the generic PCSR as the key submission within GDA that outlines the reasons supporting its top level claim that the "UK ABWR constructed on a generic site within the United Kingdom, can be operated safely under all operating and fault conditions." (Ref. 28)

44. The PCSR has 32 chapters. The following two chapters are most relevant to ONR's fault studies assessment:

- Chapter 24: Design Basis Analysis (Ref. 29)
- Chapter 26: Beyond Design Basis and Severe Accident Analysis (Ref. 30)

45. There is, inevitably, a large amount of information in other PCSR chapters which is either relevant background to the two fault studies chapters above, complements the two chapters, or is informed and impacted by the two chapters. Of notable relevance are:

- Chapter 5: General Design Aspects (Ref. 31)
- Chapter 11: Reactor Core (Ref. 32)
- Chapter 12: Reactor Coolant Systems, Reactivity Control Systems and
- Associated Systems (Ref. 33)
- Chapter 13: Engineered Safety Features (Ref. 34)
- Chapter 16: Auxiliary Systems (Ref. 35)
- Chapter 19: Fuel Storage and Handling (Ref. 36)
- Chapter 28: ALARP Evaluation (Ref. 37).

46. While the PCSR is clearly a vital and fundamental part of the UK ABWR safety case, it is only providing a summary of lower level safety case documents. Sitting beneath the PCSR (and referenced from it) are a large number of Topic Reports and Basis of Safety Case Reports. It is these references (and supporting references from these reports) which have been main areas for assessment during GDA Step 4 and provide the technical basis for most of the regulatory judgements included in this report.

47. For fault studies, the following reports have been central to ONR's assessment:

<u>Design basis reactor faults</u>

- Topic Report on Fault Assessment (Ref. 38)
- Topic Report on Design Basis Analysis (Ref. 39)
- Topic Report on SBO Analysis (Ref. 40)
- Containment Venting Strategy in UK AWBR (Ref. 41)
- Overarching Report on Support Systems Safety Case (Ref. 42)

<u>Fuel route and spent fuel pool faults</u>[1]

- Topic Report on Safety Case for Fuel Route (Ref. 43)
- Topic Report on Fault Assessment for SFP and Fuel Route (Ref. 44)
- Topic Report on Design Basis Analysis for SFP and Fuel Route (Ref. 45)

<u>Non-reactor faults</u>

- Topic Report on Fault Assessment (Ref. 38)
- Topic Report on Design Basis Analysis (Ref. 39).

[1] *When the reactor is shut down and connected to the spent fuel pool, Hitachi-GE has addressed faults as part of the reactor safety case. For faults occurring during power operations or when the reactor is shut down and not connected to spent fuel pool, the reactor and spent fuel pool safety cases have been addressed separately.*

Beyond design basis faults (reactor, fuel route and spent fuel pool)

- Topic Report on Beyond Design Basis Analysis (Ref. 46)

48. Many other reports have been referenced by Hitachi-GE and submitted to ONR in the course of GDA Step 4. These have been referenced as appropriate in Section 4 of this assessment report. However, the reports listed above, along with the PCSR, capture the majority of the fault studies safety case.

49. Fault schedules (tabular summaries of the design basis faults and the engineered protection provided against them) are included in Refs 38 and 44.

3.2 Safety case submissions addressing Regulatory Observations

50. In the early stages of my fault studies assessment of the UK ABWR during GDA Step 2, I identified five significant gaps in Hitachi-GE's fault studies safety case that needed to be addressed through Regulatory Observations (ROs):

- RO-ABWR-007 - Spurious C&I failures as design basis initiating events (Ref. 47)
- RO-ABWR-008 - Common cause failure of electrical distribution systems (Ref. 48)
- RO-ABWR-009 - Analysis of loss of off-site power events (Ref. 49)
- RO-ABWR-010 - Design Basis Analysis of essential services and support systems (Ref. 50)
- RO-ABWR-011 - Safety case for spent fuel pool and fuel route (Ref. 51).

51. An additional RO was identified in GDA Step 3:

- RO-ABWR-037 - Safety case for faults not directly related to the reactor (Ref. 52).

52. Final submissions from Hitachi-GE to address these ROs were supplied during GDA Step 4. However, this work has been fully integrated into the wider fault studies safety case set out in Section 3.1. With the original gaps filled, the safety case aspects dealt with by the ROs are not of more or less significance than any other part of the UK ABWR safety case.

3.3 Key Design Features of the UK ABWR

53. The UK ABWR design is described in detail across multiple chapters of the PCSR and the totality of that information is not repeated here. However, there are some key features which are worth highlighting as background for the assessment details that follow.

- The reactor building (R/B) houses the reactor pressure vessel (RPV), the primary containment vessel (PCV), major portions of the reactor steam supply system, steam tunnel, refuelling area, emergency core cooling systems (ECCS), heating ventilation and cooling (HVAC) systems and additional supporting systems.
- The PCV is provided by the reinforced concrete containment vessel (RCCV). The secondary containment is the R/B reinforced concrete building structure that forms the external weather envelope. The secondary containment boundary encloses the RCCV primary containment above the basemat. See Figure 1.
- The SFP is located just next to the reactor inside the R/B and the secondary containment but outside the PCV. In order to access the reactor core, it is necessary to remove the shield plug, the PCV head, the insulator, the RPV head, the dryer unit and the separator assemblies. The SFP is separated from

the reactor well and steam dryer / steam separator pit (DSP) by closed gates. For refuelling operations, the reactor well and DSP are flooded and can be connected to the SFP by removing the gates.

- The reactor core consists of 872 fuel assemblies (FAs) and 205 CRs. The core is surrounded by the core shroud which is designed to separate the coolant that flows upward through the core from the coolant that flows downward in the annular area between the core shroud and the RPV wall (the area known as the downcomer).
- The CRs are inserted into and withdrawn from the core through CR guide tube located within the lower plenum of the reactor. Each CR is connected to a fine-motion control rod drive (FMCRD) by a mechanical coupling. In normal operation, the CRs are moved in small steps by an electric motor. During a fault transient of the plant, the CRs can be hydraulically driven into the core by pressurised water from hydraulic control units (HCUs). This rapid shutdown of the reactor is called a scram. One HCU serves a CR or a pair of CRs.
- Ten reactor internal pumps (RIPs) are located at the bottom of the RPV and are used to control the core flow rate. The coolant from the RIPs is distributed to each FA through the core lower plenum and into the orificed core support plate. The coolant is then heated as it moves upward through the FAs. It exits the core as a two-phase mixture of steam and water. The steam-water mixture enters the upper core plenum where additional mixing occurs, and subsequently passes through the steam separator and the steam dryer. Dry steam exits the RPV through the four main steam (MS) lines and goes onto the turbine (See Figure 2). The water extracted by the steam separator and the steam dryer is discharged back into the annular region, mixed with the feedwater, and then is driven back into the lower plenum by the RIPs.
- The MS lines are provided with steam flow restrictors at each RPV steam outlet nozzle to limit the flow rate in the event of a postulated MS line break. The system also incorporates provisions for relief of over-pressure conditions in the RPV through the safety relief valves (SRVs), and two main steam isolation valves (MSIVs) on each line to isolate the PCV and reactor coolant pressure boundary when necessary.
- Steam is passed through the turbine, condensed in the condenser and returned to the reactor by the feedwater system (FDW). The FDW consists of two lines that transport feedwater from the feedwater pipes in the steam tunnel through the RCCV penetrations to six inlet nozzles on the RPV (each FDW line supplies three nozzles). The feedwater is drawn down to the bottom RPV, through the RIPs and into the core. See Figure 3.
- The off-gas system maintains the main condenser vacuum by extracting air and non-condensable gases (hydrogen and oxygen). It recombines the hydrogen and oxygen to reduce the risk of hydrogen combustion. However, given the nature of a direct cycle plant, it also minimises the release of radioactivity to the environment during normal operations, holding up short-lived radioactive substances in an activated charcoal bed ahead of a stack release.
- The PCV is separated into a drywell (D/W) and wetwell (W/W). The D/W is comprised of two volumes. The upper D/W volume surrounds the RPV and houses the MS and FDW lines, SRVs and the D/W coolers. The lower drywell volume houses the RIPs, FMCRDs and under-vessel components and servicing equipment. The W/W is comprised of an air volume and suppression pool (S/P) filled with water to rapidly condense steam from a RPV blowdown via the SRVs or from a break in a major pipe inside the D/W. See Figure 4.
- During power operations, both the D/W and W/W are inerted with nitrogen to minimise the risk of hydrogen deflagrations.
- The containment has a capability for rapid closure or isolation of all pipes ducts that penetrate the PCV boundary in order to maintain leak tightness. On signals of low reactor water level or high D/W pressure in the MS pipes, etc. all isolation valves that are part of systems not required for operation during fault

conditions, receive an isolation signal from the primary containment isolation system (PCIS) and are automatically closed (if they were not already closed).

- A vital safety system on the UK ABWR is the ECCS. Its main role is to inject water into the RPV in the event of a reactor fault such as loss of the main condenser, loss of coolant accident (LOCA), loss of off-site power (LOOP), etc., in order to maintain RPV water level and ensure fuel cooling. The ECCS network consists of three independent divisions (I, II, and III). Each division has a high pressure and low pressure water injection function into the RPV. See Figure 5.
- In Division I, the high pressure water injection function is provided by the reactor core isolation cooling system (RCIC). This uses a turbine-integrated pump driven by RPV steam. As a result, it can inject coolant into the RPV without an alternating current (ac) electrical power supply when the core is in a high pressure state. Coolant for injection is drawn from either the condensate storage tank (CST) or the suppression pool (S/P).
- In Divisions II and III, the high pressure water injection function is provided by the high pressure core flooder (HPCF). Each division of the HPCF consists of an electrically driven pump which can inject water from either the CST or the S/P when the reactor is in a high or low pressure state.
- All three divisions have a low pressure water injection function provided by the residual heat removal system (RHR) in lower pressure flooder (LPFL) mode. The RHR in LPFL mode draws coolant from the S/P, cools it by passing it through the RHR heat exchangers, and injects it into the RPV when the reactor is in a low pressure state.
- In other modes, the divisions of the RHR also provide several other safety and operational functions, including:
  - Removal of decay and sensible heat from the reactor after normal shutdown and in the event that the main condenser is not available (‘shutdown cooling’).
  - Removal of heat from the PCV by cooling the water of the S/P.
  - PCV cooling through sprays provided in the D/W and W/W to remove heat and condense steam in the containment following a LOCA and thus prevent over pressurisation of the PCV.
  - Backup cooling to SFP if the heat load exceeds the spent fuel pool cooling (FPC) maximum cooling capacity (eg, during a full core offload).
- There are 16 spring-loaded SRVs connected to the MS lines (see Figure 6). Depending on what is required, they individually, in groups or all together provide several safety functions through different actuation means:
  - All 16 SRVs provide an overpressure protection function to the reactor coolant pressure boundary if the direct and increasing static inlet steam pressure overcomes the restraining spring. Steam is released to the S/P via submerged spargers. The valves re-seat automatically when the re-seat pressure is reached to prevent excessive loss of reactor coolant.
  - All 16 SRVs can also provide overpressure protection through the use of a pneumatic actuator initiated automatically or manually to reduce pressure or to limit a pressure rise.
  - In addition to protecting the reactor coolant pressure boundary, the opening of the SRVs by either exceeding the setpoint of the spring or through pneumatic actuation also supports the delivery of reactor core cooling by the high pressure core cooling systems.
  - Seven of the 16 SRVs provide an automatic depressurisation (ADS) function to discharge high pressure steam to the S/P. This allows the RPV to depressurise sufficiently for the delivery of reactor core cooling by the low pressure core cooling systems. The SRVs with ADS function are equipped with one dedicated accumulator for ADS operation (in addition to the accumulator for the active overpressure protection function) and three additional ADS dedicated solenoid valves.

  - Seven out of the nine SRVs which do not form part of the ADS are also controlled by the diverse reactor depressurisation control facility (RDCF) to provide an alternative means of RPV depressurisation.
  - To enable long term heat removal and the reaching of a cold, shutdown state, any two of the SRVs provided with ADS function can be remotely operated to discharge the steam generated due to the decay heat in the RPV into the S/P. This operation is done in conjunction with the RCIC / HPCF and the RHR in shutdown cooling mode.
- The UK ABWR has a backup building (B/B) remote from the R/B which provides an alternative safety management system for design basis events, beyond design basis events and severe accidents. Notably, it includes the flooding system of specific safety facility (FLSS) which can provide cooling water supply to the RPV when the reactor is in a low pressure condition in the event of failure of the primary cooling means.[2] It consists of two trains of two pumps, with a dedicated water source, individual piping and the necessary valves, instrumentation and controls (See Figures 5 and 7).
- The UK ABWR has three emergency diesel generators (EDGs) which can supply power to the three safety divisions in the R/B if the connection to the grid is lost. The B/B has two air-cooled diesel generators (independent and diverse from the EDGs) to supports its operations, for example, FLSS injection.
- The safety system logic and control system (SSLC) is the principal C&I protection system for design basis faults. This system delivers safety functions to protect the reactor in fault conditions such as scramming the reactor, ECCS control, ADS operation, MSIV closure and PCIS operation.
- The hardwired backup system (HWBS) provides a secondary means of dealing with design basis and beyond design basis faults. It is separated, segregated and diverse from the SSLC.
- If the SSLC fails to scram the reactor, the HWBS can control reactivity by either hydraulically inserting the CRs with a separate set of actuation equipment to that used by the SSLC (an alternative rod insertion, or ARI), or by initiating the standby liquid control system (SLCS). The SLCS injects a neutron absorbing solution of sodium pentaborate into one of the HPCF lines to provide sufficient negative reactivity into the core to shut down the reactor from full power operation to cold shutdown conditions if the CRs fail to insert.
- The HWBS also provides hardwired logic to control the operation of the FLSS and RDCF.
- In the early portion of many design basis transients, decay heat from the core is rejected to the S/P water. However, over time, the S/P will also heat up and the pressure in the PCV will increase. The ECCS is the principal means of cooling the PCV and reducing the pressure. However, if this is unavailable for some reason, the operators can use the HWBS to open one of two vent lines to the stack to discharge excess heat and pressure to the atmosphere. One line is ‘hardened’ to the pressures likely to be experienced during accident conditions but is not filtered.[3] It is assumed that it will only be used when there is limited radioactivity in the PCV. The second line is also hardened, but it additionally includes a filter. This filtered containment vent system (FCVS) is primarily designed for severe accidents but is available for design basis and beyond design basis events. See Figure 8.
- As a defence-in-depth measure, the mobile flooding system of the reactor building (FLSR) system can be connected up the reactor building in extreme events to provide a similar functionality to the FLSS. It is not formally claimed for the vast majority of design basis events but it is relevant for ALARP arguments and Hitachi-GE has stated it should be put on an enhanced state of readiness during some planned maintenance activities.

[2] *The FLSS can also provide cooling water to the PCV spray header, the lower D/W, the reactor well and the SFP.*
[3] *The large volume of S/P water into which steam from the core is discharged is assumed to act as filter prior to venting from the W/W.*

3.4 Safety case approaches and principles

54. Hitachi-GE's general approaches and principles for developing its safety case and design are summarised in Chapter 5 of the PCSR (Ref. 31). They are applied throughout the PCSR and safety case documentation, including the fault studies-relevant reports identified in Section 3.1 above. They conform to principles and guidance set out in two supporting Hitachi-GE references:

- Nuclear Safety and Environmental Design Principles (NSEDPs) (Ref. 53)
- GDA Safety Case Development Manual (Ref. 54)

55. Hitachi-GE claims that through the application of the framework set out in Chapter 5 and the two supporting references, it has produced a safety case that meets UK expectations for a modern nuclear power plant (ie consistent with the expectations set in ONR's SAPs and international guidance).

56. Selected aspects of this wide-ranging framework are described below.

3.4.1 Safety Functions

57. Hitachi-GE has identified five fundamental safety functions (FSFs) that need to be provided for the UK ABWR:

- FSF 1 - Control of reactivity
- FSF 2 - Fuel cooling,
- FSF 3 - Long term heat removal
- FSF 4 - Confinement/Containment of radioactive materials
- FSF 5 - Others

58. PCSR Chapter 5 (Ref. 31) further divides these FSFs in uniquely numbered high level safety functions (HLSFs). For example, FSF 1 (control of reactivity) is broken into 10 HLSFs, including:

- HLSF 1-1 - Functions to prevent excessive reactivity insertion
- HLSF 1-2 - Functions to maintain core geometry
- HLSF 1-3 - Emergency shutdown of the reactor
- HLSF 1-4 - Functions to maintain sub-criticality, etc

59. In the fault schedule, Hitachi-GE specifies the HLSFs provided by the SSCs claimed to have a role in ensuring safety following an individual fault. The requirement to provide the specified HLSF identified in the fault schedule becomes a safety functional claim (SFC) for that SSC.

3.4.2 Event Categories

60. PCSR Chapter 5 identifies five event categories for the UK ABWR:

- Expected Events
- Foreseeable Events
- Design Basis Faults
- Beyond Design Basis Faults
- Severe Accidents

61. These categories are based on frequency and (unmitigated) consequences levels defined in the NSEDPs (Ref. 53), and they correspond directly to the Numerical Target 4 Basic Safety Levels (BSLs) and Basic Safety Objectives (BSOs) established in ONR's SAPs (Ref. 5). I have summarised the applied criteria in Table 1 of this report.

62. It is the design basis faults and beyond design basis faults that are covered in PCSR Chapters 24 and 26 respectively, and are the main focus of this assessment.

63. Design basis faults have been divided into infrequent and frequent faults. Frequent faults are those design basis faults with an initiating event frequency greater than $1x10^{-3}$ per year. Infrequent faults have an initiating event frequency between $1x10^{-3}$ and $1x10^{-5}$ per year. Hitachi-GE has also stated that if a fault sequence made up of an initiating event plus the failure of the provided prevention or mitigation SSCs has a frequency greater than $1x10^{-7}$ per year, then that sequence is also considered a design basis fault (almost certainly an infrequent fault).

3.4.3 Categorisation of safety functions and classification of SSCs

64. PCSR Chapter 5 and its supporting references (Refs 53 and 54) set out a three-tier approach to categorisation of UK ABWR safety functions that is based on the recommendations set out in ONR's SAPs (Ref. 5):

- Category A safety functions play a principal role in ensuring nuclear safety in that they are associated with the removal of intolerable radiological risks from design basis faults by either prevention of the risks or reduction of the risks to broadly acceptable levels.
- Category B safety functions make a significant contribution to nuclear safety in that they are associated with the removal of radiological risks outside the design basis by either preventing the risks or reducing the risks to broadly acceptable levels for foreseeable events and beyond design basis faults, which are identified in fault studies. Functions whose failure would lead to a demand on a Category A safety function are also categorised as B.
- Category C safety functions are those that do not fall into either of Categories A or B. They are mainly associated with the support of Category A or B safety functions or identified from ALARP analyses.

65. PCSR Chapter 5 goes on to define a three-tier approach to classify SSCs according their importance in delivering safety functions. Again, what is proposed has its origins in recommendations set out in ONR's SAPs (Ref. 5):

- Class 1 SSCs are claimed as being the principal or first-line means of delivering Category A safety functions and are referred to as A1.
- Class 2 SSCs are claimed as being the second line or diverse means of delivering a Category A safety function, or the principal or first-line means of delivering a Category B safety function, and are referred to as A2 and B2 respectively.
- Class 3 SSCs are claimed as providing a third-line means of delivering a Category A safety function, a second-line means of delivering a Category B safety function or as delivering a Category C safety functions, and are referred to as A3, B3 and C3 respectively.

66. Ref. 54 allows for two safety systems of lower class to be combined, in certain circumstances, to make a system of a higher safety class. A set of criteria are outlined which must be met when this approach is adopted, including single failure tolerance, independence between the two systems, environmental qualification for the accident conditions that will result, and availability controls identified in technical specifications.

67. Hitachi-GE has excluded reactor faults from this approach to combining SSCs; for all reactor design basis faults, simple deterministic rules are applied:

- for infrequent faults, each identified safety function is provided by first-line A1 means of protection;

- for frequent faults, each identified safety function is provided by a first-line A1 means of protection and a diverse means of delivery that is at least A2.

68. PCSR Chapter 5 observes there are a number of UK ABWR SSCs whose failure or maloperation would lead to a demand on a Category A safety function. It states that these SSCs are deemed to provide Category B safety functions and should, therefore, be classified as B2 or B3. It sets out the following classification rules:

- B2 if there is an A1 means of protection against their failure or maloperation;
- B3 if there is diverse A1 + A2 means of protection against their failure or maloperation.

69. Auxiliary services that support components of a system important to safety are considered part of that system and are therefore classified accordingly, unless failure does not prejudice successful delivery of the safety function.

3.4.4 Single failure criterion and maintenance

70. Hitachi-GE has applied the single failure criterion in the form of 'N+2' to the major A1 reactor safety systems (where N is the minimum number of safety measure divisions required to deliver a HLSF). This means that for these systems, which are usually in standby mode, both a limiting single random failure in one division and one division being unavailable due to maintenance can be accommodated.

71. For some non-reactor A1 systems which are normally in operation before a demand is placed on them to deliver a safety function in a fault condition (for example, the SFP's FPC), 'N+1' design provision is provided. Similarly, for A2 systems that would only be called upon after the complete failure of a 'N+2' A1 system, the design requirement is 'N+1'.

72. Hitachi-GE has identified some infrequent design basis reactor faults that are initiated by a common cause failure (CCF) of an A1 essential support system (for example, an electrical power supply or cooling water failure) for which only 'N+1' A2 protection is provided. A justification for acceptability of this position and why Hitachi-GE considers this to be ALARP is set out in Ref. 42.

73. A summary of Hitachi-GE's approach to redundancy, taken from Ref. 54, is given in Table 2.

4 ONR STEP 4 ASSESSMENT

4.1 Overview of assessment approach

74. I have split the assessment that follows into various sections, reflecting the assessment strategy set out in Section 2, and logical breaks in the topic area:

- In Section 4.2, I have considered general aspects of Hitachi-GE's fault studies safety case that are foundational for everything that follows, regardless of the systems involved.
- In Section 4.3, I have presented my assessment of design basis at-power reactor faults. This section is further sub-divided to consider in turn different groups of faults with similar characteristics.
- In Section 4.4, I have presented my assessment of design basis reactor faults occurring during shutdown operating states.
- In Section 4.5, I have presented my assessment of fuel route faults, including faults in the SFP.
- In Section 4.6, I have presented my assessment of non-reactor faults, involving SSCs not directly associated with the fuel inventory in the reactor or SFP.
- In Section 4.7, I have presented my assessment of beyond design basis faults. This is separated into reactor at-power faults, reactor shutdown faults, and fuel route faults. Given the inherently lower hazards involved, I have not considered any beyond design basis faults associated with non-reactor SSCs.
- In Section 4.8, I summarise the conclusions of a sampling assessment of some of the computer codes and methods used by Hitachi-GE in GDA.
- In Section 4.9, I have discussed the adequacy of Hitachi-GE's methods for determining the radiological consequences, and compared the resulting doses with the BSOs and BSLs established by Numerical Target 4 (Ref. 5). I have also included a short section on how the calculated risk to workers for the UK ABWR compares against Numerical Targets 5 and 6.
- In Section 4.10, I have captured my overall impressions on how Hitachi-GE's fault studies documentation integrate together to form a holistic safety case.
- My general assessment strategy has been to assume that the adequacy with which individual SSCs meet the engineering requirements placed on them as a result of their designated safety classification (for example, code compliance, redundancy, single failure tolerance etc) is a matter for engineering topic areas and is beyond the scope of this report. However, by exception, in Section 4.11 I provide some commentary on the engineering adequacy of three SSCs (from a fault studies perspective).

4.2 General aspects

4.2.1 Event Categories

75. SAP FA.5 (Ref. 5) provides a clear definition of what fault conditions on a nuclear facility should be considered within the design basis. Numerical Target 4 introduces the concept of frequent and infrequent faults, with 'stepped' radiological consequences limits dependent on the frequency of the design basis event.

76. I judge the approach to categorising design basis faults set out in PCSR Chapter 5 (Ref. 31) and applied throughout the UK ABWR safety case to be consistent with SAP FA.5. I also welcome the fact that Hitachi-GE has extended the definition of design basis faults to include fault sequences with frequencies as low as $1x10^{-7}$ per year, consistent with SAP FA.6.

77. The unmitigated consequences of reactor faults are almost always severe, and therefore the determination on what qualifies as a design basis fault can be usually be undertaken by consideration of just the initiating event frequency. However, Hitachi-

GE's approach recognises that there are potential design basis events away from the reactor which could have a range of unmitigated consequences. It has therefore also applied a radiological consequences test to the definition of events. This test, which considers both on-site and off-site consequences is based on Numerical Target 4 in the SAPs and therefore is fully consistent with my expectations.

78. More generally, I welcome the fact that Hitachi-GE has developed an approach that is flexible enough to deal with both reactor and non-reactor faults. It includes categorisation of low consequence, high frequency events which do not meet the definition of design basis events (foreseeable events and expected events). Given their low consequences, the safety case for these events is not a regulatory priority for me in GDA, but I do acknowledge this advanced and mature thinking which should help future detailed design work across all parts of the nuclear power plant site.

79. Hitachi-GE's approach of splitting design basis events into frequent faults ($\geq 1x10^{-3}$ per year) and infrequent faults ($<1x10^{-3}$ per year) is consistent with UK relevant good practice. This demarcation is very important for demonstrating a graded approach to the level of engineering protection provided and the applicable acceptance criteria for fault analysis, so I fully accept its adoption.

80. The PCSR defines beyond design basis faults whose unmitigated consequences lie above the Target 4 BSL but whose frequencies are below the cut-off for infrequent design basis faults, ie:

- frequency of initiating event fault $< 1x10^{-5}$ per year
- frequency of fault sequence $<1x10^{-7}$ per year.

81. Through this approach, Hitachi-GE has considered both low frequency, high consequence single initiators, and fault sequences including multiple failures. In Ref. 38, it has sensibly applied a cut-off frequency of $5x10^{-9}$ per year to the sequences it considers through deterministic means (the UK ABWR PSA model still considers sequences with lower frequencies). I consider this to be a pragmatic but rigorous approach. It allows Hitachi-GE to demonstrate that there is not a group of events just outside of the design basis that can escalate to a severe accident with disproportionately higher consequences, while also constraining what is considered by time-consuming and resource-intensive deterministic analysis.

82. Hitachi-GE's event categorisation scheme does use different terminology to that commonly used in international guidance such as Ref. 17 (for example, anticipated operational occurrences, design basis accidents and design extension conditions). However, it is my judgement that:

- It is a relatively straight forward process to map Hitachi-GE's terminology to common international terminology.
- Hitachi-GE's event categories are clearly and unambiguously defined by frequency and consequences, rather than by historical precedence.
- The events categories are consistent with widely-used UK safety case terminology.
- The events categories (and their definitions and implications) are fully integrated into the UK ABWR safety case. Other international approaches are also self-consistent but there are nuanced differences to what Hitachi-GE has applied. By using different terminology, the potential to avoid overseas interpretations being assumed by default can be avoided.
- The systematic identification of beyond design basis events for deterministic consideration is consistent with the approach proposed by Refs. 14 and 15 for design extension conditions, despite the different nomenclature.

83. On that basis, I am satisfied that Hitachi-GE's approach to event categorisation is adequate, consistent with UK relevant good practice, and achieves similar outcomes to the latest international guidance (despite differing terminology).

4.2.2 Operating Modes

84. SAP FA. 6 sets an expectation that design basis fault sequences within the inherent capacity of the facility and permitted by operating rules should be identified and considered. While the UK ABWR will spend most of its time operating at or close to full power, it will be routinely shutdown for refuelling and maintenance. Intuitively, faults occurring when a nuclear reactor is operating at full power will be more onerous than similar faults occurring when the reactor is operating at a fraction of full power or is shut down. However, BWRs such as the UK ABWR are extensively reconfigured during a routine outage; for example the PCV and RPV heads are removed, the SFP gate is opened, divisions of safety systems are taken out of service for maintenance etc. This means that a fault transient experienced by the plant during shutdown operations can progress differently from the way it would if the reactor is configured for power operations. It also means that new faults, unique to shutdown operations, can be introduced because of the changes in configuration or the maintenance / inspection tasks being undertaken.

85. Hitachi-GE's safety case recognises this, and to facilitate a systematic consideration of faults in all operating modes, its fault studies documentation (including the fault schedule, Ref. 38) uses three operating states for the reactor:

- Operating State A – Power Operation. This is the extended operational period at approximately rated power. It includes operation of the CR drive pattern change, required surveillance of equipment etc.
- Operating State B – Plant Startup and Plant Shutdown. This covers both the operational period after a planned shutdown from the reactor water temperature being lower than 100°C through to reaching its rated power, and operational period transitioning from rated power to the plant's cold temperature condition (<100°C). The two different periods of operation have been combined because the pre-fault conditions assumed in any DBA are similar.
- Operating State C – Shutdown Mode. This is the operational period at low temperature levels (<100°C).

86. Operating State C has been further split into six sub-states:

- Operating State C-1: transition to reactor cold shutdown (first 20 hours after the vacuum break of the main condensers)
- Operating State C-2: transition to reactor disassemble and reactor well gate open
- Operating State C-3: full water level in the reactor well and gate open
- Operating State C-4: transition to closed condition of the PCV/RPV top heads
- Operating State C-5: preparation of plant startup
- Operating State C-6: full core offload (similar to C-2 or C-3 but with the inventory of the core stored within the SFP and the SFP isolated).

87. I am satisfied that these operating states provide an appropriate basis for identifying and defining limiting fault sequences in accordance with SAP FA.6. I also consider them appropriate for defining permitted plant configurations and the availability of safety systems in accordance with SAP FA.9 (ie, availability controls to be captured within technical specifications).

88. It should be noted that Hitachi-GE's PSA has used a different nomenclature for these operating states (Ref. 55) however there is one-to-one mapping between the

definitions used in the fault schedule and the PSA. Of more significance is an observation that the other parts of the safety case and the generic technical specifications (Ref. 56) have used a different again nomenclature and, crucially, a different set of definitions for dividing up plant operations.

89. A detailed assessment of technical specifications is beyond the scope of this assessment report. However, Hitachi-GE has chosen to use its generic technical specification document to capture availability controls coming from the GDA safety case, including those originating from fault studies submissions and the fault schedule. As a result, there is an unnecessary potential for confusion and, in the case of shutdown faults, the technical specifications will not have sufficient resolution to capture varying availability controls that have been derived in different operating modes by fault studies analysis. Therefore I have raised the following assessment finding:

- AF-ABWR-FS-01: To allow constraints on the availability of structures, systems and components (SSCs) established by the safety case to be respected in operation (especially in the various shutdown sub-states), the licensee shall review its terminology and definitions of different operating modes to ensure that there is appropriate consistency between the fault schedule, probabilistic safety analysis (PSA) and the technical specifications.

4.2.3 Safety Functions and Classification of SSCs

90. It is my judgement that Hitachi-GE has adequately identified in PCSR Chapter 5 (Ref. 31) appropriate safety functions at both the FSF and HLSF level, in accordance with SAP EKP.4. The defining of safety functions for reactivity, cooling and confinement/containment of radioactive materials is fully consistent with normal reactor safety case practice. Hitachi-GE has chosen to separate short term fuel cooling and long term heat removal into two separate FSFs. I consider this to be appropriate for the UK ABWR design and to the benefit of its safety case. While both are ultimately associated with ensuring fuel in the core is not damaged, providing immediate high pressure safety injection into the core is significantly different in character from removing heat from the containment over a period of several hours.

91. The use of an “others” FSF gives Hitachi-GE’s scheme the flexibility to deal with non-reactor faults (the specifics of the safety function are provided at the HLSF level). It reflects a wider recognition by Hitachi-GE that its UK ABWR safety case is not limited to the reactor and it needs to consider all radioactive hazards on the generic site. I strongly welcome this.

92. Hitachi-GE’s approach to categorising safety functions is based upon, and therefore consistent with, the three-tier A, B and C approach suggested in SAP ECS.1 and TAG NS-TAST-GD-094 (Ref. 12). In an entirely appropriate way, PCSR Chapter 5 (Ref. 31) expands slightly on the brief definitions provided in the SAPs and links them to the event categories used in the UK ABWR safety case (for example, stating what safety categories are relevant for beyond design basis events and foreseeable events).

93. Similarly, Hitachi-GE’s three-tier approach to classifying SSCs is based on the SAP ECS.2 and therefore consistent with my expectations. PCSR Chapter 5 and its supporting references (Refs 53 and 54) provide additional UK ABWR guidance and deterministic rules (beyond the level of detail established in the SAPs) which I welcome. Through the course of my GDA Step 4 interactions with Hitachi-GE, and within the limitations of my fault studies assessment scope, I have found no engineering outcomes that I object to as a result of following this guidance in the specific context of the UK ABWR technology and safety case.

94. The classification scheme does allow for two independent lower class SSCs to be combined as an equivalent safety case claim to a higher class SSC providing a necessary safety function on its own. I would consider such an approach inconsistent with relevant good practice and long standing deterministic rules if it was applied to reactor faults (and therefore not acceptable). However, Hitachi-GE is clear in PCSR Chapter 5 that this approach should not be applied to reactor faults (which have large unmitigated consequences and therefore required high integrity protection than non-reactor faults), and during the course my assessment of the UK ABWR safety case, I found no examples of this being attempted.[4]

95. TAG NS-TAST-GD-094 (Ref. 12) does concede that there may be cases where such an approach is unavoidable (ie the ideal approach of providing a higher class SSC is not reasonably practicable) and recommends in those circumstances that the multiple lower class systems are considered as a whole, with a demonstration that the combination provides an appropriate level of integrity. Appendix A of Ref. 54 provides detailed advice to UK ABWR safety case authors that is consistent with the expectations of NS-TAST-GD-094, so I am content that the necessary safeguards are in place to ensure that this allowance is not used inappropriately. The examples I have seen where this approach has been used for non-reactor faults (protection for off-gas system failures and liquid radwaste system faults – see Section 4.6) have resulted in levels of protection which I judge to be appropriate for those faults and consistent with what is provided on other nuclear facilities.

96. In conclusion, I am satisfied with the scope, flexibility, and outcomes of the three-tier categorisation and classification process developed and used by Hitachi-GE for both UK ABWR reactor faults and for non-reactor faults.

4.2.4 Identification of design basis initiating events

97. SAP FA.2 sets an expectation that fault analysis should identify all initiating faults with significant radiological consequences to a person, or which could result in a significant quantity of radioactive material escaping from its designated place of residence or confinement.[5] SAP FA.5 extends this expectation by requiring all the initiating faults meeting the requirements established as being the design basis of facility to be listed. Requirements 16 and 19 of Ref. 14 establish similar expectations.

98. Gaining confidence in the completeness of the list of UK ABWR faults identified by Hitachi-GE was an area for early regulatory attention, going back to GDA Step 2 (Ref. 2). In addition to my own assessment of Hitachi-GE's early fault studies submissions (notably Ref. 57), I commissioned GRS to compared the list of identified events against IAEA, WENRA, German, Dutch and US regulatory expectations and guidance (Ref. 58). My conclusions and those of GRS on the early submissions were broadly consistent (Ref. 3):

- following Japanese practice, design basis reactor faults in Operating State A caused by a single initiator had been systematically identified through a 'logic tree' approach and a benchmarking exercise against US NRC and IAEA example fault lists;
- faults associated with multiple failures (a failure of a key protection system in addition to an initiating frequent event) had not been systematically identified;
- faults associated with C&I failures had not been systematically identified;
- faults associated with CCFs in electrical distribution systems and essential support systems (for example, cooling water or HVAC systems) had not been systematically identified;

[4] *There are a limited number of cases where these types of arguments have been applied for reactor faults in shutdown modes when the reactor is effectively operating as a SFP. These have been discussed further in Section 4.4.3.*
[5] *A significant radiological consequence is defined in SAP FA.2 as a dose of 0.1 mSv to workers, or 0.01 mSv to a hypothetical person outside the site. Doses less than these values are regarded as 'normal operations'.*

- faults during shutdown operating states had not been systematically identified;
- faults associated with the fuel route and non-reactor SSCs had not been systematically identified;
- beyond design basis faults had not been systematically identified.

99. In response to these findings and the six ROs mentioned in Section 3.2, Hitachi-GE initiated a large programme of failure modes and effects analysis (FMEA), the results of which are summarised in two of the main fault studies submissions provided for GDA Step 4:

- Ref. 38 includes reactor faults in all operating states and non-reactor faults;
- Ref. 44 includes SFP and fuel route faults.

100. In both reports, the specific events identified from the FMEA are linked to bounding initiating events already identified through other means (for example, a requirement of Ref. 18), or appropriate new events are created.

101. I consider the FMEA to be a comprehensive and systematic substantiation of the events identified by Hitachi-GE for consideration in its design basis safety case.[6] It is also traceable; it is relatively straight forward to go from the fault schedule, to the list of bounding events, and from there back to the FMEA summaries (and if necessary, consult supporting FMEA references). This has greatly helped my assessment and should be to the benefit of future safety case authors / users.

102. For the at-power reactor safety case, the original list of single initiating events has been substantiated by the FMEA. However, several new design basis reactor events have been identified by considering CCFs on C&I systems, electrical power supply systems and essential support systems as result of ONR's ROs (Refs 47, 48, 50). For example:

- All CRs (electrically) inserted fault
- Inadvertent opening of all ADS
- Inadvertent MSIV closure due to spurious failure of A1 SSLC
- Loss of all cooling water systems
- Loss of all A1 HVAC. [7]

103. These faults are an important extension to the safety case and have required additional analysis to be performed. In the case of the all CRs inserted fault, design changes have been required.

104. To develop a bounding list of reactor faults during shutdown modes, a slightly different approach was taken by Hitachi-GE. Ref. 38 states that work undertaken to support the development of a shutdown PSA has been used to identify potential initiating events, and the outcome of this work has been reviewed and consolidated into a list of bounding events to be considered by DBA. I am content with this approach and the resulting list of shutdown (design basis) faults ultimately identified. Details of ONR's assessment of the adequacy and completeness of the list of faults for PSA are reported elsewhere (Ref. 59).

105. Before its work to address ROs RO-ABWR-011 (Ref. 51) and RO-ABWR-037 (Ref. 52), Hitachi-GE had not systematically identified faults associated with the fuel route and non-reactor SSCs. I am satisfied that this requirement has now been demonstrably met through Refs. 38 and 44.The scope of the fuel route operations, SSCs, and safety functions considered in Ref. 44 are adequate for GDA, and the types of faults identified (loss of decay heat removal, LOOP, loss of water inventory,

[6] *Ref. 38 states that its results also support the initiating events considered in the UK ABWR PSA model, in addition to the design basis safety case.*
[7] *The full list of new additional events identified as a result on ONR's ROs on CCFs is given in Table 2.3-3 of Ref. 38.*

reactivity insertion, fuel drop and collision, drop of heavy equipment, and over-raise) are consistent with my expectations. The scope of the non-reactor SSCs and processes with potential radioactive consequences in a fault condition considered in Ref. 38 is also adequate for GDA.I note that faults associated with the solid radwaste system are identified but Hitachi-GE does not go on to provide DBA for it because of the immaturity of the design at this point in time. This is a reasonable decision to make and consistent with the GDA scope defined in the radioactive waste management topic area (Ref. 60).

106. SAPs EHA.3, EHA.4 and FA.5 provide clear expectations that internal and external hazards should be considered as initiators for design basis events. The auditable FMEA summarised in Refs. 38 and 44 shows that hazards have been considered as potential initiators for component failures, alongside, for example, mechanical failure, operator error, maintenance errors, C&I failures etc. Separately, the 'gross' challenges specific hazards could pose to the reactor and fuel route (for example, fire, internal explosion, seismic event etc) are summarised in these two reports, referencing more detailed information supplied in internal hazards, external hazards and PSA safety case documentation. I have no objections to this approach. The completeness and severity of these hazards are assessed elsewhere in the GDA Step 4 assessment reports of the relevant ONR specialists and I have not looked to challenge or repeat their reviews.

107. What Refs. 38 and 44 uniquely do is link and bound the potential impact of the hazards to limiting design basis faults already identified. Only those hazards that cannot be bounded by other events have been taken forward for DBA and inclusion on the fault schedule. This does mean that on first review, the fault schedules included within Refs 38 and 44 do not appear to identify all the internal and external hazards the reader may expect to see. For example, the only external hazards included on the fault schedule are 'water based biological fouling' and 'seismic activity'. Hazards such as high air temperature, wind, snow, external flooding etc do not appear. While this is perhaps a little 'unconventional', it is clearly explained and auditable within the main text of the reports that contain the tabular fault schedules, and therefore not a concern of significance.

108. The challenge from internal and external hazards on non-reactor buildings and operations (with a radiological hazard) is not dealt with in any detail in the submissions I have reviewed. Given that the design of many non-reactor SSCs is relatively immature or not confirmed, this is probably appropriate. In addition, for GDA, both I and Hitachi-GE have needed to be proportionate with our efforts. My assessment priorities are focused on the main safety functions that need to be protected to ensure the reactor core and spent fuel inventory remain safe. Therefore, this 'omission' is not an issue for whether a DAC can be recommended. It should be addressed in future safety case submissions after GDA and therefore the following assessment finding is raised:

- AF-ABWR-FS-02: To address the limitations in the prioritised GDA scope adopted by Hitachi-GE, the licensee shall provide a proportionate consideration of the impact of internal and external hazards on non-reactor facilities and activities (with potential to result in a significant dose being received by a person) in future design basis safety case submissions.

109. I would anticipate that the level of proportionality applied is based upon the graded approach to categorisation, classification, codes and standards etc, established by Hitachi-GE in Chapter 5 of the PCSR (Ref. 31).

110. As well as requiring the identification of design basis initiating events, SAP FA.5 (Ref. 5) sets an expectation that initiating fault frequencies are determined on a best-estimate basis (with a caveat for natural hazards). Hitachi-GE has done this, but in a

very limited way. To determine whether an initiating event or fault sequence is within the design basis (and frequent or infrequent), it has generally followed some basic rules based on SSC classification:

- The failure frequency of a Class 1 SSC is assumed to be between 1 x 10^{-3} and 1 x 10^{-5} per year, and therefore an infrequent fault[8];
- The failure frequency of a Class 2 SSC is assumed to be between 1 x 10^{-2} and 1 x 10^{-3} per year, and therefore a frequent fault;
- The failure frequency of a Class 3 SSC is assumed to be between 1 x 10^{-1} and 1 x 10^{-2} per year, and therefore a frequent fault;
- The frequency of a small line break inside primary containment resulting in a LOCA is assumed to be a frequent fault;
- The frequency of a medium or large break inside or outside containment is assumed to be an infrequent fault;
- A frequent fault in combination with a failure of the Class 1 SSC providing a claimed safety function is an infrequent (design basis) fault sequence;[9]
- An infrequent fault in combination with a failure of the Class 1 SSC providing a claimed safety function is outside of the design basis.

111. For the purposes of the GDA, these assumptions are adequate. As reliability targets for SSCs, they are consistent with my expectations as established by TAG NS-TAST-GD-094 (Ref. 12). For much of GDA Step 4, the PSA (which could provide specific, quantitative failure frequencies) was still in development and Hitachi-GE would not have been able to make progress with its design basis safety case if it had waited for values to become available. In addition, given that the results of detailed design work, procurement, installation and commissioning work etc which could substantiate any reliability assumptions are not available in GDA, providing detailed frequencies at this point in time could suggest an inaccurate level of precision while not altering the fundamental claims and arguments of the deterministic safety case.

112. It is my expectation that, over time, substantiated frequencies are attributed to the identified design basis events and that the current event categories are confirmed. If the event category cannot be supported, the safety case will need to be revised and modifications may be required.

113. I consider this to be particularly important work for design basis faults caused by CCFs of A1 essential support systems. In its response to RO-ABWR-010 (Ref. 42), Hitachi-GE has made some reasonable assumptions about the level of redundancy, segregation and hazard tolerance provided for in the design of A1 essential support systems, such that their failure can be assumed to be an infrequent design basis event. This has informed its ALARP arguments about what level of engineering is needed to protect against the consequences of such CCF failures. However, there are additional measures, beyond just the systems' architecture, that will need to be controlled during operation to achieve the assumed level of reliability against CCF, for example: maintenance approaches, lubricant oil supplies, drainage systems, 'smart' firmware devices etc.

114. I have therefore identified two assessment findings:

- AF-ABWR-FS-03: The licensee shall confirm the GDA event categories applied to design basis events with substantiated initiating event frequencies when

[8] *Consistent with the approach taken in e.g. Ref. 12, Hitachi-GE has defined integrity requirements/assumptions as failures on demand as well as failure frequencies. For example, a Class 1 SSC is expected have a failure frequency between 1 x 10^{-3} and 1 x 10^{-5} per year, or probability of failure of demand between 1 x 10^{-3} and 1 x 10^{-5}.*

[9] *For LOOP events of different durations, occurring with different combinations of CCFs, Hitachi-GE used recommendations provided by ONR in RO-ABWR-009 (Ref. 49). These supplied values were consistent with those considered by UK licensees to demonstrate the resilience of their sites to LOOP events following Fukushima.*

detailed design and probabilistic safety analysis (PSA) information becomes available, and update the safety case and fault schedule appropriately.

- AF-ABWR-FS-04: The level of design provision established in GDA for faults associated with A1 essential supports systems is based on an argument that the likelihood of a common cause failure (CCF) is very low. The licensee shall demonstrate that it has done everything reasonably practicable in terms of design, operation and maintenance to minimise the vulnerability of the A1 essential support systems to CCFs (in addition to the assurances provided in GDA on the amount of the redundancy and segregation etc delivered by the systems' architecture).

115. In conclusion, it is my judgment that for GDA Hitachi-GE has adequately identified design basis faults within its UK ABWR safety case, and appropriately allocated event categories to those faults. The list of faults will of course need to be kept under review as part of the development of a site-specific safety case and as the details of the design are further developed. This is assumed to be 'normal business' for any future licensee, but in addition to that, three specific assessment findings have been raised for it to address.

4.2.5 Approach to single failure, maintenance and redundancy for design basis faults

116. SAPs EDR.2, EDR.3, EDR.4 and FA.6 define some well-established expectations for redundancy, resilience to common cause failure, single failure tolerance and the consideration of maintenance in safety cases for design basis faults.

117. Informed and driven by the requirements set out in its safety case guidance and principles (Refs 53 and 54), Hitachi-GE's safety case for the UK ABWR includes extensive consideration of these topics. As stated in Section 3.4.4 and Table 2, Hitachi-GE has established some basic rules to ensure that UK ABWR safety systems are sufficiently reliable, notably a 'N+2' requirement for standby A1 SSCs and 'N+1' for standby A2 SSCs providing frontline protection for design basis faults and diverse protection for frequent design basis faults respectively. Looking at the consequences and outcomes of following these rules is a fundamental objective for this fault studies assessment. However, claims, arguments and evidence relevant to the SAPs above are presented in Hitachi-GE's submissions for many different topic areas (ie not just restricted to fault studies documentation) and I have not attempted to pass comment in this report on all applicable claims in the safety case.

118. As an example of this, engineering basis of safety case reports and the Topic Report on Mechanical Engineering SSCs (Ref. 61) set out to systematically demonstrate that each considered system meets basic rules on single failure, redundancy etc, and therefore substantiate two safety property claims (SPCs):

- Mechanical Engineering SPC 1 – [SSCs] to be designed with redundancy against single failure of any dynamic component under the worst permissible system availability state so that a single failure does not prevent the delivery of a safety function.
- Mechanical Engineering SPC 2 - [SSCs] to be designed with mechanical, C&I, or electrical functional independence such that failure of one dynamic component does not lead to a common cause failure that could prevent the delivery of a safety function.

119. I welcome these as objectives but as a general assessment strategy, I have assumed that how the UK ABWR meets these claims is a matter for colleagues who specialise in engineering topics.

120. Hitachi-GE has recognised that internal hazards have the potential to undermine the resilience of SSCs to single failures and CCFs etc. It has therefore specified an additional SPC on internal hazards (Mechanical Engineering SPC 4) which establishes three requirements for systems:

- Class 1 systems that mitigate the effects of frequent faults or infrequent faults and that prevent the occurrence of events that lead to exposures above the BSL are designed with physical separation between their redundant divisions or are designed to withstand the hazards.
- Class 2 systems that mitigate the effects of frequent faults are designed with physical separation against hazard sources occurring outside their compartment or are designed to withstand the hazard.
- Class 1 systems are physically separated from their equivalent Class 2 alternative systems or are designed to withstand the effects of the hazard occurring in the Class 2 systems.

121. These claims are substantiated in internal hazards safety case documentation, and in cases where they are not met, ALARP arguments are made for the adequacy of the UK ABWR design in Ref. 62. Again, I welcome these claims and the provision of ALARP arguments as appropriate, but as part of my assessment strategy I have assumed that the details provided in these reports have been examined by colleagues who specialise in internal hazards (Ref. 63).

122. Even with this assessment approach, I have still examined several key aspects of the UK ABWR design and safety case, some which are described in further details later in this report:

- The ability of the A1 ‘N+2’ ECCS to take the reactor to a stable, safe state following a LOCA event, assuming a limiting single failure and permitted maintenance (see Section 4.3.7).
- The ability of the A2 ‘N+1’ FLSS to take the reactor to a stable, safe state as a diverse means of providing of water injection, and establishing what assumptions have been made about single failures and maintenance (see Section 4.3.9).
- The general assumptions about single failure and equipment availability made in the reactor transient analysis (see Section 4.3.2).
- The adequacy of the level of redundancy and diversity provided by the extant SRV design provision (See Section 4.11.1).
- The maintenance assumptions made during shutdown operations, when barriers between divisions may be opened to allow access and key SSCs are taken out of service for maintenance (see Section 4.4).

123. In general, I am satisfied that the UK ABWR A1 reactor safety systems are designed with the single failure criterion taken into account and maintenance is either not practical when the reactor is at-power (eg MSIVs or SRVs) or will be controlled by technical specifications (eg EDGs). In many cases, I am satisfied that this is adequately explained in the safety case documentation for specific systems. For example, PCSR Chapter 13 (Ref. 34) summarises in detail the approach taken in the design for isolating the primary containment following a fault, typically through the closure of two isolating valves (ie single failure tolerant). I have found some weaknesses in how the fault studies documentation explains what has been assumed in the analysis which I will discuss later (see Section 4.3.2).

124. Through ROs RO-ABWR-008 and RO-ABWR-010 (Refs 48 and 50), I asked Hitachi-GE to supplement its initial safety case submissions with demonstrations that the UK ABWR is resilient to failures in essential support systems (ie ac power supply and distribution, HVAC and cooling water for ‘frontline’ A1 SSCs), with clarity provided on what it assumes about single failures and availability controls on these systems.

Hitachi-GE's consolidated response, drawing together claims and arguments distributed across the UK ABWR safety case is provided in Ref. 42. This submission was assessed to facilitate the closure of the two ROs and judged to be acceptable. It establishes, and substantiates, some significant claims for the essential support systems:

- Each essential support system is assigned to the highest safety class of the safety systems it is supporting.
- The same approach to the provision of redundancy is applied to essential support systems as is applied to frontline safety systems (ie as per Table 2). This results in adequate levels of redundancy based on the application of single random failure analysis, robustness to internal hazards and the requirements of planned maintenance.
- They are not the limiting factor in the delivery of any FSF.
- Their design architecture supports the assumption that a CCF is an infrequent design basis fault.[10]
- They are either designed to tolerate design basis hazards or are protected against them.

125. I consider Ref. 42 on essential support systems to be an important addition to the safety case. It adequately addresses gaps against the SAPs and UK relevant good practice in Hitachi-GE's initial safety case (which have previously also been observed in other initial reactor safety case submissions to ONR originating from overseas).

126. Ref. 42 is also particularly valuable in a UK-context because civil reactors have historically adopted a four-division design for safety systems, while the UK ABWR only has three divisions. This difference in design provision prompted me to seek clarity on what assumptions are made for planned maintenance, given the apparent constraints with having one fewer division. In Ref. 42, Hitachi-GE has stated that:

- No more than one safety division of A1 and A2 equipment will be taken out of service for planned maintenance regardless of mode of reactor operation. The notable exception is the simultaneous maintenance of one RHR train and one FLSS train in Operating States C-3-2, C-3-3, C-4-1, which is justified by the confirmation of availability and preparation for rapid connection of the FLSR or some other Class 3 system.
- Where there is redundancy within a single division of essential support systems, for example, multiple pumps, then it is possible to undertake planned maintenance on more than one division at any one time.
- The overwhelming majority of planned maintenance on the 6.9kV Class 1 switchboards can be undertaken on specific circuits with the remaining circuits live and available for operation.

127. I welcome the clear presentation of these conclusions in Ref. 42 and I judge it to be a good example of meeting the expectation of SAP FA.9 that DBA should provide the basis for conditions governing permitted plant configurations and the availability of safety systems.

128. I have observed that an important aspect of the UK ABWR design which allows it to tolerate maintenance on the A1 ECCS, despite apparently having fewer divisions of safety systems than existing reactor designs in the UK, is the provision of the B/B. This adds two A2 division of safety injection via FLSS, which are physically separated and diverse from the three divisions of the ECCS. I will comment on the adequacy of the FLSS design later in this report.

[10] *See assessment finding AF-ABWR-FS-04 raised in Section 4.2.4 on the need for a future licensee to substantiate this claim.*

129. As stated in Section 3.4.4, Ref. 42 has identified examples of infrequent design basis events caused by the CCF of an A1 essential support system which are only protected by an A2 'N+1' system. An extended ALARP discussion is provided in Ref. 42 on why this acceptable and why doing anything else would be grossly disproportionate. Although I do not accept it is consistent with UK relevant good practice to have a global rule that any infrequent fault caused by a CCF in an A1 system can have relaxed expectations (compared to any other infrequent design basis event), I am content that in the case of the UK ABWR and the specific faults identified, adding enhanced design provisions would not be ALARP.

130. In conclusion, I am satisfied with the design provision of UK ABWR for single failures, maintenance and redundancy. I also judge that adequate work to substantiate the UK ABWR design architecture and provision has been demonstrated in the fault studies documentation, noting that other ONR specialists have considered how Hitachi-GE has demonstrated specific SSCs compare against the SFCs made on them. I do have some additional comments on the single failure tolerance of the FLSS in Section 4.11.2.

4.2.6 Diversity for frequent faults

131. As stated in Section 3.4.3, Hitachi-GE has recognised in PCSR Chapter 5 (Ref. 31) and its supporting references that diverse means of providing FSFs should be provided for frequent design basis reactor faults to meet UK relevant good practice. This expectation is also extended to other facilities and operations on the UK ABWR site where the radiological hazard could result in a large unmitigated release in a fault condition. The most significant example of this broader application is the SFP.

132. This has resulted in Hitachi-GE clearly identifying in the fault schedule (Ref. 38) and Table 24.3-1 of PCSR Chapter 24 (Ref. 29) both the principal Class 1 means and the diverse Class 2 means of providing the reactivity control, fuel cooling and long term heat removal FSFs for the reactor.

133. The fuel route fault schedule (Ref. 44) and Table 24.3-1 of PCSR Chapter 24 provides similar clarity for the FSFs to be provided for frequent faults associated with the SFP.

134. In an attachment to the main fault schedule (Ref. 38), the SSCs and their safety classification which support the Class 2 SSCs delivering the FSFs are clearly identified (ie, the C&I platforms, the HVAC, cooling water and power supplies). This powerfully illustrates the end-to-end diversity for SSCs providing the FSFs.

135. I welcome the clarity provided by these submissions. In my opinion, it demonstrates that Hitachi-GE's design basis safety case for the UK ABWR has been written with an obvious understanding of UK relevant good practice for the provision of diversity for frequent faults, and with an objective to show that these expectations are met.

136. My assessment of Hitachi-GE's analysis to demonstrate the effectiveness of the identified diverse SSCs for frequent faults is captured as appropriate in later sections of this report, notably Sections 4.3.9 and 4.3.10.

137. A notable exception to the comprehensive provision of diverse protection for frequent faults is the SRVs. The RPV over-pressure protection function is required for both frequent and infrequent fault transient. This is exclusively provided by the 16 SRVs. While there is redundancy in the number of SRVs provided (demonstrated in an appendix to Attachment A of Ref. 39), and diversity in the means of actuation (C&I and electrical power), all the SRVs are the same design. The acceptability of this position has been considered in Section 4.11.1.

4.2.7 Identification of beyond design basis initiating events

138. There is a long-established expectation for DBA to demonstrate that a small change in an analysis parameter will not lead to a disproportionate increase in radiological consequences, ie there should be no cliff edge effect (SAP FA.7). This includes the severity and frequency of the initiating event. In addition, PSA techniques are expected to be applied to faults / fault sequences outside of the design basis, thereby extending the scope of the safety case. However, as discussed in Section 2.1.3, following the events at Fukushima there has been an increased focus and a formalisation in the guidance to consider deterministically events more severe than those analysed within the design basis or which assume a claimed safety measure is circumvented or fails in an unpredicted way (for example, paragraph 663 of the SAPs or Requirements 20 of Ref. 14). The objective of such analysis is to demonstrate that either the plant is robust to such events, or to consider if it is reasonably practicable to provide additional engineered provision to prevent further escalation to significant fuel degradation or core damage (ie prevent it developing into a severe accident).

139. By following UK safety case practice to demonstrate diversity in safety measures for frequent faults, Hitachi-GE is already partly meeting the international expectation to look at events involving multiple failures, as part of the design basis safety case. In Refs 38 and 44, Hitachi-GE extends this consideration even further.

140. In Ref. 38, it has identified all the A1 and A2 SSCs which provide HLSFs following reactor faults during power and shutdown operating states, and assumed a CCF failure frequency for them based on their classification (ie in a similar way to which initiating event frequencies have been allocated for design basis events). For each major design basis fault type (for example, non-LOOP transient, short/medium/long term LOOP faults, small/medium/large LOCA etc), it has systematically considered the failure of one or more SSCs providing a safety function and compared the resulting fault sequences with its 5×10^{-9} per year frequency cut-off. Through this process, it has identified:

- 12 Operating State A (ie at power) bounding beyond design basis events;
- 9 Operating State C bounding beyond design basis events.

141. A similar process has been followed in Ref. 44 for the fuel route, resulting in five beyond design basis events being identified.

142. In my judgement, Hitachi-GE's approach is acceptable and pragmatic. I consider the resulting list of events to be appropriate. It has not used the PSA to identify qualifying sequences (a definitive PSA model was not available for most of GDA Step 4), and the frequencies derived by Hitachi-GE's through this semi-quantitative method should not be considered to be an alternative or a challenge to the frequencies evaluated by the PSA. However, through the combination of demonstrating diversity for frequent faults, and making auditable judgements on further events to analyse by deterministic methods, I am satisfied that it is complementing the insights provided by the PSA and meeting post-Fukushima expectations for identifying beyond design basis events / design extension conditions.

143. I have not considered the treatment of severe external hazards with a beyond design basis return frequency, or combinations of internal hazards within this fault studies assessment report. These matters are dealt with elsewhere (Ref. 63 and 64).

4.2.8 Approach to single failure, maintenance and redundancy for beyond design basis faults

144. ONR's SAPs (SAP FA.15) set an expectation for BDBA to be performed on a best estimate basis. Similar expectations are established in international guidance such as

Ref. 14. This means that the penalising assumptions made in DBA for single failures, maintenance and redundancy do not need to be applied.

145. I have found Hitachi-GE's approach to categorisation and classification (as described in Section 3.4.3) and its approach to redundancy (as described in Table 2) to be consistent with this expectation. The provision of safety functions for beyond design basis events is categorised as Category B, and the principal means of delivering that function is classified as B2. In the case of a safety system normally on standby (eg the FLSS), the UK ABWR is provided with a N+1 capability. This means beyond design basis systems are not provided with sufficient redundancy to still be effective assuming a single failure and extended unavailability due to maintenance. However, this is consistent with relevant good practice.

146. Most of the UK ABWR SSCs delivering a Category B safety function for beyond design basis events are also claimed to provide the same safety function in a backup capacity to A1 systems for frequent design basis faults. This means their requirements are being driven by design basis objectives for an A2 system. While this safety case detail (A2 versus B2) results in minimal differences in terms of design architecture, it does mean that the availability constraints for a system are driven by the more onerous DBA requirements than the BDBA expectations. For example, Hitachi-GE has stated that no more than one safety division of A1 and A2 equipment will be taken out of service for planned maintenance regardless of mode of reactor operation.

147. With these controls on availability established, I am satisfied that the UK ABWR approach to single failure, maintenance and redundancy for beyond design basis faults is fully consistent with expectations.

4.3 Design basis reactor transient analysis

4.3.1 Background

148. At the centre of any reactor safety case is transient analysis to demonstrate that the mitigated consequences of design basis faults are acceptable.

149. SAP ERC.1 (Ref. 5) on the design and operation of reactors states that safety systems should be able to provide robust and reliable protection against scenarios which challenge physical barriers which confine radioactive materials. SAP ERC.3 sets an expectation that a change in parameter, such as temperature, flow, coolant voiding etc should not cause uncontrollably large or rapid increases in reactivity. These expectations need to be demonstrated through analysis. SAP FA.7 (Ref. 5) states that this analysis should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.

150. Hitachi-GE's transient analyses for design basis reactor faults are summarised in PCSR Chapter 24 (Ref. 29). However, its full suite of transient analysis is presented in Ref. 39, and it is this report which has been the main subject of my assessment. It provides analysis for each of the bounding faults identified in Ref. 38, supplemented in many cases by additional sensitivity studies to strengthen Hitachi-GE's safety case arguments.

151. For faults in Operating States A and B, Hitachi-GE has grouped faults together:[11]

- Non-LOCA reactor transients
  - Non-isolation events
  - Isolation events
  - RPV water level decreasing events

[11] *The analysis of faults almost always assumes the initiating event occurs at or close to full power. The notable exception are CR faults which are more limiting during startup operations (Operating State B).*

  - LOOP
  - Inadvertent opening of SRV
- CR faults
- LOCA events, (including main steam line breaks)
- CCF initiated events, including anticipated transients without scram (ATWS)

152. A full list of the reactor faults considered in Ref. 39 is given in Table 3.

153. The distinction between non-isolation events and isolation events predates the development of the UK ABWR safety case. Both involve initiating events which require a reactor scram. In the case of a non-isolation event, the Class 3 feedwater and condensate systems should be available to maintain RPV water level and remove decay / sensible heat, and therefore allow the reactor to be taken to a safe stable state after the initial scram. Isolation events are associated with the closure of the MSIVs (either directly related to the initiating event or because of the response of the protection systems). As a result, the RPV water level is maintained using the ECCS and the heat is removed by blowing down steam via the SRVs and using the RHR in S/P cooling mode or shutdown cooling mode. However, in line with UK relevant good practice set out in SAP FA.6, in its UK ABWR safety case (notably, the fault schedule), Hitachi-GE has taken no credit for the correct performance of Class 3 SSCs where they could alleviate the consequences of the transient. In this scenario, during a 'non-isolation' event the conditions for MSIV closure and ECCS injection (low reactor water level) would be reached relatively quickly, and the same SSCs as claimed for an isolation event would be initiated to take the reactor to a stable, safe state.

154. As a result of this commonality in how a stable, safe state is reached, the majority of Hitachi-GE's transient analysis for the non-LOCA faults in Attachments A and B of Ref. 39 focuses on the initial period immediately after the initiating event has occurred (tens of seconds), demonstrating that a problem can be detected by the SSLC and the CRs inserted before fuel acceptance criteria are violated. It has then separately analysed in Attachment G of Ref. 39 a bounding isolation event to show that a single division of ECCS is sufficient to take the reactor to a stable, safe state. This demonstration is claimed to be applicable for most of non-LOCA design basis faults.

155. Hitachi-GE has provided separate demonstrations to show the resilience of the UK ABWR to LOCA faults. This also is a multi-step process. In Attachment C of Ref. 39, it presents analysis for a range of LOCAs (inside and outside of containment) to show that, on a conservative basis and assuming single failures and permitted maintenance unavailabilities, the reactor will scram and the ECCS will provide sufficient (and early enough) safety injection for fuel acceptance criteria to be met. This analysis is focused on the first few hundred seconds after the initial break.

156. In Attachment D of Ref. 39, Hitachi-GE has analysed the two most severe inside PCV LOCA faults (FDW line break and MS line break) to demonstrate that PCV pressure and temperature acceptance criteria are not exceeded. For both events, it has separately analysed (with different computer codes) the short term response (tens of seconds) of the PCV to LOCA to determine the peak D/W pressure and temperature, and the long term response (several hours) of the PCV to determine the peak W/W (including the S/P) temperatures and pressures.

157. For frequent design basis faults, Hitachi-GE has recognised the need to demonstrate through analysis that the A2 systems claimed to provide a diverse means of delivering a FSF (notably FSF-1, FSF-2 and FSF-3) are effective, assuming a CCF of the A1 systems designed to deliver the same FSFs. In Attachment E of Ref. 39, Hitachi-GE has analysed the frequent faults identified in Ref. 38 assuming an A1 scram has failed, with the aim of demonstrating that fuel, RPV and PCV acceptance criteria are all met if

just A2 systems delivering the FSF-1 function respond.[12] In Attachment H of Ref. 39, Hitachi-GE has analysed bounding frequent faults assuming a CCF of the ECCS, firstly to demonstrate the effectiveness of the FLSS and RDCF to deliver FSF-2 (fuel cooling) in the short term, and then secondly to demonstrate the effectiveness of containment venting (together with the FLSS and RDCF) to deliver FSF-3 (long term heat removal).

158. A LOOP is a relatively straight forward design basis event if the EDGs operate. Hitachi-GE has provided analysis of the initial few seconds of the event, alongside other non-LOCA transients in Attachment A of Ref. 39. Assuming there is a fuel supply to the EDGs (there are on-site fuel supplies for at least 7 days), the bounding analysis presented in Attachment G of Ref. 39 to demonstrate the ability of a single division to take the reactor to a stable, safe state is claimed to also be applicable to a LOOP event. However, in response to RO-ABWR-009 (Ref. 49) and in a variation of the FSF-2/FSF-3 diversity demonstration, Hitachi-GE has analysed in Ref. 40 short-term (<2 hour) and medium-term (<24 hour) LOOP events, assuming a CCF of the EDGs (so called station blackout or SBO events). The objective of this analysis is to show that all applicable acceptance criteria are met through the operation of the steam-driven but time-limited A1 RCIC, and the A2 FLSS, RDCF and containment venting systems.

159. The approach I have taken in the following sub-sections for assessing Hitachi-GE's transient analysis for design basis events is influenced by the approaches described above. In turn, I have looked at:

- the general approach Hitachi-GE has taken in its analysis to plant conditions, plant parameters and assumptions;
- the acceptance criteria against which the results of transient analysis have been compared;
- a sample of Hitachi-GE's analysis for the initial few seconds of non-LOCA fault transients;
- reactivity faults involving the CRs (withdrawal and insertion);
- Hitachi-GE's analysis to demonstrate that a stable, safe state can be reached following a non-LOCA fault;
- LOCA faults;
- ATWS faults demonstrating diversity in the provision of FSF-1 for frequent faults;
- Hitachi-GE's analysis to demonstrate the effectiveness of the diverse means to provide FSF-2 and FSF-3 for frequent faults;
- short and medium term SBO events.

160. My judgements on the general adequacy of the computer codes and methods used by Hitachi-GE are given in Section 4.8. My assessment of how the mitigated radiological consequences for the reactor events compare against Numerical Target 4 of the SAPs is also reported in a later section (Section 4.9)

4.3.2 Analysis conditions and assumptions

161. UK and international guidance expect transient analysis of design basis events to be performed on a conservative basis (for example, SAP FA.7 or Ref. 14). This is in addition to the penalising assumptions SAP FA.6 identifies for fault sequences such as:

- limiting single failure in the claimed safety measures;
- the worst normally permitted configuration of equipment outages for maintenance, test or repair; and

[12] *To maximise the challenge considered by analysis, the correct functioning of the A2 ARI to initiate CR insertion has been disregarded.*

- the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.

162. During the early interactions with Hitachi-GE in GDA Steps 2 and 3, not all assumptions were clearly stated in its fault studies documentation. When I pursued this missing information through meetings and RQs, I established that some assumptions included in the initial submissions were inconsistent my expectations for DBA. However, over the course of GDA, Hitachi-GE has repeated the bulk of its analysis with UK-consistent assumptions, and improved the quality of its documentation. While there remains variability on the level of information provided (which I will comment on throughout this report, including in this section), it is my judgement that the final fault studies reports (notably PCSR Chapter 5 and Ref. 39) adequately describe the major assumptions in the UK ABWR design basis transient analysis across a range of different faults.

163. In this report it is neither necessary nor practicable to repeat every single assumption made in Hitachi-GE's transient analysis. However, I do consider the following items particularly noteworthy and relevant to my conclusions on the adequacy of the analysis:

- System characteristics such as SRV delay / stroke time, RIP coastdown time constant etc, have been set to bound the applicable design specifications. All setpoints for protection systems are claimed to be conservative and include instrument uncertainty, calibration error and instrument drift.
- SRVs providing the overpressure protection function are assumed to open at their higher passive A1 spring-loaded setpoints (increased by 3% from their nominal setpoints), rather than at their lower C3 pneumatically actuated setpoints.
- In a design change made during the course of GDA, all the RIPs receive their power from one of four separate electrical divisions through motor-generator (MG) sets (in earlier ABWR designs, only a fraction of the RIPs were connected to MGs). The mitigating response of the MGs to grid frequency variations or LOOP events has been neglected in the analysis.
- The safe operation of the UK ABWR is governed by a power / flow operating map. This allows core flow to be in the range of 90% to 111% rated flow when the reactor is at rated (100%) thermal power. Non-LOCA transient analysis has therefore been performed at 100% reactor power, and either 90% or 111% flow, depending on which is more limiting. LOCA analysis considering longer term safety limits that are not strongly influenced by pre-fault flow levels has assumed 100% flow and 102% power.
- Ref. 39 states whether an initial core or an equilibrium core has been assumed in a specific calculation, and if beginning of cycle (BOC) or end of cycle (EOC) is the limiting assumption. It explains that pressurisation events have been analysed at EOC for the equilibrium core because the void reactivity feedback is higher and (more significantly) all CRs are withdrawn from the core making the axial power shape higher peaked in the core (the primary mitigation for the increase in power resulting from the events is the insertion of CRs from below). For flow reduction events, the primary mitigation is void reactivity feedback (void fraction increases with lower flow) and therefore initial core BOC is analysed because of the lower void reactivity feedback. For loss of feedwater heating faults, the equilibrium core is limiting due to high void feedback but Hitachi-GE states it is difficult to identify what the limiting conditions are within a cycle so it has performed analysis at a range of positions. Similarly, for CR withdrawal and drop faults, analysis has been performed with both initial and equilibrium cores, and at a range of irradiations / exposures to demonstrate that the results are bounding.

- For those analyses where decay heat is important, Ref. 39 identifies the curves used (decay heat is not a significant consideration in those short-term analyses considering plant behaviour and acceptance criteria prior to reactor scram). Additional justification for the decay heat curves used was provided by Hitachi-GE in response to RQs I raised (Refs 65 and 66). There is some variation in the specific curves used, which mainly seems to be driven by historical precedence and practice in the US for BWR analysis, however, all have an internationally well-known background (ANSI/ANS 5.1 1971 or ANSI/ANS 5.1 1994). Two sigma uncertainty has been applied, apart from some aspects of the LOCA analysis where US 10CFR50 Appendix K (Ref. 67) requires 20% to be applied.

164. I am content with all these assumptions and with how they have been documented in the GDA submissions. Not all of them are substantiated by supplied sensitivity analyses, however I acknowledge that there are decades of BWR experience, analysis and regulatory interactions in Japan and the US which support Hitachi-GE's knowledge base of what is bounding for the UK ABWR.

165. As stated in the previous sub-section, Hitachi-GE's UK ABWR analysis makes no claims on the correct performance of lower class SSCs if they could alleviate the consequences of the event being analysed. They have been assumed to work correctly if this would make the transient worse. This is in accordance with SAP FA.6. In the case of the short-term non-LOCA transient analysis, the control systems whose correct operation have to be considered are the recirculation flow control (RFC) system, the turbine electro hydraulic control system (EHC), and the feedwater control system (FDWC). I am content that the assumptions made about the operation of these Class 3 systems have been clearly described and justified in Ref. 39.

166. In its original GDA Step 2 submissions, Hitachi-GE supplied analysis following Japanese and US BWR practice which took credit for the correct performance of these systems, to the benefit of the predicted consequences. It also assumed the SRVs opened at their lower C3 pneumatically actuated setpoints. It has retained this analysis in Ref. 39 to supplement what it describes as 'transient analysis of common UK practice'. I welcome this. Although the analysis is not fully consistent with the SAPs, it does retain many conservatisms and it more realistically demonstrates how the plant is expected to behave following a design basis fault. It is also informative for ALARP considerations on whether more should be done to reduce risks and safety margins further, because it is showing the contribution 'real' systems already included with the UK ABWR design can make to safety, even though they are not credited in the UK analysis.

167. Single failure and maintenance considerations applied to the divisions of ECCS are extensively set out in Hitachi-GE's LOCA analysis in Ref. 39. However, there is very limited discussion on these topics linked to the short-term non-LOCA analysis in Attachment A of Ref. 39. By way of examples:

- There is no discussion in Attachment A on single failure and maintenance assumptions associated with the SSLC and the MSIVs. Through discussions with Hitachi-GE, I have established that these SSCs have single failure tolerance accounted for in their design, and no maintenance will be performed on them in Operating State A. I am therefore satisfied that it is not necessary to make any additional penalising assumptions in the analysis. However, this is not stated in the submission.
- Hitachi-GE has acknowledged that its short-term non-LOCA analysis assumes all 16 SRVs are available to mitigate the increases in reactor pressure, despite it claiming elsewhere in the safety case that the failure of a single SRV can be tolerated. To address this, it has included a sensitivity case in Attachment A to demonstrate for a limiting fault (feedwater controller failure – maximum

demand) that assuming a failure of one SRV to open has a very small impact on the predicted transient behaviour and all acceptance criteria are met. I judge this approach to be a pragmatic 'fix' that supports its claim on SRV redundancy but it demonstrates to me that the reported DBA has not been performed with the intention of supporting a deterministic design basis claim on SRV redundancy. As a further illustration of this point, the applicable basis of safety case report (Ref. 68) states that only 14 out of the 16 SRVs are required, and references PSA work as the substantiation (despite single failure and maintenance being a 'classic' DBA concern).

- In a similar observation, the applicable basis of safety case report for the CRs (Ref. 69) states that single failure tolerance has been demonstrated by analysis showing that the reactor can reach a hot shutdown state if two out of the 205 CRs do not insert (pairs of CRs share a HCU). However, rather than referencing DBA work to substantiate this deterministic claim, Ref. 69 identifies a PSA reference. Meanwhile, Attachment A of Ref. 39 says nothing about what has been assumed in its analyses with regard to CR single failure. In response to a question, Hitachi-GE has supplied some historic qualification reports that show that modelling of a reactor scram to examine short-term challenges to fuel integrity is not sensitive to CR single failure assumption (Ref. 70). I accept the arguments put forward with regard to the insensitivity of the analysis, and ultimately have no concerns about the shutdown margin provided by the CR. Unfortunately, this is not discussed in the main submission.

168. For the purposes of GDA, I have obtained sufficient information to reach conclusions on the adequacy of the assumptions made in the DBA. I am broadly content that appropriate assumptions have been made, and I will discuss any exceptions on a case-by-case basis in the rest of Section 4.3. However, the limited discussion on single failure and maintenance assumptions in Attachment A of Ref. 39, and the failure to link these to claims made elsewhere in the safety case are examples of a general weakness in the documentation that I will discuss a number of times in Section 4.3 and will summarise in Section 4.10.

4.3.3 Acceptance criteria for design basis reactor faults

169. SAP FA.7 (Ref. 5) states that DBA should demonstrate for fault sequences, so far as is reasonably practicable, that the correct performance of the claimed passive and active safety systems ensures that:

- none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactive material is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity;
- there is no release of radioactivity; and
- no person receives a significant dose of radiation.

170. If these criteria cannot be fully met, it is expected that radiological consequences are minimised and comparisons made against the BSOs and BSLs set out in Numerical Target 4.

171. In PCSR Chapter 24 (Ref. 29) and Ref. 39, Hitachi-GE puts forward an approach for reactor DBA acceptance criteria that I judge to be consistent with the expectations of SAP FA.7. I am satisfied that in most cases (there is one exception), they represent appropriate tests for the results of DBA.

172. PCSR Chapter 24 recognises that the first line of defence against radioactive release is the fuel cladding. For all design basis reactor faults it defines three criteria for the fuel:

- the calculated maximum fuel cladding temperature shall not exceed 1,200°C;

- the calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation; and
- for reactivity insertion faults, the fuel enthalpy shall not exceed the limit value to prevent generation of mechanical energy.

173. These are all internationally well-established criteria for light-water reactor DBA, for example, US NRC's 10.CFR50.46 (Ref. 19) and Chapter 4.2 of its 'Standard Review Plan', Ref. 18). However, PCSR Chapter 24 goes on to recognise that it is reasonably practicable to impose greater margins to fuel failure for frequent design basis faults:

- the calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning / creep rupture (perforation) temperature, so as to preclude cladding failure;
- fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the thermal over-power (TOP) or the mechanical over-power (MOP) limits.
- for reactivity insertion faults, enthalpy addition shall not exceed the design limit.

174. Ahead of demonstrating the first frequent fault criterion, Hitachi-GE has identified a preliminary test, which if met, should ensure there is no significant increase in fuel cladding temperature or mechanical damage without the need for further analysis:

- the critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.

175. The exact value of the safety limit MCPR could vary based on the core design adopted for a particular operating cycle. For the design basis analysis in PCSR Chapter 24 (Ref. 29) and its supporting reference (Ref. 39), Hitachi-GE has considered a MCPR of 1.06 to be appropriate for the GE14 fuel and associated core design assumed in GDA.

176. These fuel-based acceptance criteria are discussed in more detail in PCSR Chapter 11 (Ref. 32), and judged to be appropriate in a parallel ONR assessment to this fault studies review (Ref. 71). Within the scope of this fault studies report, I consider the phenomena considered to be appropriate for reactor DBA, and I welcome the graded approach to fuel acceptance criteria.

177. In later sub-sections of this assessment of design basis reactor transients, I will identify some potential challenges in specific fault sequences to the frequent fault limit on maximum fuel cladding temperature. The observation made in Ref. 71 is that above 800°C, there is a significant change to the cladding microstructure, which would make the fuel's continued operability uncertain. The judgement of the ONR fuel specialist is that a brief exposure of low-burnup cladding to temperatures up to 800°C for a few seconds would probably not prevent a utility making a case to return the plant (and the fuel) to power operation. It is therefore likely there will still be significant margin to cladding failure at, or even slightly above, this limit in the early part of a fault transient while the RPV is still pressurised.

178. PCSR Chapter 24 states that the reactor circuit boundary is the second line of defence for preventing significant releases of the radioactivity for non-LOCA faults. As with the fuel criteria, it applies a graded approach dependent on the frequency of the initiating event:

- for infrequent faults, the pressure on the reactor coolant boundary should be maintained below 120% of the maximum allowable working pressure;
- for frequent faults, the pressure on the reactor coolant boundary should be maintained below 110% of the maximum allowable working pressure.

179. For LOCA events, the pressure boundary is already failed so no acceptance criteria apply.

180. The adequacy of the reactor pressure boundary for both normal operations and in fault conditions is being assessed outside of this assessment report by ONR structural integrity specialists (Ref. 72). However, I am satisfied that the identified acceptance criteria are sensible and appropriate, noting they provide a margin to the expected point of failure.

181. The third line of defence identified in PCSR Chapter 24 for reactor faults is the PCV. For most reactor design basis faults (regardless of frequency), Hitachi-GE has stated that the following acceptance criterion applies:[13]

- the pressure and temperature on the reactor containment pressure boundary shall be maintained below the maximum design pressure and temperature.

182. It references out to PCSR Chapter 13 (Ref. 34) for the applicable design pressures and temperatures. These values are also summarised in Table 4 of this report.

183. Ensuring the containment is not compromised during a fault transient is important for nuclear safety and I welcome the inclusion of an acceptance criterion to demonstrate that this issue is considered during GDA. The design values identified in PCSR Chapter 13 (and summarised in Table 4) are long-standing and have been demonstrated in analysis for other ABWR reactor designs in the US and Japan. However, as I will discuss later in some of the following sub-sections, there are a number of events identified for the UK ABWR which challenge the established limits. As a result, I will report some specific assessment conclusions on this acceptance criterion later in this report.

184. If there are no fuel failures, no breaks in the reactor pressure boundary, and no challenge to the integrity of the PCV, for most faults it can be assumed that requirements of SAP FA.7 for there to be no release of radioactivity and no person to receive a significant dose of radiation are met. However, the reactor coolant has a limited radioactive source term even in normal operations, and some faults by their very nature involve a break in the reactor pressure boundary or a bypass of the containment. Hitachi-GE has recognised this in PCSR Chapter 24 and defines some on-site and off-site dose targets that are consistent with Numerical Target 4 in the SAPs (Ref. 5).

185. Unlike other regulators, ONR does not define technology-specific limits or acceptance criteria for specific parameters. Ultimately, my judgements of whether DBA is demonstrating adequate protection for a fault are informed by a comparison of the predicted radiological consequences against the expectations of the SAPs and Numerical Target 4. However, I am content with how Hitachi-GE uses the acceptance criteria as the first demonstration of acceptability, and only discusses the radiological consequences when necessary.

4.3.4 Non-LOCA reactor transients

186. Attachment A of Ref. 39 details Hitachi-GE's analysis for the initial period of non-LOCA transients. The same methods are applied for each fault considered (specifically conservative analysis with the ODYN, ISCOR and TASC computer codes) to demonstrate that fuel and RPV pressure boundary acceptance criteria are met.

187. All the faults analysed are frequent faults (see Table 3), and therefore the relevant (onerous) acceptance criteria apply.[14] [15] For the majority of the events, the calculated

[13] *In some shutdown modes, the PCV will be open and therefore no acceptance criterion applies.*

MCPR remains above the MCPR safety limit of 1.06. Fuel cladding and RPV pressure boundary limits are also not challenged. However, for the following five events, the critical power ratio has been calculated to be less than 1.06:

- (Total) Loss of reactor coolant flow
- Feedwater controller failure – maximum demand
- Generator load rejection with failure of all bypass valves
- Loss of main condenser vacuum
- LOOP.

188. For these five events (the last three being very similar), Hitachi-GE has calculated that the peak cladding temperature never exceeds 800°C and is already reducing by the end of its short term analysis considering just the first few seconds of the transient. On that basis, it is claiming fuel failure will not occur.[16]

189. I have commented on the general adequacy of the computer codes used for these non-LOCA analyses in Section 4.8 later in this report, and in Section 4.3.2 above I have already stated that I am content with level of conservatism assumed in Hitachi-GE's transient analysis. Therefore, if the analysis results which show compliance with acceptance criteria are taken at face-value, the major objectives for the fault studies safety case have been met. However, I selected four events for closer examination, including commissioning independent confirmatory analysis with my TSC (see Section 2.2) to determine if there were any specific or general insights to be gained:

- Partial loss of reactor coolant flow
- Complete loss of reactor coolant flow
- Feedwater controller failure – maximum demand
- Generator load rejection with failure of all bypass valves.

4.3.4.1 Partial loss of reactor coolant flow

190. I chose this event to be part of my sample for detailed assessment as a representative example of a flow reduction event. It is also an example of a non-isolation event for which the MSIVs are not expected to close.

191. There are 10 RIPs, connected as pairs or threes to four different groups of medium-voltage buses. This is to prevent four or more RIPs simultaneously tripping from a single failure of one bus. In the initial UK ABWR design proposed in GDA (based on a reference Japanese plant) only some of the RIP groups were connected to MG-sets. The original analysis conservatively assumed the failed group was the one without a MG-set, disregarding the mitigating effects the extra electrical inertia could provide to the transient. During the course of GDA, Hitachi-GE identified a need to connect all the RIP groups to MG-sets in order to meet UK grid-code requirements. In its final analysis in Ref. 39, Hitachi-GE still takes no credit for the beneficial effect the MG-sets would have on this transient. I have no objections to this significant conservatism for demonstrating compliance with acceptance criteria in GDA however future transient analysis may be necessary to inform the design requirements of the MG-sets.

---

[14] The frequent fault generator load ejection with turbine bypass has not been analysed using 'UK methods' because the operation of the C3 turbine bypass is not assumed. The event is therefore bounded by generator load ejection without bypass.
[15] A long term LOOP event is the only infrequent fault identified in Attachment A of Ref. 39 and Table 3. However, over the period covered by the transient analysis, it is identical to the frequent short term and medium term LOOP events. It has therefore not been analysed.
[16] When analysed using the slightly relaxed assumptions of US / Japanese methods, Ref. 39 shows that four out of the five events do not go beneath the MCPR limit. The total loss of reactor coolant flow fault still fails to stay above the limit but in the US and Japan safety documentation the event is effectively claimed to be an infrequent fault and MCPR is not an applicable acceptance criterion.

192. I am satisfied that Ref. 39 adequately details (and justifies) the assumptions made in the analysis for the correct performance or otherwise of the Class 3 RFC, EHC and FWDC systems.

193. The transient analysis shows that after the three RIPs trip, core flow decreases and voids in the core increase rapidly. The reactor power decreases and the RPV water level rises. The pump flow in the still operating RIPs actually increases due to the decreased flow path resistance. There is a change in core power ratio (ΔCPR) but it is small and it remains above the MCPR safety limit. There is no threat to other acceptance criteria, for example, the peak surface heat flux of the fuel cladding does not exceed its initial value, and SRVs are not required to lift so there is no challenge to the containment boundary pressure limit.

194. Even with the conservative assumptions made on the performance of control systems, the setpoints for a turbine trip, MSIV closure or a reactor scram are not reached. The fault schedule credits the same A1 ECCS systems to take the plant to a safe shutdown state (and these would be available and effective if needed) but the analysis shows the reactor settling to a new equilibrium power of about 80% of rated power. Only if necessary would the operators transfer the reactor to cold shutdown using the normal shut down operations for the plant.

195. GRS analysed the same transient using its ATHLET model (Ref. 22). Its results closely matched Hitachi-GE's, including on the margins to safety limits and scram setpoints. This independent work strengthens my confidence in Hitachi-GE's analysis.

196. I do note that Hitachi-GE's text in Ref. 39 for its 'UK practice' analysis is not clear about the fact that it has assumed that nine rather than 10 RIPs are running initially (it is stated more clearly in the US/Japanese analysis for the same transient that is retained in Ref. 39). One consequence of this has been that GRS modelled 10 RIPs reducing to seven RIPs, rather than nine RIPs reducing to six RIPs. I am satisfied that this does not have a significant impact on the conclusions that can be reached from the independent transient analysis (both GRS and Hitachi-GE have assumed 111% initial flow despite the different number of operating RIPs), however it does illustrate a need for slightly more information to be provided in UK ABWR documentation (notably PCSR Chapter 24 and Ref. 39) to reach the highest safety case standards for traceability and clarity (see Section 4.10).

197. Somewhat unusually for design basis transient analysis, rather than showing the effectiveness of the safety systems to protect against this fault (ie a scram and the ECCS), the results are demonstrating the effectiveness of the RIP design architecture. I welcome this, noting that such an approach is fully consistent with the expectations of SAPs EKP.2 and FA.4 for showing robustly the fault tolerance of the engineering design.

4.3.4.2 Complete loss of reactor coolant flow

198. I chose to sample this event because it is an obvious partner to the partial loss of reactor coolant flow fault. In addition, this fault has been historically treated as an infrequent fault in US and Japanese safety documentation and therefore compared against less onerous acceptance criteria than are applied to frequent faults. In the UK ABWR safety case, Hitachi-GE has recognised that B3 classification of the RIPs and their support systems to circulate reactor coolant in normal operations (Ref. 73) means that a complete failure should be treated as a frequent event.

199. The analysis assumption is that power supplies to all RIPs are simultaneously lost. As with the partial loss of flow event, no credit is taken for the MG-sets. I am content with the arguments for which Class 3 control systems are assumed to operate in the analysis, notably the EHC, because they make the transient worse.

200. The transient analysis shows that when all the RIPs trip concurrently, the core flow rapidly reduces and the voids increase. Approximately 2 seconds later, an A1 reactor scram is initiated on 'core flow rapid coastdown'. Due to the rapid reduction in the flow rate, the MCPR does briefly fall beneath the 1.06 safety limit. The resulting boiling transition reduces the heat transfer from the fuel cladding to the coolant, and the fuel cladding temperature increases. However, this increase is stopped by the reactor scram.

201. Hitachi-GE's analysis following 'UK practice' predicts that that peak cladding temperature never exceeds 500°C despite the boiling transition. As a result, it claims that fuel failure will not occur. Other acceptance criteria are not challenged. Similar results are predicted by its 'US/Japanese practice' analysis with slightly less onerous assumptions made. A boiling transition and some cladding heat up is still predicted, but to a lesser degree.

202. GRS analysed the same transient using its ATHLET model (Ref. 22). As with the partial loss of reactor coolant flow event, its results closely matched Hitachi-GE's. All acceptance criteria were met, with the exception of the 1.06 MCPR limit. Slightly higher peak cladding temperatures were predicted (still around 500°C) but the 800°C limit for fuel failures was not challenged.

203. A total loss of reactor coolant flow event is categorised by Hitachi-GE as a non-isolation event. In its transient analysis, although the RPV water level does increase, it never reaches the 'Level-8' high water setpoint for a turbine trip, even with the RFC frozen. GRS observed a similar behaviour in its analysis but raised the question of what would be consequences for the event if non-safety equipment designed to protect the turbine from damage did prompt a turbine trip. It was concerned that the rapid closure of turbine stop and control valves could result in a RPV pressure rise and reactivity insertion (these phenomena are discussed further in Section 4.3.4.4 below).

204. I challenged Hitachi-GE on this point through a RQ. In its response (Ref. 74), Hitachi-GE conceded that it would expect the turbine to be tripped after the reactor scram by the B3 systems that protect the turbine. However, due to the reactor power levels dropping to decay heat levels after the scram, it claims the consequences of the pressure rise are bounded by those seen in generator load rejection (with failure of all bypass valves) and loss of main condenser vacuum faults. In order to demonstrate the effectiveness of the A1 systems on their own to provide the necessary A1 FSF-1 reactivity control functions, it has chosen to exclude this B3 functionality. I judge these arguments to be an acceptable response to GRS's observations, but again it illustrates that slightly more information and discussion within the main safety case documentation would strengthen the underlying safety case for the UK ABWR.

205. Ultimately, I am satisfied that Hitachi-GE has adequately shown the UK ABWR is protected against this event, and I am further reassured by GRS's results which support the same conclusions despite the independent methods used.

4.3.4.3 Feedwater controller failure – maximum demand

206. I chose to sample this event because it is an example of a pressurisation fault. In addition, when it is analysed using US / Japanese practice, there remains a margin to the MCPR limit of 1.06. However, in Hitachi-GE's UK-practice analysis, not only does the MCPR fall beneath the MCPR limit, it has the smallest margin to the 800°C fuel cladding limit of any frequent faults which experiences a boiling transition.

207. The event involves a sudden feedwater flow increase because of a malfunction in the FDWC. The conservative assumption is that the flow instantly reaches 141% of rated flow, noting that the protective function of the reactor feedwater pumps is designed to limit flow to 136%. To pessimise the fault, Hitachi-GE has frozen the RFC and EHC.

208. The increase in feedwater flow raises the water level and the subcooling in the core, resulting in a reactor power increase. These increases are gradual so if nothing else happened, the plant would settle to a new equilibrium condition. However, to make the transient challenging, Hitachi-GE has assumed a C3 turbine trip on high RPV water level ('Level 8'). This sequentially results in a turbine trip, feedwater pump trip, main stop valve (MSV) closure and a reactor scram.

209. Hitachi-GE's transient analysis shows that the MSV closure results in a large RPV pressure rise and a reactor power spike. RPV pressure is mitigated by the SRVs opening (in the 'UK-practice' analysis, at their higher A1 passive setpoints rather than the lower C3 pneumatically actuated setpoints). The peak neutron flux predicted is 288% of rated and the MCPR falls beneath the safety limit of 1.06. The fuel cladding temperature increases due to the boiling transition, peaking at 734°C, before dropping away after the reactor scram.

210. Ref. 39 states that all acceptance criteria are met, although there is a much greater challenge to the safety margins when compared against other frequent faults. The analysis by US / Japanese practice shows the same behaviour in the initial portions of the transient, but by crediting lower C3 SRV setpoints, a trip of the RIPs and the availability of the turbine bypass, the associated pressure and neutron flux rises are less. The MCPR remains above the limit and therefore there is no significant rise in peak clad temperature.

211. GRS analysed the same transient using its ATHLET model and the conservative assumptions of Hitachi-GE's 'UK-practice' analysis (Ref. 26). It predicted similar behaviour, including a boiling transition following the drop in MCPR. Despite calculating a smaller neutron flux peak (213% compared to 288%), GRS's model predicted a peak cladding temperature of about 830°C (ie in excess of the frequent fault cladding acceptance criterion).

212. Informed by some additional sensitivity cases, GRS hypothesised that the difference in peak cladding temperature prediction could be due to an assumption by Hitachi-GE of a constant gap conductance for the region between fuel pellet and the cladding. GRS's default model (which predicted the higher temperatures) assumes the conductance in the gap varies as a function of the thermal expansion of the fuel pellet and the cladding. Turning this model off to be consistent with Hitachi-GE's approach had a significant effect on the ATHLET results, with no boiling transition or cladding heat up predicted.

213. I put this observation to Hitachi-GE in the form of an RQ, and asked it to justify its cladding temperature model. In the RQ response (Ref. 75), Hitachi-GE has explained the basis for its historical constant gap conductance model and presented results from its own sensitivity calculations. They show only that assuming a dynamic gap conductance model has only a limited impact on its calculations.

214. I am satisfied for the purposes of GDA that Hitachi-GE has considered the challenge posed to its results by GRS's independent modelling and reviewed the basis for its own modelling accordingly (Ref. 75). All computer models have some uncertainty associated with them, and GRS's results performed over a few months and supported by only a limited amount of design-specific validation, do not invalidate Hitachi-GE's long-established methodology. My judgement, based on all the analysis performed, is that there is little margin to the 800°C acceptance limit and the uncertainty associated with predicted peak cladding temperature is a similar size to that margin. However, despite the 800°C acceptance limit being a key aspect of Hitachi-GE's safety case logic for frequent faults, I see no safety benefit in demanding greater sophistication and benchmarking of the modelling for the following reasons:

- the frequent fault 800°C acceptance limit is conservative and exceeding it slightly does not automatically result in a major fault escalation (see Section 4.3.3);
- there are many other aspects of Hitachi-GE's modelling and analysis assumptions for this fault which are unambiguously conservative;
- there remains significant margin to the established 1200°C temperature limit for protecting against fuel failures;
- even if there was some consequential fuel damage, the RPV and PCV are intact for these events, and there will be negligible on-site and off-site radiological consequences (see Section 4.9);
- the feedwater controller failure is a limiting fault. Other non-LOCA transients have more margin to the acceptance limit and therefore more refined modelling of peak cladding temperature will not benefit their safety case arguments;
- if there is no boiling transition, there is no cladding heat up and therefore no concern about the uncertainty in the cladding heat up modelling. There are 'real' engineered systems (albeit Class 3) included within the UK ABWR design which are shown by conservative analysis to be effective in maintaining a margin to the MCPR limit.

215. In addition to the challenge this event poses to Hitachi-GE's declared acceptance criteria, I have also considered the expectation set out in SAP ERC.3 (Ref. 5) that changes in coolant condition and coolant voiding in normal operation and fault conditions should not cause uncontrollably large or rapid increases in reactivity. The analysis for this event does show a rapid increase in reactivity (a peak neutron flux up to 288% of rated) however I am satisfied that it is not uncontrollably large (the Class 1 SSCs can respond before any fuel is damaged). ERC.3 also states (in the context of reactor stability in normal operation) that the consequences of any adverse change (in this case, the feedwater controller failure) should be limited. Given that the US / Japanese analysis crediting Class 3 SSCs shows a margin to the MCPR limit, I am content that the UK ABWR is consistent with this expectation.

216. In conclusion, I am cautious about Hitachi-GE's prediction for the peak cladding temperature for this fault. However, for the purposes of GDA, I am satisfied that the UK ABWR design is robust for this limiting frequent fault, and resolving the residual uncertainty in the analysis is unlikely to have a measurable effect of nuclear safety.

4.3.4.4 Generator load rejection with failure of all bypass valves.

217. I chose to sample this event because I was keen to understand the behaviour of a direct cycle reactor design where the turbine is directly connected to the reactor. It is also very similar to other isolation events (eg, turbine trip, loss of main condenser vacuum, LOOP) but it subjects the plant to a very slightly more onerous sequence of events. The insights from review of this fault can therefore be applied to others.

218. In a 'real' event, when the generator load rejection occurs, the turbine control valves (TCVs) close rapidly when a power load unbalance is detected with the turbine generator and the reactor subsequently scrams. Four of the ten RIPs trip (prompted by the TCV closure), and the turbine bypass valves (TBVs) open to mitigate a rise in RPV pressure. The SRVs would open when the RPV pressure reaches the C3 pneumatic actuated setpoints.

219. In the DBA, the reactor scrams on the closure of the TCVs but no credit is taken for the TBVs opening and the RIP trip function. The RFC is assumed to be frozen and the EHC is not important given the nature of the initiating event and the assumptions made on TBVs.

220. The transient analysis in Ref. 39 shows that the reactor power rapidly increases due to the RPV pressure increase caused by the TCV rapid closure following the load

rejection. The scram limits neutron flux and surface heat flux to 269% and 118% of rated value respectively. The SRVs (assumed to open at the higher setpoints of their A1 spring-loaded operational mode) limit the reactor pressure increase to 8.46 MPa (gauge). These actions are insufficient to prevent the MCPR falling beneath the 1.06 safety limit and the fuel cladding temperature does increase. However, this peaks at 624°C, which is below the 800°C limit for fuel damage.

221. In the equivalent analysis reported in Ref. 39 following US/Japanese practice, credit is taken for RIP trip function and the SRVs are assumed to open at their lower C3 setpoints. The resulting transient is essentially the same but the neutron flux and surface heat flux are limited to 199% and 108% respectively. The MCPR stays above the safety limit.

222. GRS analysed the generator load rejection event without bypass with its ATHLET code coupled to its COCOSYS containment model (Ref. 24). In its 'reference calculation' it was able to show good agreement with Hitachi-GE transient analysis, and predicted no acceptance criteria would be violated. It did predict a lower initial power transient than Hitachi-GE, which resulted in the MCPR staying above the safety limit and no increase in peak cladding temperature. This was attributed to a lower void reactivity feedback being assumed in GRS's analysis, which prompted it to perform sensitivity studies using a revised reactivity coefficient derived from the three dimensional (3D) core model developed by GRS with the QUABOX/CUBBOX code (Ref. 76). In this way, GRS was able to match the neutron flux peak of Hitachi-GE and predict a boiling transition. However, as with the feedwater controller fault modelling, its predictions for the peak cladding temperature increase were greater than those of Hitachi-GE (in excess of the 800°C limit for fuel damage).

223. The conclusions I have reached from GRS's independent confirmatory analysis are similar to those reached for the feedwater controller fault. Hitachi-GE's long established plant transient analysis method is supported by GRS's analysis, if no boiling transition is predicted. Historically, this has always been demonstrated by US/Japanese analysis, and it remains the case for the majority of the frequent faults analysed, even when more onerous assumptions are made on the correct performance of Class 3 SSCs. The GRS analysis does inject some doubt into Hitachi-GE's predictions of increases in peak cladding temperature which are vital for demonstrating compliance with the applicable acceptance criteria for frequent faults when the MCPR limit is not met.

224. The same mitigating factors that I identified for the feedwater controller fault also apply. However, GRS's analysis also identified a further conservatism in Hitachi-GE's analysis associated with the MS line length. The power peak of concern in this fault is caused by the pressure wave which travels down the MS line from the closed TCVs to the RPV. The insertion of the CRs limits the size of this peak and I am satisfied it does not constitute an unacceptable challenge to the expectation of SAP ERC.3 for uncontrollably large increases in reactivity to be avoided. Hitachi-GE has assumed a relatively short MS line, based on the layout of the Japanese reference plants. A longer MS line is likely for a UK plant. Through its analysis, GRS demonstrated that a longer MS line would result in it taking longer for the pressure wave to reach the RPV, and therefore power peak generated could be lower when the CRs enter the core.

225. Informed by this insight from GRS, I asked Hitachi-GE through an RQ to investigate the size of this conservatism, and crucially to establish if there are any constraints on the length of the MS lines that should be considered in site-specific UK ABWR developments. In its response (Ref. 75), Hitachi-GE demonstrated that there was a small sensitivity to its modelling when following UK-practice, with a slightly lower peak cladding temperature being predicted. The effect was more significant on the analysis following US / Japanese practice, because the RIP trip function is effective in reducing the reactor's power before the pressure wave arrives, and therefore the ΔMCPR

experienced during the transient is significantly reduced (from a value which already did not challenge MCPR safety limit). Hitachi-GE therefore recommends that the MS line length assumed in the GDA calculations establishes a minimum length for site-specific layouts, and longer lengths are expected to result in increased safety margins.

226. Given that the MS line length is a parameter that impacts the reactor DBA and it is something that is in the control of the licensee during the early stages of site development (but then will be fixed for the operational life of the reactor), I do consider it important that any fault studies implications are taken into account when finalising the site layout. I have therefore raised the following assessment finding:

- AF-ABWR-FS-05: ONR's GDA fault studies assessment has established that some of Hitachi-GE's reactor transient analyses are potentially sensitive to the assumed length of the main steam (MS) lines. The licensee shall ensure that any decisions on the length of the MS lines made for the final site specific design take appropriate cognisance of the impact on reactor fault studies, as part of wider evaluations to ensure design choices reduce risks to be ALARP.

4.3.5 Reactivity faults involving the CRs

227. Following the review of design basis events undertaken in Ref. 38, Hitachi-GE has identified a need to analyse the consequences of the following limiting reactivity faults involving CRs:

- CR withdrawal error at reactor startup
- CR withdrawal error at power
- CR drop
- All CR insertion at power.

228. Its analyses for all these faults are summarised in Attachment B of Ref. 39. Additional details are provided in Ref. 77 for the CR withdrawal error at power fault, and Ref. 78 for the all CR insertion fault.

229. The CR drop is associated with a mechanical failure and has been categorised as an infrequent event. The other faults are all associated with either a procedural error by the operator or a malfunction in the B3 rod control information C&I system (RCIS), and therefore have generally been categorised as frequent faults (for CR withdrawal errors at power, different combinations of withdrawals have been considered with differing frequencies). The starting expectation for frequent faults is that there are at least two means of protecting against the fault; an A1 means which should ensure the onerous frequent fault acceptance criteria are met, and an A2 means which can ensure the slightly relaxed infrequent fault acceptance criteria are met (assuming a CCF of the A1 protection).

230. In the following sub-sections, I have considered each of these faults in turn.

231. Hitachi-GE has also identified a need to consider CR faults during shutdown operating states. My assessment of the safety case for these faults is reported separately in Section 4.4.7.

232. It should be noted that relevant parallel assessments on detecting reactivity abnormalities have also been performed in the fuel and core design and C&I assessment areas (Refs 71 and 79). The fuel and core assessment has considered the adequacy of the core monitoring and protection instrumentation coverage, while the C&I assessment has reviewed appropriateness of the instrumentation design and architecture.

233. All the faults have been analysed with similar methods. The 3D PANACEA code has been used to predict the changes in reactor power, core reactivity, and fuel enthalpy from large surveys of potential CR faults. If a boiling transition is predicted by PANACEA for a specific scenario, the TRACG code has been used to reanalyse that case in more detail.

234. The adequacy of the PANACEA code has been assessed outside of this report in the fuel and core topic area (Ref. 71). Discussion on the adequacy of TRACG is provided in Section 4.8.2 of this report.

4.3.5.1 CR withdrawal error at reactor startup

235. For many reactor faults, it is usually bounding to analyse the resulting transient from rated power. However, in the case of the CR withdrawal faults, a transient from rated power can have different characteristics from an equivalent fault during startup. If a withdrawal error occurs during startup, there is limited thermal feedback and the result is a rapid transient, hopefully quickly responded to by the available protection. This contrasts to faults at power, where thermal feedback counteracts the inserted reactivity and can lead to a prolonged transient that takes longer to reach protection setpoints. It is therefore appropriate that Hitachi-GE has separated out its analysis.

236. The most basic form of this accident is a continual withdrawal of the CR group when the reactor comes critical. As the CR(s) erroneously withdraw, the reactor period gets shorter, leading to scram from the A1 start-up range neutron monitor (SRNM) period short protection. Protection is also provided if necessary by the A1 average power range monitor (APRM) which could prompt a scram on high neutron flux, should that setpoint be reached first.[17]

237. In principle, detection of high RPV pressure by the HWBS also provides diverse A2 protection for this fault. This would initiate SLC boron injection to terminate the event (in other words, it would effectively become an ATWS event). However, Hitachi-GE has demonstrated in Attachment B of Ref. 39 that void-Doppler reactivity feedback coupled with the correct operation of the SRVs will result in the conditions for an automatic HWBS response not being met. It goes on to show that the infrequent fault acceptance criteria can be met without the automatic response (the fault schedule assumes a manual actuation of diverse scram systems after 30 minutes). I am content with this demonstration and I have not considered the need for diverse protection further.

238. The analysis to demonstrate the effectiveness of the A1 protection considers six core states: BOC, middle of cycle (MOC) and EOC for the both an initial core and an equilibrium core. Four starting temperatures representing conditions that could occur between cold shutdown to start-up has also been considered. I am satisfied that this represents a reasonable survey of the potential conditions the UK ABWR could be in prior to a CR withdrawal fault during startup.

239. Hitachi-GE has applied a proprietary three-step process to identify limiting CR withdrawal faults and assess their consequences. The first step uses the PANACEA code to identify potentially challenging CR group withdrawal patterns for further analysis. This approach and the screening criterion applied are only briefly described in Hitachi-GE's submission. However, I am satisfied that this is a reasonable approach which should be effective in identifying the CRs with the highest worth.

240. Those CR groups identified in the first stage of the process are taken forward to a second stage involving analysis with a simplified model, which assumes an adiabatic boundary condition at the fuel cladding (again using PANACEA). This assumption is intended to give a bounding estimate of the fuel's enthalpy increase. Finally, the most

[17] *Before the SRNM's setpoint for a scram is reached, a lower setpoint prompts a block of further CR withdrawals. However, this is not claimed in the DBA.*

limiting scenarios are modelled using a full 3D TRACG model which can account for thermal hydraulic feedback.

241. In my judgement, this three-stage process is adequate for GDA. It is a systematic and rigorous method for identifying limiting scenarios for further analysis, and I consider the 3D TRACG model used for the last stage to be suitable for modelling of CR withdrawal transients. I note that for the limiting scenarios taken all the way through the three-stage process, the 'realistic' TRACG modelling predicts lower fuel enthalpy rises than the adiabatic assumption made in the second stage. This provides me with added reassurance on the conservatism in the second-stage screening process and confidence that the most limiting scenarios are being considered.

242. I do view it to be an old-fashioned approach, established when computing time for transients was a more significant consideration than it is now. A future licensee may want to consider analysing a greater range of candidate faults directly with a 3D model to provide a clearer line of argument. Perhaps linked to the age of the methodology and its long-standing acceptance by overseas regulators as an approved analysis route, the approach it is not well described in Hitachi-GE's submission. Attachment B of Ref. 39 gives the impression it is summarising the results of analysis by an already discussed and approved methodology. However, no references are provided to any additional sources of information. Therefore, despite my positive judgement on its adequacy for GDA, there are improvements that could be made in future safety cases.

243. Amongst the analysis assumptions which are only described in a limited manner is the starting power. The analysis using the 3D TRACG model assumes that the faults start at around [redacted] of rated power. In a response to a RQ (Ref. 80), Hitachi-GE stated that this value was chosen to maximise the enthalpy release in the fuel during the transient. I challenged Hitachi-GE further to justify this value, observing that CR withdrawal errors starting from lower powers could result in higher rates of reactivity increase but could be below the sensitivity range of the SRNM. Ultimately I received an adequate response which explained how sensitivity studies on Japanese ABWRs had informed the choice of starting conditions (Ref. 81). However, it represents an example of how the discussion which accompanies the analysis results could be improved.

244. As another example of potential future improvements, there is limited description and justification of the severity of the RCIS malfunction or operator error assumed. It is apparent the CRs are assumed to be in the process of being withdrawn following a rule-based sequence at the point at which the fault occurs (ie they continue to be withdrawn beyond the desired point). This includes a limitation on the number of CRs being withdrawn as a group during startup to 26. These assumptions have merit, they result in the most likely manifestations of a fault being considered, and probably encompass the most challenging transients in terms of detecting a problem before fuel damage occurs. However, the rules and constraints on rod withdrawal are all managed by the B3 C&I system RCIS. Attachment B of Ref. 39 provides no justification for why CR withdrawal events during startup involving more than 26 CRs should be excluded from the analysis, therefore I have raised the following assessment finding:

- AF-ABWR-FS-06: To address limitations in the level of detail and justifications provided in GDA submissions, the licensee shall review and update the UK ABWR safety case to demonstrate that control rod (CR) withdrawal faults during startup, caused by malfunctions in the Class 3 rod control and information system (RCIS) and involving a greater number of CRs than is permitted by the standard withdrawal sequence controls, have adequate protection.

245. Despite these caveats on the scope and accompanying explanation of the analysis, I am satisfied that Hitachi-GE has demonstrated effectiveness of the A1 SRNM short period scram for an extensive survey of potential CR withdrawal events. For all the

cases considered, the scram is shown to be initiated before the point of prompt critical reactivity insertion, and therefore the rise in reactor power and enthalpy are too small to cause a failure in fuel cladding (the frequent fault acceptance criterion of relevance). When taken together with the analysis showing tolerable plant conditions even if the A1 scram is assumed to fail, it is my judgement that the UK ABWR has adequate protection for CR withdrawal error at reactor startup faults (subject to the resolution of the assessment finding in future safety cases).

4.3.5.2 CR withdrawal error at power

246. The UK ABWR design has a number of features to protect against CR withdrawal faults at power, caused either by operator error or a malfunction in the RCIS:

- a rod block monitor (RBM) stops further CR withdrawal if the local power near the withdrawn rod reaches a prescribed level;
- an alarm on high neutron flux is initiated by the APRM to alert the operator;
- an alarm on high neutron flux is initiated by the local power monitor (LPRM) near the withdrawn rod to alert the operator.
- procedures require the operators to check local thermal parameters at every step of a withdrawal.

247. However, none of these measures are formally claimed in the design basis safety case and the fault schedule. The formal claims are on:

- an automatic A1 scram initiated by the detection of high neutron flux or simulated high thermal power by the APRM;
- an automatic A2 initiation of a recirculation pump trip, feedwater stop and SLCS/ARI initiation on detection of high RPV pressure;
- in cases where the transient is not severe enough to reach the setpoints of the automatic A1 or A2 SSCs, a manual initiation is assumed, after an appropriate amount of time.

248. The methodology used by Hitachi-GE to demonstrate the effectiveness of these measures is similar to that used for CR withdrawals during startup. A range of CR withdrawal errors are considered, for both the initial core and an equilibrium core, and at different points in the operational cycle. The analysis is done in stages, firstly a screening analysis is performed with the PANACEA code, and then TRACG is used to model the limiting sequences predicted by the PANACEA code.

249. It is my view that the description of the methodology and the limited discussion of key analysis assumptions provided in Attachment B of Ref. 39 have the same shortfalls as those identified for the equivalent faults during startup. It is effectively only providing a summary of the analysis, assuming the methodology followed has been established and accepted elsewhere. However, the reporting of at power faults is accompanied with a separate, more detailed report (Ref. 77). In a superior way to what is provided for startup faults, Ref. 77 does the following:

- Systematically discusses the initiating events it is considering and their potential causes.
- Details the types of events that could occur (single or multiple withdrawals, within a CR gang group or outside of normal patterns) and categorises them as frequent or infrequent faults.
- Describes the available protection.
- Defines the acceptance criteria to be considered in the analysis
- Briefly summarises the methodology, aided by a flow chart and figures illustrating the pattern of CRs withdrawals considered in different analysis cases.
- Summarises the initial reactor conditions assumed in the analysis.

- Provides results of analysis modelling the unmitigated consequences of the erroneous withdrawal of one or two CRs, with the purpose of identifying if fuel failures are predicted. For unmitigated more severe CR withdrawal events, an assumption of consequential fuel failures is made without reference to analysis.
- Informed by the unmitigated consequences analysis and frequency categorisation applied, it identifies the number of protective SSCs required and the necessary classification. For the most severe scenarios, A1 and A2 protection is required. For some of the less severe cases involving just one or two CRs, only C3 protection is required.
- Presents the results of PANACEA and TRACG analyses for the cases identified as needing A1 and / or A2 protection. It shows that all applicable acceptance criteria are met.
- For completeness, it provides analysis showing the effectiveness of the C3 RBM.[18]

250. Based on a review of Ref. 77, I am satisfied that Hitachi-GE has comprehensively considered a range of CR withdrawal faults to demonstrate that sufficient protection is provided and that it is effective. Although its analysis tools are long-established, Hitachi-GE has applied them in a new way to substantiate the new safety case claims made for the UK ABWR that result from following its own guidance (Refs. 53 and 54). By following its own guidance for DBA, it is straight forward for me to make a positive comparison against the requirements of the SAPs (FA.4 to FA.8).

251. As part of my GDA Step 4 interactions with Hitachi-GE on this topic, I asked through an RQ for further justification of its analysis assumption that the C3 automatic power regulator (APR) is frozen. The APR can maintain power by adjusting recirculating flow or CR positions (other than fault CRs). If it continued to operate during the fault transient, the power rise caused by the withdrawal would be reduced, potentially delaying or preventing APRM scram. I wanted to understand if this could allow a more significant radial distortion of the core's power profile. Hitachi-GE supplied a useful qualitative response to the RQ (Ref. 82). It discusses what would happen if the APR is assumed to operate during the modelled transients. The APR would reduce the reactor core flow to maintain the reactor at rated power despite the injection of reactivity caused by the CR withdrawal. If reactivity insertion from the CR withdrawal is sufficiently large, the APR would eventually be deactivated on reaching the low flow boundary of the power / flow operational map. Any continuing reactivity insertion would result in a power rise and scram. The TRACG analysis has been performed assuming the reactor is at the minimum core flow permitted by the operational map for rated power, while also assuming a conservative maximum linear heat generation rate that bounds what would be expected if the APR was operating (if core flow is reduced by the APR, the steam void increases and power is suppressed).

252. Ideally this response would be fully integrated into the safety case discussion in Attachment B of Ref. 39 and Ref. 77, and supported by analysis to substantiate its assertions. However, I am satisfied with the engineered protection included within the UK ABWR design. I judge it to be highly unlikely any further analysis of the assumptions on APR operation will result in any design modifications and therefore I am content that the totality of the information provided is adequate for GDA.

4.3.5.3 CR drop fault

253. Attachment B of Ref. 39 describes a number of design features included in the UK ABWR to limit the likelihood and consequences of a CR separating from the FMCRD. However, a CR drop remains a fault which is analysed within the DBA. The

[18] *The RBM can be credited in safety analysis following typical US / Japanese practice. As a result, Hitachi-GE has access to an established methodology which demonstrates the effectiveness of RBM for a range of CR movements and statepoints in the operating cycle.*

consequence of the CR separating and falling out of the core is a power rise. A feature of this event, which makes it different from the other CR faults considered, is the speed with which the CR moves. The assumed drop velocity (limited by a hollow piston design) is 700 mm/s. This compares with the normal CR FMCRD withdrawal speed of 33 mm/s.

254. The fault schedule (Ref. 38) and Attachment B of Ref. 39 both identify an A1 scram initiated by the short reactor period signal of the SRNM or the neutron flux high signal of the APRM as the notional protection for this fault. However, Hitachi-GE's analysis takes no credit for the negative reactivity caused by the scram of the CRs. Instead it models (with PANACEA and TRACG) the power suppression caused by the Doppler effect to show that there is no significant power increase or enthalpy rise which could challenge the integrity of the fuel cladding.

255. To maximise the consequences of the CR drop, the reactor is assumed to be at or near to criticality. In the analysis, the power is assumed to be [redacted] core flow is [redacted] of rated, and the fuel cladding surface temperature is [redacted]. Cases have been analysed assuming temperatures of 20, 100, 160 and 286°C. As with other CR faults, cases at BOC, MOC and EOC, for both the initial core and equilibrium core, have been considered.

256. During startup, CRs are likely to be moving in gang mode. It is unlikely that CRs would be moved in the available single CR withdrawing mode. However, the reactivity insertion caused by a CR drop will be larger for the latter scenario, so faults in both modes of CR control have been analysed.

257. Assuming gang mode operation, the bounding results demonstrate that no prompt critical reactivity insertion is predicted and the power rise is too small to challenge the fuel cladding. Assuming the single CR mode, the limiting case predicts larger power increases and enthalpy rises but infrequent fault acceptance criteria for the fuel are not challenged.

258. Based on my review of Attachment B of Ref. 39, I am satisfied that Hitachi-GE has undertaken comprehensive analysis to demonstrate the tolerance of the UK ABWR design to CR drop faults. A similar criticism to that made on other CR faults can be made about the limited depth and detail provided in supplied reports on the methodology followed and some of the analysis assumptions made. There is no discussion, for example, of the importance of the CR and hollow piston design in limiting the severity of the transient and whether this is an evolution from earlier BWR designs which may not have had the same tolerance of CR drop faults. However, the conclusions Hitachi-GE is making from the results of its comprehensive analysis are clearly stated. While I am content that the analysis itself is adequate for GDA, it is my view that there could be worthwhile improvements made to future safety case documentation.

4.3.5.4 All CR insertion fault

259. In normal operation, the CRs are moved in staggered, limited movements as groups. During a scram, they are hydraulically inserted together (and quickly), backed-up by the slower electric drive mechanism of the FMCRD. The electrically-driven insertion of the CRs is controlled by the Class 3 RCIS. The safety concern is that a failure in the RCIS could result in the CRs being spuriously driven in (slowly), resulting in excessive local power peaking in the upper parts of the core. The reduction in power due to the insertion of the CRs is accompanied by a reduction of voids in the upper part of the core, followed by a large increase in reactivity. This could cause fuel to fail.

260. There are long-standing counter measures included in the ABWR design to protect against such an occurrence:

- If a FMCRD run-in signal is generated, the control system will also send a run-back signal to the RIPs, decelerating them to their minimum speed.
- Unless the prompt for CR insertion has come from a scram or ARI signal, the control system moves the CRs in four groups (sequentially with time intervals).

261. Both of these methods should be effective in limiting the local power peaking and preventing fuel failures. However, both are either delivered by the RCIS or require signals from the RCIS, and therefore neither can be assumed to be available if the expectations of SAP FA.6 for DBA are to be met.

262. Hitachi-GE recognised this shortfall against UK expectations as part of its systematic review of design basis initiating events (Ref. 38) and identified the slow insertion of all the CRs as a new event to be considered. The outcome of this consideration is summarised in Ref. 39. However, significantly more detail is provided in Ref. 78 and it is this reference which has been the basis for my assessment. Ref. 78 does the following:

- Describes the safety concern with the all CRs inserted fault.
- Describes the RCIS system in which the initiating event originates.
- Defines the limiting event to be considered.
- Identifies the applicable acceptance criteria.
- Summarises the assumed analysis conditions (for example, rated power and pressure, CR insertion speed). It was also stated that BOC, MOC and EOC statepoints for both an initial core and an equilibrium core have been considered.
- Presents analysis of the unmitigated consequences of a slow all CRs inserted fault. PANACEA has been used to generate normalised core axial power shapes, illustrating the distortion in the upper core as the rods insert. TRACG analysis has been used to predict when the conditions for extensive pellet cladding interaction (PCI) and stress corrosion cracking (SCC) fuel cladding failures are reached and the likely extent of any fuel damage.
- Given that an all CR inserted fault is assumed to be a frequent fault (the initiating event being a failure of a Class 3 system), it states that the dose consequences for the unmitigated event (>100 mSv) establish a starting expectation for A1 and A2 protection.
- It provides some additional context for the unmitigated consequences case. It discusses how the off-site dose could be limited by a combination of existing A1 protection and passive C3 components. The PCI cladding failures would trigger a high radiation signal on the MS radiation monitor and prompt the closure of the MSIVs. This action would limit the time during which activity is reaching the condenser to five seconds, and restrict the predicted off-site releases (via the stack) to 120 mSv. However, according to Hitachi-GE's categorisation and classification scheme (Ref. 54), this level of off-site dose still requires additional engineered protection.
- It discusses how in a 'real' event the release from the stack, via the condenser, would be significantly reduced by the C3 offgas system. While it is basically a passive system, the offgas system does need steam to operate. When the MSIVs close, the direct steam supply is lost. However, the UK ABWR is equipped with a 'house boiler' which can be manually started from the main control room. Assuming this action could be completed in 30 minutes, the off-site dose could be reduced to 0.12 mSv.
- Informed by the unmitigated consequences analysis, an optioneering process to identify what additional engineered measures are reasonably practicable is described in detail. Ways to prevent the all CRs inserted fault occurring and to protect against the consequences are both considered. Two candidate changes are identified:

  - an A1 rod block function provided by a hardwired system that is diverse from the RCIS;
  - an A1 axial-peaking power range monitor (A-PPRM) added to the SSLC and capable of triggering a scram.
- The A-PPRM is stated to be the favoured option (although both are considered to be credible) and PANACEA analysis is reported to show that a reactor scram triggered when an axial power difference of 140% is detected will be effective in preventing fuel damage. Additional analysis is presented to show that such a setpoint would not be prohibitive for normal power operations and startup / shutdown procedures.
- It states that despite the predicted unmitigated consequences and the assumed frequency of the initiating event, no diverse A2 means of protecting against the fault will be pursued because the end point of all the CRs being inserted is an inevitable shutdown.

263. The conclusion of Ref. 78 is that there are effective, implementable countermeasures available, and these will be developed further during the site-specific design phase. It is also stated that ways to improve the assumed initiating event frequency will be pursued in later phases of the project (it is currently claimed to be 1×10^{-2} failures per year, based on the safety classification of the RCIS but with no consideration of the RCIS architecture).

264. I judge Hitachi-GE's conclusions and the endpoint to be reasonable for GDA. The work presented in Ref. 78 that supports these conclusions is clear, systematic and logical. Its own safety case principles and deterministic rules are followed to identify an initial expectation for the level of engineered protection which should be provided. This expectation is consistent with my own views (informed by the SAPs). Hitachi-GE has not ignored this expectation but has used it as a starting point to establish what it is reasonably practicable to provide. The selection of the A-PPRM as the favoured option is a judgement by Hitachi-GE, but the basis for that judgement is well documented.

265. I am also content with the argument that diverse A2 protection is not reasonably practicable. It is my view that while the initiation in the Class 3 RCIS of an all CR insertion event is a frequent fault, there are lots of design features included within the UK ABWR design (albeit not A1 or A2, and some not independent of the RCIS) which will reduce significantly the frequency of a large radioactive release as a result of the initiating event. Noting that the end-point of the fault transient is a shutdown reactor, I am satisfied that these extant measures, when combined with a design change to add a new A1 measure, do support a claim that risks have been reduced ALARP without an extra A2 SSC.

266. As a result, based upon my review of Ref. 78, I am satisfied for GDA that the UK ABWR will be provided with adequate protection for an all CR insertion fault.

4.3.6 Hitachi-GE's analysis to demonstrate that stable, safe state can be reached following a non-LOCA fault

267. Hitachi-GE's systematic fault-by-fault analysis of non-LOCA events in Attachments A and B in Ref. 39 appropriately focuses on the reactivity challenges in the initial few seconds of each transient. However, SAP FA.8 establishes an expectation that the design basis safety case should demonstrate that safety measures are capable of bringing a nuclear facility to a stable, safe state.

268. The fault schedule in Ref. 38 claims that through the use of the A1 SRVs and a single division of ECCS, the RPV water level can be controlled (FSF-2) and long term cooling can be provided (FSF-3) until the plant reaches cold shutdown. These claims were not substantiated by any analysis in early submissions to ONR. In addition, the fault schedule identifies several manual operations which are required to reach cold

shutdown. SAP FA.6 does not preclude manual actions being claimed within the design basis, but it sets an expectation that for demonstrations to be provided to show that sufficient time is available to identify the need for a required action and perform all the necessary tasks. For these reasons, I asked Hitachi-GE to provide additional analysis within its safety case documentation to support the claims it has made on reaching cold shutdown.

269. The requested analysis is provided in Attachment G of Ref. 39. From the starting point of an assumed isolation event, a reactor scram, RPV pressure control through the A1 SRVs functionality, and the successful automatic initiation of at least one division of high pressure ECCS injection (ie a controlled hot shutdown state), the report explains how cold shutdown can be achieved through A1 measures (manual depressurisation with two SRVs and the RHR successively being used in LPFL mode, S/P cooling mode and finally shutdown cooling mode). Three different scenarios are described:

- all three divisions of ECCS are available (the likely scenario following a design basis isolation event);
- only Division II or Division III ECCS is available (high pressure injection provided by the HPCF);
- only Division I ECCS is available (high pressure injection provided by the RCIC).

270. Hitachi-GE has identified the final scenario as the limiting case to analyse because the RCIC becomes unavailable to maintain the water RPV water level as the reactor is depressurised (in contrast with the HPCF pumps which can still operate at low pressures). This means that the Division I RHR has more functions to deliver in such circumstances. The following operations are identified (starting from the controlled hot shutdown state):

- once the S/P temperature passes over 49°C, the operator manually starts the RHR in S/P cooling mode;
- with the S/P temperature lowered, the operator switches the RHR back to LPFL mode to restore water level;
- the operator initiates a rapid depressurisation of the RPV by manually opening two SRVs;
- once the RPV pressure is less than 0.93 MPa (gauge), the operator switches the RHR from LPFL mode to shutdown cooling mode, taking the reactor to cold shutdown.

271. Ref. 39 reports a base case analysis for the above, undertaken with the SHEX code, to demonstrate that the S/P water temperature does not exceed the design basis criterion of 104°C before shutdown cooling mode is initiated (at which point the reactor's decay heat is being directly removed from the RPV rather than being rejected into the S/P). Assuming an appropriate 'two sigma' decay heat curve, a rapid depressurisation with two SRVs, and an hour's delay in switching from LPFL mode to shutdown cooling mode once the RPV water level has been fully restored, the maximum S/P water temperature is predicted to be 89°C.[19]

272. Ref. 39 goes onto to provide a range of sensitivities to demonstrate what deviations in operator actions can be tolerated before the S/P water temperature limit will be challenged. The following were considered (relative to the base case assumption):

- delays of up to 4.5 hours in initiating RPV depressurisation;

[19] *The analysis assumes operator switches the mode of the RHR to shutdown cooling once the RPV water level has been restored to 'Level 8'. By this time, RPV pressure is predicted to be approximately 0.34 MPa (well inside the pressure window for starting shutdown cooling). If the HPCF or another RHR is available to maintain water levels, shutdown cooling could be initiated earlier.*

- delays of up to 90 minutes in switching over from LPFL mode to shutdown cooling mode (in addition to the one hour delay in the base case);
- combinations of delays for initiating RPV depressurisation and starting shutdown cooling;
- depressurisation rates of 10, 25 and 55°C / hour;
- S/P initial temperatures 15, 20 and 25°C higher than the base case assumption of 35°C.

273. I am satisfied that through all this analysis, Hitachi-GE has adequately demonstrated that a single division of ECCS and manual depressurisation of the RPV with two SRVs can bring the UK ABWR to a safe stable state following an isolation fault. It will be for a future licensee to develop definitive procedures for taking the plant to cold shutdown following an isolation fault (whether that is with three divisions available or just one). The necessary operator actions will need to be substantiated once these are developed, and I would expect the thermal hydraulic analysis discussed above to be reviewed or repeated to demonstrate that the procedures are effective. However, I consider this to be all part of normal business for site licensing. For the purposes of GDA, it is my judgement that sensitivities illustrate that there is plenty of time to perform the necessary actions, and substantiating them in the future should not be a problem.

4.3.7 LOCA faults

274. As stated in Section 4.3.1 above, Hitachi-GE has broken its evaluation of LOCA faults in Operating State A into several discrete parts:

- Attachment C of Ref. 39 details the short-term analysis (hundreds of seconds) of small, medium and large break LOCAs within containment, considering the RPV water levels and the integrity of the fuel cladding through use of the LAMB, TASC and SAFER computer codes.
- Attachment C of Ref. 39 also details the short-term analysis for two breaks (MS line and FDW line) outside of containment. Again, it considers the RPV water levels and the integrity of the fuel cladding through use of the LAMB, TASC and SAFER computer codes.
- Attachment D of Ref. 39 details the short-term (tens of seconds) and long-term (hours) pressure and temperature responses in the PCV following in-containment feedwater line breaks and main steam line breaks (the limiting faults for containment performance). The M3CPT code is used for short-term behaviour and SHEX for the long-term behaviour.

275. I have broken my assessment of LOCAs up in a similar manner. In the following sub-sections I have in turn considered the analysis for in-containment LOCAs, outside containment LOCAs, and the containment performance. I also report the insights I have gained from commissioning GRS to perform independent confirmatory analysis of a sample of LOCA faults. Because GRS has used a modern ‘best-estimate’ thermal hydraulic code coupled to a containment code, it can use the same analysis route to look at all parts of a transient. I have therefore kept my TSC insights together, even though they are applicable to different parts of Hitachi-GE’s dispersed methodology.

276. General comments on the adequacy of Hitachi-GE’s computer codes and methods are given later in this report in Section 4.8.2.

277. It should be noted that Ref. 39 restricts itself to presenting the thermal hydraulic analysis for guillotine breaks in various pipes connecting to the RPV. The link to the wider safety case for LOCA faults is provided by PCSR Chapter 24 (Ref. 29). It explains that as a general rule the pipework within the containment is Class 1, although runs of pipe as they leave the containment may be lower (justified by the consequences of their failure). The justification for the applied safety classifications,

and the resulting codes and standards applied which ensure the assumed failure rates and severities are provided in PCSR Chapter 7 (internal hazards, Ref. 83) and Chapter 8 (structural integrity, Ref.84). The assessment of the claims, arguments and evidence in these chapters is beyond the scope of this report, and it is assumed they have been assessed by the relevant ONR specialists as they judge appropriate.

278. A feature of the UK ABWR design which is not discussed in great detail in Ref. 39 but which I do acknowledge is that the break flow for most of the LOCA faults considered is limited by flow limiters, nozzles at the RPV or sparger nozzles. A summary table in Attachment C of Ref. 39 demonstrates that Hitachi-GE has used these design features to limit the amount of flow lost through breaks but their importance to achieving acceptable results is not expanded upon in the fault studies documentation.

279. The fault schedule (Ref. 38) claims that all considered pipe breaks (inside or outside of containment) are infrequent (<1 x 10^{-3} per year), apart from small (instrument) line breaks which are not a challenge to RPV or PCV acceptance criteria. No frequencies are presented in the fault schedule to support these claims however inspection of the LOCA initiating event frequencies in Ref. 85 shows that DBA event categories are consistent with the assumptions made in the PSA.[20]

4.3.7.1 LOCAs inside containment (short-term analysis)

280. Attachment C of Ref. 39 presents analysis for the following events:

- Small LOCA inside PCV
  - RPV bottom drain line break
- Medium LOCA inside PCV
  - HPCF line break
  - LPFL line break
- Large LOCA inside PCV
  - FDW line break
  - MS line break
  - RHR outlet line break.

281. The designation of small or medium LOCA does not appear to have any specific implications. For large LOCAs there is a difference; for these events Hitachi-GE makes no claims on the ADS because the break is big enough to reduce the RPV pressure enough for low pressure injection on its own. All the faults have been assessed against the same infrequent fault acceptance criteria. Hitachi-GE has modelled a complete guillotine break of actual lines (which vary in size) that are part of the pressure reactor pressure boundary. This contrasts to common practice on pressurised water reactor (PWR) LOCA modelling, where 'break spectrum analysis' is often performed considering a range of break/hole sizes in a large pipe, assuming the break to be in the most challenging part of the circuit. I judge Hitachi-GE's approach to be appropriate; the UK ABWR does not have large 'hot-legs' and 'cold-legs' connected to steam generators. In addition, which line on the UK ABWR experiences the break is an important factor in how the event transient proceeds and which SSCs are available to respond to the loss of inventory. I also observe that the cases considered do represent a reasonable spectrum of break sizes.

282. Ahead of presenting the transient analysis, Ref. 39 systematically reviews each potential break location and the resulting ECCS availability to deliver the short-term cooling function (FSF-2). It does this twice, firstly just assuming a single failure in addition to consequential losses due to the break, and secondly assuming a single failure and an ECCS division being unavailable due to maintenance. I consider this to

[20] *Inadvertent opening of a SRV, which can be considered a form of LOCA, has been assessed as a frequent fault in Attachment A of Ref. 39*

be a comprehensive and powerful demonstration that the expectations of SAP FA.6 have been met.

283. At this point in time (ie during GDA), it has not been established if a future UK ABWR operator will want or need to undertake planned maintenance on a division of ECCS (or an essential support system to a division of the ECCS) in Operating State A. Japanese ABWR practice is not to do such maintenance. Crucially, this GDA analysis does demonstrate that maintenance unavailability can be tolerated, giving the licensee valuable flexibility. However, this has only been possible because of a design change (relative to the Japanese reference plant). In LPFL mode, each division of the RHR draws water from the S/P, passes it through the RHR heat exchanger, and injects it into the RPV outside the core shroud. RHR Division I is arranged to inject water via the FDW line 'A'. Divisions II and III inject via dedicated low pressure lines into the RPV. In the event of a LOCA in FDW line 'A', and if limiting single failures and maintenance assumptions are made on the availability of Divisions II and III ECCS safety injection, the only remaining system on the reference plant would be the RCIC. This will initially be effective in compensating for water inventory lost through the break but as the RPV depressurises, it cannot be relied upon (see Section 5.1.1.2 of Ref. 86). As a result, to prevent the loss of the core cooling function by the ECCS, in the UK ABWR the Division I LPFL is provided with a bypass line which allows it to inject coolant into the RPV through FDW line 'B'. The break of FDW line 'A' is detected automatically by measuring differential pressure between the two lines, and the valve opening signal is sent to the bypass line injection valve (to FDW line B) instead of the injection valve (to FDW line A).

284. It was crucial for Hitachi-GE to make this design change to allow it to substantiate its 'N+2' claim for LOCA faults (along with another design change to increase the capacity of the RHR heat exchangers). I strongly welcome these design changes, firstly because of the flexibility it will offer the licensee, and secondly because I judge it to be an excellent example of the systematic application of design basis principles as established in SAPs FA.6, FA.8 and FA.9.

285. In addition to the availability assumptions, Ref. 39 adequately captures in tabular and (in the case of pump performance) graphical form the multiple other analysis assumptions made for the short term LOCA analysis. Other information, including discussion of the transient behaviour is extremely limited. PCSR Chapter 24 (Ref. 29) does improve on this slightly for the limiting HPCF LOCA.[21] My general observation is that the quality of safety case discussion for LOCA faults (including for containment performance which I will comment on later) is not high. I judge it to be inferior to that provided for non-LOCA faults. This is disappointing for such an important group of faults. However, building upon several extensive discussions with Hitachi-GE during the course of GDA, and through my own examination of the transient analysis results presented in Ref. 29, I am content that there is enough information provided for me to assess the adequacy of the UK ABWR design.

286. With the exception of the MS line break (which involves gas-phase piping rather than water-phase piping), the LOCA transients are all very similar:

- At zero seconds, an instantaneous double-ended break of a pipe is assumed. The RPV water level drops to 'Level 3', prompting a scram. A consequential LOOP is assumed, resulting in all the RIPs being lost and a rapid decrease in core flow.
- At around 1 second, the MCPR falls beneath the 1.06 safety limit and boiling transition occurs. The resulting drop in heat transfer from the fuel cladding to

[21] *Hitachi-GE argues that the HPCF LOCA is limiting. It has predicted a similar peak cladding temperature for all the LOCA faults analysed however the HPCF fault sees the biggest drop in coolant inventory before the ECCS recovers the water level.*

the coolant causes the peak cladding temperature to rise. For all the breaks modelled, the action of the scram limits the predicted peaks to ~640°.

- The water level continues to drop. A few minutes into the transient, low water 'Level 1.5' is reached, prompting available RCIC and HPCF systems to start, and MSIV closure to be initiated.
- Assuming the water level continues to drop (for smaller breaks, with full availability of high pressure ECCS, this may not happen), at 'Level 1' (typically tens of seconds after 'Level 1.5' has been reached) the LPFL receives a signal to start and ADS actuation is initiated (on a 30 second delay, assuming high dry well pressure has also been detected). Note, ADS actuation is not assumed for the large FDW line LOCA or the RHR outlet line LOCA.
- A few hundreds of seconds into the transient, LPFL injection starts and the water level starts to recover. Hitachi-GE typically terminates this part of its LOCA analysis at 500 seconds, with the RPV water level increasing.

287. The MS line break transient is slightly different. The double-ended break within the containment prompts MSIV closure on a high steam flow signal, which in turn results in a reactor scram. A boiling transition occurs within circa 1 second and the action of the scram limits the peak cladding temperature increases to ~640°C. Significantly, the steam-driven RCIC is assumed not be available for this event. ADS operation is also not credited for this large LOCA event. The water level passes through 'Level 1.5' and then quickly down to 'Level 1'. Depending on the limiting single failure and maintenance assumptions made, any available HPCF system will get a signal to start at 'Level 1.5' but there is insufficient time for injection to start and prevent 'Level 1' being reached. The LPFL is initiated at 'Level 1'. It, and any available HPCF, recovers the water level.

288. I am satisfied for all the LOCAs considered that this short-term analysis demonstrates that all fuel acceptance criteria are met, even when making conservative assumptions about the availability of ECCS divisions. It is notable that the increase in fuel cladding temperature occurs in the initial few seconds of the transient is short-lived, and is much lower than the 1200°C limit applied for infrequent faults. It occurs due to the boiling transition, not because of prolonged fuel uncovery. Earlier in this report, I identified some uncertainty in Hitachi-GE's ODYN / TASC modelling of peak cladding temperature in circumstances where the MCPR safety limit was not maintained. For these LOCA analyses where SAFER has been used to predict the peak cladding temperature, I am not concerned about the impact of similar uncertainties on the safety case arguments presented by Hitachi-GE:

- There is a much larger margin between the predicted peak cladding temperature and the infrequent fault temperature limit of 1200°C considered in this fault, than there is in the non-LOCA analysis which considers the more onerous 800°C limit for frequent faults.
- In a 'real' LOCA, there would not be an instantaneous guillotine break, LOOP, initiation of reactor scram and loss of all RIPs. In addition, the MG-sets would slow the decrease in core flow. Taken together, these factors should reduce the predicted increase in fuel cladding temperature.

4.3.7.2 LOCAs outside containment (short-term analysis)

289. Attachment C of Ref. 39 presents analysis for the following events:[22]

- MS line break outside PCV
- FDW line break outside PCV

[22] *Attachment C of Ref. 39 acknowledges that a third 'outside of containment' LOCA event is identified in the fault schedule: reactor water clean-up line break. However, the consequences for the reactor are bounded by the two events analysed. The radiological consequences to people of this event (and from smaller instrument line breaks) are assessed in Attachment F of Ref. 39. I have no concerns with this approach.*

290. Hitachi-GE has used the same methods and assumptions as those used for inside containment breaks, including on limiting ECCS single failure and maintenance availability. There are however some significant differences in the protection for these events, how the transient proceeds, and the radiological consequences.

MS line break outside of PCV

291. For the MS line break outside of containment, the first few seconds of the transient are very similar to that discussed above for the equivalent in-containment fault. A guillotine break occurs at time zero. This is assumed to be accompanied by a LOOP, a rapid detection of high steam flow, a prompt for MSIV closure, and then a reactor scram. Boiling transition occurs but the scram limits the fuel cladding temperature increases to around 640°C.

292. After this point, the transient deviates from the in-containment equivalent. Once the MSIVs are closed after five seconds, the RPV is effectively isolated from the break. However, steam is still being generated by the reactor and the RPV pressure gradually increases until SRV setpoints are reached at around 80 seconds. The SRVs keep opening and closing to release steam but this action results in a reduction in RPV water level. After 200 seconds, the low water 'Level 1.5' is reached, which is used to prompt the initiation of the available high pressure ECCS injection (unlike the in-containment fault, the steam-driven RCIC remains available when the break is downstream of closed MSIVs).

293. I am satisfied that the analysis for the MS line break in Attachment C of Ref. 39 demonstrates that the UK ABWR is tolerant to this challenging fault. However, as stated for in-containment LOCAs, the accompanying discussion is very limited and I have had to draw my own conclusions about how the analysis supports and links into the safety case. The following (generally positive) observations about the adequacy of the UK ABWR are my own:

- It is very important to demonstrate an adequate safety case for this fault because it has the potential for a large amount of radioactive steam to bypass the containment.
- A vital aspect of the UK ABWR *design* is that it has two MSIVs on each of the four MS lines (one inside of containment and one outside). This arrangement is single failure tolerant (and no maintenance can be performed on the MSIVs in Operating State A). As long one MSIV on each of the MS lines closes, the challenging part of this transient is limited to a few seconds (see Figure 2).
- A vital aspect of the UK ABWR *analysis* is that it shows there is no consequential fuel damage as a result of the early (post-boiling transition) cladding heat up. Therefore, the radiological consequences of the event are a function of the pre-fault activity in the circuit (relatively low, mainly activation products rather than fission products), an additional spike term from pinhole failures driven by the pressure drop, and the duration of the steam release (five seconds).
- Even if the initial failure of a MS line caused consequential damage to adjacent MS lines (an issue considered in the internal hazards topic area), the reactor scram and MSIV closure should occur on the same timescales, resulting in consequences for the reactor that are very similar to those predicted for the base-case single break scenario. Given that the four MS lines eventually connect through a common-header ahead of the turbine, the assumptions made on the mass of steam released in the radiological consequences analysis would also be largely unchanged.
- By closing the MSIVs, the RCIC remains available to manage RPV water level. Only one division of high pressure ECCS is needed, so this event can tolerate both a limiting single failure and a division being unavailable due to planned maintenance.

294. PCSR Chapter 24 (Ref. 29) does provide some welcome additional explanations and comments to that given in Attachment C of Ref. 39. It crucially provides a link to the radiological consequences analysis presented in Attachment F of Ref. 39. I will comment on the adequacy of this radiological consequences analysis in Section 4.9 of this report. However, it is important to appreciate at this point in my assessment that this fault (and specifically this short-term portion of the transient analysis for the fault) is key to determining the limiting condition for operation (LCO) defined in the generic Technical Specifications for pre-fault radioactivity levels in the circuit. My judgement on the adequacy of this specific piece of analysis is relevant to almost every other DBA reactor fault, because ultimately I link most of my conclusions back to Numerical Target 4 in the SAPs (Ref. 5). Hitachi-GE claims that for all design basis reactor faults, there is no consequential fuel damage. Therefore, the radiological consequences from an event are linked to the pre-fault LCO source term. If the LCO source term is not valid, then comparisons against Numerical Target 4 have little value.

295. During the course of GDA Step 4, I pointed out to Hitachi-GE that a break smaller than a complete guillotine break in a MS line might result in the break being un-isolated for longer before a high steam flow is detected (in some cases, the high steam flow setpoint may never be reached). While the resulting transient will be less onerous for the fuel in the reactor, the total release of radioactivity could be greater. Through Appendices added to Attachments C and F of Ref. 39, I am satisfied that Hitachi-GE has addressed this concern. Additional prompts for MSIV closure have been identified, different integrated steam and water masses leaving the RPV have been calculated, and revised dose calculations performed. Ultimately, Attachment F of Ref. 39 concludes that the original complete guillotine break event is the limiting fault for determining the pre-fault circuit activity LCO. I agree with this conclusion.

FDW line break outside PCV

296. An important aspect of design to protect against a FDW line break outside primary containment is the provision of check valves at the PCV boundary which stop reactor coolant being discharged outside of containment. Therefore, if there is at least one division of high pressure ECCS available, the event is effectively the same as the non-LOCA loss of all feedwater flow fault (in terms of ensuring the continuing integrity of the fuel, there are different radiological consequences to people). As a result, Hitachi-GE does not present any additional analysis in Attachment C of Ref. 39 for scenarios where a single failure of an ECCS division is all that is assumed. However, it has recognised that if ECCS maintenance is permitted during Operating State A, normal design basis assumptions could result in no high pressure ECCS injection being available to respond to a FDW line(B) break (the RCIC connects to FDW line (B), maintenance and single failures could leave the two divisions of HPCF unavailable). The LPFL would be the only means of providing the FSF-2 fuel cooling function.

297. The ‘standard’ design logic requires both low water RPV levels and high D/W pressures to initiate an ADS signal. In the case of the FDW line break outside of containment, a high D/W pressure will not be detected, and the LPFL would be ineffective while the RPV remains at high pressure. The possibility of such a scenario was identified by Hitachi-GE prior to entering GDA and a feature called ‘Transient ADS’ has always been included within the UK ABWR’s C&I logic for beyond design basis events. This prompts the SRVs providing the ADS functionality to open after a 10 minute delay from the low water ‘Level 1’ setpoint being reached. What has changed during the course of GDA fault studies interactions is recognition that a complete unavailability of all high pressure ECCS is a design basis event if maintenance of a division is allowed for. a result, the ‘Transient ADS’ function has been defined as ‘A1’ rather than ‘B2’, and the Class 1 SSLC has been modified accordingly to provide this capability. I welcome this change, and consider in another good example of Hitachi-GE rigorously applying of design basis approaches, as set out in SAP FA.6 and FA.9 (Ref. 5).

4.3.7.3 PCV response to LOCAs

298. The result of a LOCA inside containment is that a steam-water mixture is released into the D/W. Vent pipes connect the D/W to the S/P. These transmit the released steam from the D/W to the water of the S/P, where it is condensed.

299. The objective of the PCV performance analysis presented in Attachment D of Ref. 39 is to show that the calculated pressures and temperatures do not exceed design values. These design values are established in PCSR Chapter 13 (Ref. 34). The maximum pressures and temperatures in the D/W occur in the first few seconds of the transient. Therefore, Hitachi-GE's short-term analysis only considers the first two hundred seconds of the transient and neglects ECCS injection as a conservatism. The gas temperatures and pressures in the W/W also peak in the first tens of seconds of the transient, however it takes hours for the S/P water temperature to reach its peak. Therefore, Hitachi-GE extends the duration of its long-term analysis accordingly, assuming a single division of ECCS (HPCF and RHR) is operating (the other two divisions are assumed to be unavailable due to a limiting single failure and maintenance). After 30 minutes, it is assumed that the RHR is put into S/P cooling mode with the associated heat exchanger being credited. After about 7 hours, the RHR heat exchanger can match the energy being deposited in the S/P and the water temperature stops rising (at which point, Hitachi-GE terminates its analysis).

300. The UK ABWR is equipped with a containment spray system, linked to two out of the three RHR pumps and heat exchangers. Although this functionality is provided for these types of events, early on in GDA, Hitachi-GE took the decision not to claim containment spray in its DBA to simplify its arguments to demonstrate an 'N+2' capability. I understand the rationale for this decision and recognise it as an additional conservatism within the analysis that could be relevant to ALARP judgements. The containment spray is assumed in PSA modelling.

301. With regards to other assumptions, it is my judgement that Attachment D of Ref. 39 provides an adequate summary of what has been modelled in the analysis, and I consider them to be appropriate for DBA modelling. As part of my interactions with Hitachi-GE, I asked for supporting references for LOCA analysis and was provided with a GE-Hitachi (Hitachi-GE's sister-company and contractor for DBA) safety analysis report (Ref. 87). Inspection of this report revealed that Attachment D is providing a summary of the text in Ref. 87, but the original source reference is a superior place to look for more information on the modelling and the origins of parameters. Significantly, what Ref. 87 demonstrates to me is that Hitachi-GE's PCV modelling methodology is actually a well-established and well-controlled US methodology, modified to support the conservative assumptions made in the UK ABWR DBA safety case.

302. Table 4 summarises the bounding temperature and pressure values calculated from the considered MS line and FDW line LOCAs. Inspection of these results leads me to the following observations:

- There is little margin between design values and calculated values. In the case of D/W temperature, the stated design value is exceeded.
- While the lack of margin is not ideal, I do recognise that the analysis contains many conservative assumptions, and exceeding the design values does not result in a 'cliff-edge' failure of the PCV.[23] The objective of defining conservative acceptance criteria is to show that if you are <u>at</u> or below them, safety is assured.

[23] *Analysis performed in support of the PSA (Ref. 88) shows that overpressure failure in the upper flange area of the PCV is not likely to occur until twice the design pressure and at temperatures of 300°C.*

- I accept Hitachi-GE's argument that it is acceptable for the D/W (gas) temperature following a MS line break to exceed D/W design parameter for circa one second very early on in the transient because D/W structural materials will remain below the design temperature. It is the temperature of the PCV liner and concrete that is important for maintaining containment, not the gas temperature.

303. On the last point, it is my view that the PCV temperature acceptance criteria assumed in the UK ABWR safety case should be reviewed and potentially refined in the future. I recognise that the extant criteria were developed to be consistent with the output of the associated analysis route. It adopts a very basic nodalisation for gas spaces in the D/W and W/W (a single node for each), but with some of the less onerous availability assumptions made in US/Japanese practice, it has previously been possible to make positive comparisons between results and the criteria without adding caveats about what they represented. With the margins eroded in the UK ABWR analysis, it rapidly becomes obvious that the temperatures immediately adjacent to the break in the initial period of the transient will be different from those in an area on the other side of the reactor. Similarly, the temperature of the PCV structure (locally and on average) will be different from the gas temperature, especially over a short period of time. The extant temperature criteria do not have any time, location, average, gas or structure specifications associated with them. This issue is illustrated in the next subsection where the independent TSC analysis I commissioned adopted a more refined nodalisation of the PCV volume and structure. I will discuss a similar issue associated with extended SBO events in Section 4.3.8. As a result, I have raised the following assessment finding:

- AF-ABWR-FS-07: As a result of changes made during GDA to meet UK relevant good practice, Hitachi-GE's 'traditional' analysis methodology was not able to demonstrate simple compliance with long-established primary containment vessel (PCV) design limits, without calling on additional calculations and discussion. The licensee shall review the design basis acceptance criteria defined for dry well (D/W) and wet well (W/W) temperatures in the GDA safety case and ensure there is no ambiguity on what needs to be demonstrated in any future safety case analysis to provide the necessary assurances that PCV integrity will be maintained in fault conditions.

4.3.7.4 Independent Confirmatory Analysis

304. The validation evidence to demonstrate the adequacy of Hitachi-GE's codes and methods used to assess LOCA faults has been commented on in Section 4.8.2 of this report. As a parallel exercise, I also commissioned GRS to perform independent confirmatory analysis of three LOCA faults (inside PCV) to gain additional insights into the issues associated with these events and further assurance on Hitachi-GE's conclusions.

305. Using its ATHLET thermal hydraulic code coupled to its COCOSYS containment code, GRS has analysed (Ref. 25):

- HPCF break (short-term fuel and RPV considerations)
- FDW line break (short-term fuel and RPV considerations, PCV pressures and temperatures)
- MS line break (short-term fuel and RPV considerations, PCV pressures and temperatures).

306. As stated previously, GRS's computer codes are capable of modelling all aspects of the transient and do not need to break the analysis up into a series of discrete parts using different methods.

307. Despite the differences in approach, GRS's results for the HPCF break are generally comparable with Hitachi-GE's and support the safety case conclusions. The timing of key events in the fault sequence are similar, and both sets of calculations predict the peak cladding temperature to occur in the very early period of the transient, associated with the boiling transition (and not with an extended period of fuel uncovery). Consistent with results of the non-LOCA analysis discussed in Section 4.3.4 above, GRS's prediction of peak cladding temperature is higher than Hitachi-GE's. While it would be useful to gain additional confidence in Hitachi-GE's peak cladding temperature modelling, in both Hitachi-GE's and GRS's calculations there remains a large margin to the 1200°C infrequent fault safety limit. In addition, as stated in Section 4.3.7.1, in a 'real' event the reduction in core flow is likely to be less severe than that assumed in the analysis.

308. For both FDW line break and the MS line break, GRS struggled to produce results for the fuel and RPV that were as severe as Hitachi-GE's (which is supportive of a conclusion that Hitachi-GE's modelling is conservative). A boiling transition was not predicted in the early portion of the transients, meaning that no significant fuel cladding temperature rises were predicted. The time at which the conditions for LPFL injection are reached is delayed by a few minutes in the GRS calculations compared to Hitachi-GE's, but this does not have a significant effect on meeting acceptance criteria.

309. The major observation from the extended analyses looking at the PCV performance has already been mentioned in association with assessment finding AF-ABWR-FS-07. With the finer nodalisation used in GRS's COCOSYS model, peak D/W temperatures in the vicinity of the two breaks considered are predicted to be above the design temperatures set out in Table 4 for several minutes. Despite this, the maximum predicted temperature for the containment structure is around 130°C. Given that Ref. 88 demonstrates that containment failure is expected to occur at structure temperatures greater than 300°C and at twice the design pressure, I am satisfied these results do not undermine Hitachi-GE's design basis claim that the containment will remain intact during these events.

310. GRS's predictions for the other PCV parameters (as identified in Table 4) are generally smaller than Hitachi-GE's, again supporting the argument that Hitachi-GE's analysis is conservative and therefore appropriate for DBA.

4.3.7.5 Conclusions on LOCA analysis

311. I am satisfied that Hitachi-GE has demonstrated through conservative analysis that a single division of ECCS is adequate to manage the full range of LOCAs identified, and this supports its claim that the UK ABWR has a 'N+2' capability. Compliance with appropriate acceptance criteria for infrequent faults has been shown, and this conclusion is supported by the independent confirmatory analysis I have commissioned.

312. I have raised an assessment finding on the definition of PCV temperature limits. As currently defined, there are some examples of the predicted D/W local gas temperatures exceeding the declared limit. I accept Hitachi-GE's arguments as to why this does not mean the PCV will fail, but this should be clarified and demonstrated in future safety cases, in part through more specific criteria.

313. Attachments C and D of Ref. 39 do adequately capture the key assumptions made in the analysis. Further improvements could be made to ensure that all the qualities of a good safety case document established in TAG NS-TAST-GD-051 (Ref. 13) are demonstrated. Even when Ref. 39 is read in conjunction with PCSR Chapter 24 (Ref. 29) and the fault schedule (Ref. 38), it is more difficult than it should be to gain an appreciation of the LOCA safety case. Ultimately though, it is my judgement that robust

safety arguments have been made (throughout the totality of the safety case documentation) that are sufficient for GDA.

4.3.8 Short and medium-term SBO events.

314. The possibility of a LOOP is widely recognised by nuclear power plant designers as an event that needs to be protected against. The UK ABWR is no exception to this, and it is provided with three redundant and physically separated A1 EDGs (supported by fuel supplies for seven days) to ensure there is sufficient ac power available for all necessary safety functions to take the reactor to a stable, safe state. However, to address the requirements of ONR's RO-ABWR-009 (Ref. 49), and in accordance with its own safety case principles set out in Refs 53 and 54, Hitachi-GE has recognised in the fault schedule (Ref. 38) that it needs to consider, as an infrequent design basis fault, a frequent LOOP in combination with a CCF of the EDGs. Such events are commonly called SBOs.

315. Ref. 38 identifies two SBOs which meet the frequency requirements of a design basis event:

- a short-term LOOP lasting up to two hours with a CCF of the EDGs
- a medium-term LOOP lasting up to 24 hours with a CCF of the EDGs.

316. Both events initially proceed in the same way. A reactor scram is initiated by the LOOP, most likely from a monitored parameter on the turbine (eg 'turbine control valve fast closure' or 'turbine stop valve closure') or from a reduction in RPV water level caused by the loss of feedwater or RIP flow. An uninterruptable dc supply ensures the scram function remains available despite the loss of ac power.

317. The A1 steam-driven RCIC and the passive spring-loaded SRVs remain available to deliver the short-term FSF-2 fuel cooling function for both events. The RCIC is claimed in the DBA safety case to have a 'coping time' of eight hours (as a post-Fukushima severe accident resilience measure, it has been shown to be effective for up to 24 hours, but this is not a design basis assumption). It is therefore more than sufficient for managing an SBO which lasts up to two hours. On the return of ac power (either from the grid or an EDG), the operator can manually depressurise the RPV using two SRVs and take the plant to a cold shutdown state using one or more of the restored RHRs.

318. It is important to note that the reliance on the single train RCIC for design basis SBO faults puts constraints on when planned maintenance can be performed on it while the reactor is at power. Hitachi-GE has substantiated its 'N+2' claim on the ECCS for LOCA faults. This has the potential to provide UK ABWR operators with additional flexibility in when they perform maintenance on EDGs or the HPCF. However, the SBO analysis and associated fault schedule entry (Ref. 38) assumes the RCIC is never deliberately made unavailable. Given that the RCIC is not reliant of ac power or active cooling, this constraint does not necessarily apply to all the A1 SSCs in Division 1.

319. If the SBO extends beyond two hours, the operators will need to take action to establish low pressure water injection into the RPV before the RCIC's eight hour coping time expires. In the design basis safety case, the claim is that the B/B with its diverse air-cooled diesel generators remains available to power A2 FLSS low pressure water injection. As with short-term SBO, the operators need to manually depressurise the RPV sufficiently for the FLSS to inject. During the course of GDA Step 4, Hitachi-GE established that the battery capacity to the A1 control system used to open two SRVs will not be sufficient to support this operation during an extended event. However, after making a design change to increase SRV accumulator capacity, Hitachi-GE state that the supported A2 RDCF SRV valves will remain available and controllable, as they are supported by the B/B power supplies.

320. Once the RPV is depressurised, the FLSS can take over the role of cooling fuel in the RPV from the RCIC. The generated steam is condensed in the S/P, however this can only be a temporary heat sink for decay heat if there is no active RHR heat removal from the containment. Therefore, the eventual claim in the UK ABWR fault schedule for an extended SBO is that the PCV will be vented to atmosphere to reject the heat (FSF-3). The design basis safety case assumption is that the event, including venting, is terminated by the restoration of ac power and the RHR after 24 hours.

321. Hitachi-GE provides conservative DBA to demonstrate the effectiveness of claimed SSCs for a medium-term SBO in Ref. 40. Despite the differences in the fault schedule claims between the different duration events, it does not provide any analysis explicitly for the short-term SBO. I judge this to be a reasonable approach to take:

- The immediate challenge to the fuel of a loss of ac power prior to the scram has been demonstrated for all related events in the LOOP analysis in Attachment A of Ref. 39.
- The effectiveness of a single division of RHR to take the reactor from hot shutdown to cold shutdown following a non-LOCA fault has been demonstrated in Attachment G of Ref. 39.
- The behaviour of the RPV water level, S/P temperature etc for the full duration of the assumed short-term SBO transient is identical to the first two hours of the 24 hour medium-term SBO transient analysed in Ref. 40.

322. Hitachi-GE has used the SAFER code to model the thermal hydraulic behaviour of the core, the RCIC / FLSS injection and the RPV water level during the medium-term SBO. The SHEX code has been used to analyse the containment pressure and temperature. Four different cases have been run, cognisant of the following considerations:

- The act of depressurising the RPV to facilitate low pressure injection will eventually take the RCIC out of operation (the one system that is known to be operating to cool the reactor). The decision of when to start depressurising the RPV should therefore be taken knowing the availability status of low pressure injection systems (RHR, FLSS or FLSR).
- If there is early confidence that low pressure injection is available, a controlled depressurisation consistent with the generic Technical Specification advised cooldown rate of <55°C/hour can be initiated after four hours. This would take about 1.6 hours to reach FLSS injection pressure. [24]
- If it took longer to establish the availability of low pressure systems, a more rapid depressurisation may be needed to ensure FLSS injection is ready to take over at the end of the RCIC's eight hour coping time. The limiting scenario would be a rapid depressurisation at eight hours. This would take about 10 minutes to reach FLSS injection pressure.
- For a design basis event, it is assumed the operators will initiate containment venting once the PCV design pressure of 310 kPa (gauge) is reached (if they are satisfied there is no significant fuel damage and they are not having a severe accident). If the pressure reached twice design pressure and manual venting had not been initiated, the rupture disc of the passive containment overpressure protection system (COPS) is designed to open, resulting in venting through the filtered FCVS route (the severe accident assumption).

323. The resulting four cases are:

- medium-term SBO with a controlled depressurisation (55°C/hour) initiated at four hours. Containment venting at 310 kPa (gauge);

[24] *Limits of < 55°C/hour are established for reactor coolant system heatup and cooldown temperature rates for normal operation in the generic Technical Specifications, and are consistent with the assumption made in RPV thermal cycle design calculations. However, they are not design basis requirements. Another advantage of a slow depressurisation rate is that it allows a controlled transfer of water injection from the RCIC to the FLSS operating at its maximum pressure.*

- medium-term SBO with a rapid depressurisation initiated at four hours. Containment venting at 310 kPa (gauge);
- medium-term SBO with a rapid depressurisation initiated at eight hours. Containment venting at 310 kPa (gauge); and
- medium-term SBO with a rapid depressurisation initiated at eight hours. Containment venting at 620 kPa (gauge), ie just before the COPS opens.

324. I am satisfied that the first three of these are appropriate sequences to consider as part of the design basis safety case. I also note that they are consistent with assumptions made in the PSA for non-core damage states. I consider the fourth case to be a sensible sensitivity to run for demonstrating that there are no cliff-edge concerns associated with the timing of venting.

325. The analysis for all cases does not predict any problems with respect to fuel acceptance criteria or managing water levels. Unsurprisingly, if the operator does vent the containment at 310 kPa (gauge), the analyses show that the D/W and W/W design pressure of 310 kPa (gauge) is not exceeded. The timing of venting is shown to be insensitive to the depressurisation rate; 12.8 hours is predicted for all three DBA sequences. The fourth case predicts that 620 kPa (gauge) would be reached at 19.7 hours.

326. In all cases, the peak D/W and W/W temperatures exceed the ‘traditional’ design values Hitachi-GE sets out in PCSR Chapter 13 (Ref. 34) and has applied in, for example, its LOCA analysis (see Table 4). With reference to containment performance analysis work undertaken to support the PSA (Ref. 88), Hitachi-GE states in Ref. 40 that the PCV boundary can be assumed to be maintained if temperatures are less than 200°C at pressures up to 620 kPa. It is my judgement that this revised limit should be acceptable for DBA (Ref. 88 shows that the PCV failure in D/W upper flange area is not expected below 300°C at 620 kPa), however all the concerns I raised in Section 4.3.7.3 on LOCA acceptance criteria that resulted in assessment finding AF-ABWR-FS-07 still apply:

- The simple nodalisation used in SHEX is predicting an average gas temperature, but it is most likely that a local temperature in the PCV structure (the flange in the D/W upper head region) that is important for failure.
- There are no time limits imposed on the acceptable durations of high temperatures. For LOCA faults, high D/W temperatures only last a few seconds. For these extended SBO events, high temperatures are persisting for hours.

327. The analysis assumption for these design basis sequences is that ac power is restored at 24 hours into the transient, allowing RHR cooling of the S/P to be started and ending the need for containment venting. The results in Ref. 40 show that even with 11 hours of effective containment venting and two RHR divisions activated on the restoration of power, it would still take 2.5 hours to bring the S/P temperature below 100°C, and a further two hours for the RPV water to reach the same temperature (the definition of cold shutdown). I welcome the fact that Hitachi-GE has presented this information. It has not simply assumed the fault can be terminated on the restoration of power. In accordance with SAP FA.8, it has continued its analysis to demonstrate how and when a stable, safe state can be reached.

328. The analysis shows that claiming restoration of power will terminate an extended SBO event is not a trivial assumption. If power was restored immediately before or after venting commenced, the RHR would need to deal with S/P water temperatures significantly higher than the ‘traditional’ 104°C design value (up to 167°C, according to the analysis). Venting helps to stop further rises in S/P water temperature but it is not predicted to result in a significant drop in temperature. I therefore actively looked for evidence in relevant basis of safety case reports that SBO events had been

considered. I am satisfied that the basis of safety case report on containment heat removal systems (Ref. 89) identifies performance requirements on the RHR for these events. It is my judgment that the basis of safety case for the RHR (Ref. 90), specifically the section detailing the requirements for the RHR heat exchangers, does not clearly identify what is required for terminating design basis SBO events. Performance specifications above 100°C are not specified. I also observe that the transient analysis in Ref. 40 assumes two RHRs operate on the restoration of ac power but only one would be available if it was only a single EDG (or the defence-in-depth Class 3 diverse additional generator) that was started first. If it is assumed that a single RHR and heat exchanger is sufficient to bring the reactor to cold shutdown, this needs to be both demonstrated in the transient analysis and the performance specifications in Ref. 90.

329. I have established through interactions with Hitachi-GE that it recognises this shortfall in the declared RHR requirements in Ref. 90, and it has provided me with evidence that it has flagged in on a database of open issues to be passed to future licensees (Ref. 91). As a result, I am content that results of DBA for extended SBOs will be reflected in the final RHR design.

330. As part of the wider independent confirmatory analysis work, I asked GRS to model a medium-term SBO with its ATHLET code coupled to its COCOSYS containment model (Ref. 23). GRS's modelling of the reactor's behaviour and the timing of key events (up to containment venting) is consistent and generally supportive of Hitachi-GE DBA results. However, in a similar observation to those reached by the independent LOCA analysis, GRS's more detailed containment modelling predicted peak dry well temperatures which were both higher than those calculated by SHEX and the declared PCV acceptance criterion set out in PCSR Chapter 13 (Ref.34) . In contrast to LOCA events, high gas temperatures are maintained for a sustained period of time during an extended SBO and therefore the PCV structure (including the likely failure point at the PCV top flange) could also be at elevated temperatures.

331. The high temperatures in the D/W head region predicted by GRS's analysis were brought to Hitachi-GE's attention in meetings and through RQs as part of routine GDA Step 4 interactions. Hitachi-GE did two things in response to this feedback:

- It added an additional section to Ref. 40 which summarised 'hand-calculations' it performed to demonstrate that heat transferred from the RPV head region to the PCV head structure via the PCV gases in the head region will not result in temperatures which challenge the PCV head structure.
- In response to a RQ (Ref. 92), it supplied additional design details and predicted heat losses for the PCV head region to allow GRS to better model the UK ABWR.

332. Hitachi-GE's calculations in Ref. 40 predict peak D/W structural temperatures between 88°C and 113°C, depending on the assumptions made. GRS's revised containment modelling predicted D/W gas temperatures beneath the 171°C design limit, and therefore even lower structure temperatures. On their own, I am satisfied that Hitachi-GE's calculations show that the UK ABWR RPV design is adequate for conditions experienced in design basis SBO faults. I take additional reassurance by the fact that acceptable results have also been predicted by GRS's different method. I also note that Hitachi-GE's calculations, and the information it supplied to GRS, have their origins in real heat transfer data taken from operating Japanese ABWRs (during normal operations, not SBO conditions), and therefore are fully consistent with the expectations of SAP AV.2 for using where possible information validated by comparison with actual experience.

333. An important factor in limiting the temperature seen by the PCV head structure, which is taken into account in the updated analyses, is the presence of reflective metal

insulation (RMI) on the RPV head. If the RMI is not correctly installed and / or fails to maintain its integrity during the SBO event (perhaps due to ageing), much higher structural temperatures could be experienced in a fault condition. This point was not adequately captured in Hitachi-GE's initial safety case but following discussions with it on this topic, I am satisfied that the final version of Ref. 40 does the following:

- assigns a safety classification to the RMI (C3), which should ensure that its contribution to nuclear safety is appreciated throughout the operational life of a UK ABWR; and
- identifies that SFCs should be attributed to RPV RMI in future safety case documents.

334. The need to improve the visibility of the RMI in the safety case is also captured on Hitachi-GE's assumptions database which it will pass on to future licensees (Ref. 91). I am content with this endpoint for GDA.

335. GRS also investigated the effectiveness of containment venting to remove heat through its ATHLET / COCOSYS codes. The UK ABWR fault schedule (Ref. 38) takes credit for there being two ways of venting the containment (specifically from the W/W air space) during a design basis event: the unfiltered 'hardened' vent route and the FCVS. Both routes are classified A2, controlled from the A2 HWBS, and powered from the B/B (ie available in a design basis SBO). However, as a bounding analysis assumption (with regard to radiological consequences), venting is assumed to be through the unfiltered hardened route.

336. A detailed design for either venting route is not currently available. Hitachi-GE has assumed in Ref. 40 a flow rate of 57 tonnes/hour at 310 kPa(gauge) in its SHEX calculations and has shown that this is sufficient to stop S/P water temperature increases for the modelled decay heat. With its more detailed COCOSYS model, GRS used Hitachi-GE supplied geometrical data for the vent system and generic pressure losses. The resulting flow area proved to be insufficient to achieve Hitachi-GE's assumed flow rate at 310 kPa(gauge). As a result, GRS's initial calculations predicted a slower fall in W/W pressure following venting. In a sensitivity case, it increased the venting area to achieve the same flow rate as Hitachi-GE assumed. Unsurprisingly, this resulted in falls in W/W pressure consistent with Hitachi-GE's predictions. This independent analysis highlights to me a need for a future licensee to demonstrate that the final designs of the hardened venting route and FCVS (both are claimed in the fault schedule as options) are shown to be effective in reducing PCV pressure and temperature in extended SBO events. As a result, I have raised the following assessment finding:

- AF-ABWR-FS-08: In the absence of detailed design information during GDA, it was necessary for Hitachi-GE to make assumptions about achievable flow rates in its demonstrations of the effectiveness of primary containment vessel (PCV) venting in design basis fault conditions. The licensee shall demonstrate that the final designs of the unfiltered hardened vent system and filtered containment vent system are effective in reducing PCV pressure and temperature in extended station blackout (SBO) events (and other frequent reactor faults where venting is claimed as a diverse measure).

337. SAP ECS.2 sets an expectation that the principal means of fulfilling a Category A safety function in a design basis event should be Class 1. However, this infrequent event is an example of the type of fault mentioned in Section 4.2.5 where many of the required safety functions are being delivered by Class 2 systems. Hitachi-GE's UK ABWR specific guidance on categorisation and classification (Ref. 54) recognises that such situations can occur for infrequent reactor faults involving a CCF of an A1 system (in this case, a CCF of the EDGs), and argues that A2 provision is acceptable due to

the risk gap to relevant good practice being very modest. It is my judgement that this acceptable for these faults following reasons:

- The SBO fault sequences have unique aspects to them which mean they claim the A2 SSCs as the principal means of protection. The majority of the safety case claims on the same SSCs to deliver the same safety functions are as redundant backups to A1 systems or for beyond design basis events. In both cases, A2 provision in fully consistent with relevant good practice.
- For the mechanical systems claimed, the main architectural difference between A1 and A2 SSCs is the level of redundancy. However, the significant factors in their reliability to operate for these events are their diversity and independence from the EDG CCF and the SSCs which rely on them for their power. These factors would be unchanged if the SSCs were made A1.
- To depressurise the RPV to allow the FLSS to inject, Hitachi-GE has made a design change to allow the A2 RDCF SRVs to perform this action. Ref. 40 details an extended optioneering review that was undertaken before this final design detail was settled upon. This review included options involving A1 provision but these were ultimately rejected as not being ALARP. I am satisfied with the performed review and note that the A2 SRVs and accumulators delivering the safety function are physically identical to their A1 equivalents. The only difference is that they are controlled from the A2 HWBS.

338. The significant issue I have not discussed in this section is the radiological consequences of venting, especially through the unfiltered hardened route. I am satisfied that Hitachi-GE has adequately demonstrated that fuel, RPV and PCV acceptance criteria have been met. However, this has been achieved through a deliberate and extended release of activated steam to atmosphere. I will discuss in Section 4.9 how the predicted consequences from this operation compare against Numerical Target 4 in SAPs, and therefore whether containment venting is acceptable for design basis faults.

339. Of relevance to this postponed discussion is that consequential fuel damage is not predicted for all the design basis SBO events considered, and therefore the source term for the venting release is limited by the pre-fault operational LCO on circuit activity. Also of relevance is the mass of steam released. Hitachi-GE's SHEX calculations predict approximately 500 tonnes of steam would be released (Ref. 40), assuming venting starts at 310 kPa (gauge) and is then terminated at 24 hours with the restoration of ac power. This integrated steam mass release is shown to be largely independent of whether the RPV is blown down early in a controlled way, or rapidly depressurised at eight hours.

340. Delaying venting until 620 kPa (gauge) is predicted to result in 335 tonnes of steam being released. I will discuss my views on the benefits of delaying venting (and perhaps reducing the radiological consequences) against the disbenefits in Section 4.9.3.

341. GRS's predictions for the mass of steam released were broadly consistent with Hitachi-GE's. It is therefore my judgement that conclusions on the acceptability of containment venting can be reached on the basis of Hitachi-GE's SHEX predictions.

4.3.9 Hitachi-GE's analysis to demonstrate the effectiveness of the diverse means to provide FSF-2 and FSF-3 for frequent faults

342. Attachments A and G of Ref. 39 demonstrate how non-LOCA faults can be successfully managed in the short and long-term through the operation of the ECCS and the SRVs. However, Hitachi-GE recognises in PCSR Chapter 5 (Ref. 31) a need to demonstrate for frequent faults that the UK ABWR has a diverse Class 2 means of cooling available. This demonstration is provided in Attachment H of Ref. 39.

343. The fault schedule (Ref. 38) repeatedly identifies the following SSCs as the diverse means of providing the FSF-2 function for frequent reactor faults:

- Alternative SRV (RDCF) initiated by low water 'Level 1' and a timer delay
- FLSS initiated by low water 'Level 1' and a timer delay

344. Attachment H of Ref. 39 summarises analysis undertaken on two faults with the SAFER code to show that infrequent fault acceptance criteria can be met (the argument being that it is appropriate to judge the consequences of a frequent fault with a CCF of A1 SSCs against infrequent fault criteria):

- loss of all feedwater flow fault (limiting frequent faults involving decrease in RPV water level)
- feedwater controller failure - maximum demand (limiting frequent fault involving an increase in reactor power).

345. I am satisfied with the fault selections made by Hitachi-GE and the appropriateness of the acceptance criteria considered. I also judge the level of conservatism included in the calculations to be acceptable, noting the following from the list of assumptions provided in Ref. 39:

- the reactor is assumed to have been operating at 102% of rated power prior to scram;
- an initial core flow of 90% has been assumed for the loss of feedwater flow fault, 111% for the feedwater controller fault;
- an appropriately conservative decay heat curve has been used (the same as used in LOCA analysis);
- the SRVs are assumed to provide an A1 overpressure protection function at the spring loaded setpoints;
- only one of the two FLSS trains has been assumed to be operating;
- a ten minute timer delay has been assumed for the initiation of FLSS and RDCF from the low water 'Level 1' setpoint being reached.

346. The transient analyses for both events show similar behaviours. The MSIVs close when low water 'Level 1.5' is reached. This occurs earlier for the loss of feedwater flow fault given the nature of the initiating event. Generated steam is repeatedly discharged to the S/P through the SRVs and the RPV water level continues to drop but the conditions inside the RPV are relatively stable until the RDCF opens ten minutes after 'Level 1' is reached. The act of depressurising the RPV causes an initial spike in water level followed by a rapid drop. This drop is recovered by the initiation of FLSS injection. During this period of water level change, there is an increase in peak fuel cladding temperature and some local fuel oxidation, but the predications are significantly below the 1200°C and 15% clad oxidation acceptance criteria. Hitachi-GE terminates its FSF-2 analysis after 40-50 minutes, with the FLSS controlling the RPV water level and fuel temperatures.

347. I am content that these results support Hitachi-GE's claims on the effectiveness of the claimed systems non-LOCA faults.

348. Ref. 39 does not provide any direct discussion or analysis to demonstrate that there is diverse design provision for small LOCAs. While the limiting small LOCA involving a guillotine break of the A1 RPV bottom drain line is designated as an infrequent fault, the fault schedule (Ref. 38) does identify breaks in instrument lines and a spurious opening of a SRV as frequent faults. Despite a lack of specific discussion, I am satisfied that the UK ABWR has adequate protection. The size of these LOCA events is such that the Class 3 feedwater system and associated C&I should be able to maintain the RPV water level. Even if no credit is taken for the control systems, and a

CCF of the high pressure ECCS is assumed, these events are less of a challenge to the FLSS than the loss of all feedwater flow fault.

349. Another potentially challenging small LOCA scenario could be a CCF of low pressure ECCS (the RHR/LPFL) with a high pressure ECCS division out on maintenance. However, the analysis of the bounding RPV bottom drain down line break in Attachment C of Ref. 39 shows that two divisions of high pressure ECCS are sufficient to maintain the RPV water above the 'Level 1' setpoint for automatic initiation of the LPFL and ADS. The reactor would therefore stay in a controlled, high pressure state until the operator is satisfied that low pressure safety injection is available (either the LPFL or the FLSS), at which point a manual depressurisation could be performed. From this point on, the event would be less of a challenge for the FLSS than the loss of all feedwater flow fault.

350. The alternative means to the A1 RHR for providing the long-term FSF-3 identified by the fault schedule (Ref. 38) for frequent faults is containment venting.[25] Hitachi-GE has demonstrated the effectiveness of this measure in Attachment H of Ref. 39, in a variation of the SHEX SBO analysis discussed in Section 4.3.8 above.

351. To maximise the increase in PCV temperature, an inadvertent MSIV closure has been selected as the bounding fault. The FDW system is assumed to continue to supply water to the RPV (until depleted) as this is at a higher temperature than the S/P, condensate water storage tank and B/B water temperatures that could otherwise be used. The initial reactor power is assumed to be 102% rated and a conservative decay heat curve has been used. I am satisfied that all these assumptions are appropriate.

352. At four hours, the operator starts to depressurise the RPV at a controlled rate of 55°C/hour. The FLSS provides the long-term low pressure water injection. When the PCV pressure reaches 310 kPa(gauge), the operator initiates containment venting. With these assumptions, venting is initiated for this bounding event at around 11 hours (about two hours earlier than the venting time for the medium-term SBO). Despite this difference, the comparisons against temperature and pressure acceptance criteria are very similar to those made for the SBO events. Venting is effective in keeping D/W and W/W pressures below design limits, but the S/P water temperature exceeds the design temperature of 104°C and there is the potential for localised temperatures in the D/W to exceed limits if additional arguments are not made.

353. Ultimately, I judge that Hitachi-GE has demonstrated sufficiently for GDA the effectiveness of venting as a diverse means of delivering the FSF-3 function for frequent faults, subject to the discussion on the radiological consequences of venting in Section 4.9, and the resolution during site licensing of the two assessment findings identified earlier:

- AF-ABWR-FS-07: As a result of changes made during GDA to meet UK relevant good practice, Hitachi-GE's 'traditional' analysis methodology was not able to demonstrate simple compliance with long-established primary containment vessel (PCV) design limits, without calling on additional calculations and discussion. The licensee shall review the design basis acceptance criteria defined for dry well (D/W) and wet well (W/W) temperatures in the GDA safety case and ensure there is no ambiguity on what needs to be demonstrated in any future safety case analysis to provide the necessary assurances that PCV integrity will be maintained in fault conditions.

- AF-ABWR-FS-08: In the absence of detailed design information during GDA, it was necessary for Hitachi-GE to make assumptions about achievable flow

[25] *Containment venting is the means of removing heat from the containment. Low pressure safety injection, whether that is the LPFL or FLSS, still needs to be provided for the FSF-3 function to be delivered.*

rates in its demonstrations of the effectiveness of primary containment vessel (PCV) venting in design basis fault conditions. The licensee shall demonstrate that the final designs of the unfiltered hardened vent system and filtered containment vent system are effective in reducing PCV pressure and temperature in extended station blackout (SBO) events (and other frequent reactor faults where venting is claimed as a diverse measure).

4.3.10 ATWS faults demonstrating diversity in the provision of FSF-1 for frequent faults

354. The UK ABWR has a design history that includes a significant US contribution. It has therefore long-established features provided to meet the requirements on the US regulator. In the case of ATWS faults, US regulations are very specific for BWRs (Part 50.62 of Ref. 19):

- each BWR must have an ARI system that is diverse (from the reactor trip system) from sensor output to the final actuation device;
- each BWR must have a SLCS with the capability of injecting into the reactor pressure vessel a borated water solution;[26]
- each BWR must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS.

355. As a result, the UK ABWR has all these systems and is therefore consistent with the much less prescriptive expectations of SAP ECR.2 (Ref. 5) that at least two diverse systems should be provided for shutting down a civil reactor.

356. In addition to the design provision, Hitachi-GE recognised at an early point in the GDA process that it would need to demonstrate through DBA that these measures were effective for frequent faults, assuming a CCF of the A1 scram provision. However, initial submissions to ONR were limited in scope, only providing me with a fraction of the safety case claims, arguments and evidence I was looking for in GDA Step 4 to show that the UK ABWR can be brought to a stable, safe state following a design basis ATWS event.

357. The final submissions are much improved and I am satisfied that enough information has been provided for GDA. However, it is my opinion that the safety case still does not meet the highest standards established by TAG NS-TAST-GD-051 (Ref. 13) for information to be easily accessible and a clear trail to be provided from the claims to the arguments and evidence. Over the course of GDA Step 4, I have expended a significant amount of effort to build up the following ‘route-map’ through the ATWS safety case:

- The fault schedule (Ref. 38) claims for most frequent faults that the combined automatic actions of either the ‘SLCS / RPT / feedwater stop’ or the ‘ARI / RPT’ are a diverse means of delivering the FSF-1 safety function. For some faults, where the design basis transient is not onerous enough to trigger the setpoints for automatic action, manual SLCS or ARI actuation is claimed. The fault schedule goes on to present again those frequent faults which can initiate an automatic ATWS response as individual infrequent ATWS faults in their own right.
- A C&I-focused description of the SSCs identified in the fault schedule as the response to ATWS events is provided in Ref. 93.

[26] *The US regulation continues in more detail, prescribing for the SLCS that the flow rate, level of boron concentration and boron-10 isotope enrichment, and accounting for reactor pressure vessel volume, should ensure that the resulting reactivity control is at least equivalent to that resulting from injection of 86 gallons per minute of 13 weight percent sodium pentaborate decahydrate solution at the natural boron-10 isotope abundance into a 251-inch inside diameter reactor pressure vessel for a given core design. It also states that the SLCS and its injection location must be designed to perform its function in a reliable manner and that its SLCS initiation must be automatic.*

- The engineering claims and requirements for the SLCS boron injection system are provided in Ref. 94.
- The arguments and evidence to support the claim that the SLCS will be effective in providing adequate shutdown margin are provided in Ref 95.
- Attachment E of Ref. 39 presents analysis with the ODYN code to show for frequent design basis faults, assuming a CCF of the A1 scram function (and not crediting the A2 ARI scram function), that appropriate acceptance criteria for RPV pressure, PVC pressure, S/P temperature and peak fuel cladding temperature are met during the initial tens of minutes of a transient.
- In Appendices to Attachment E, sensitivity studies have been performed with the TRACG code to show that the modelling limitations and simplifications in the ODYN code are conservative. These include consideration of RPV water levels below the range of applicability of ODYN, and using a '10 Theta' model of the core to investigate the impact of the asymmetry in boron injection and mixing.
- PCSR Chapter 12 (Ref. 33) provides an additional description of the SSCs claimed for ATWS events.
- PCSR Chapter 24 (Ref. 29) provides a high level description of ATWS events and presents a single, representative piece of fault analysis extracted from Attachment E of Ref. 39. It also discusses in a section towards the end of the chapter (at a very high level) how the UK ABWR could be taken to safe shutdown state following an ATWS event.

358. These submissions are what I have considered in my assessment of ATWS faults.

359. Reflecting the dispersed nature of Hitachi-GE's safety case, I have broken my own assessment up into discrete sections.

4.3.10.1 Adequacy of the fault schedule

360. I have no objections to how ATWS events have been captured on the fault schedule, ie demonstrating that diverse means of providing the reactivity control function (FSF-1) are provided for all frequent faults, while identifying ATWS events as infrequent faults in their own right and showing what SSCs are necessary to take the UK ABWR to a safe shutdown state. This is a comprehensive approach which identifies what is considered within the design basis safety case and what SSCs are claimed (and their safety classification).

361. In the infrequent fault presentation of ATWS events in the fault schedule, the A1 ECCS and SRVs are claimed to be available to provide fuel cooling (FSF-2) and long-term heat removal (FSF-3). I consider this to be an appropriate claim to make if the reason for the ATWS is not a complete failure of the A1 SSLC C&I protection system (for example, a mechanical problem is causing a scram not to be successfully completed). However, if the fault is linked to a SSLC failure, an argument could be made that the ECCS would also not be available.

362. The fault schedule does identify the A2 RDCF SRVs, FLSS and containment venting as non-claimed defence-in-depth measures. These have been demonstrated in Attachment H of Ref. 39 as being capable of taking the plant to a stable, safe state for the limiting non-LOCA frequent faults (see Section 4.3.9). If the SSLC is the cause of a frequent fault escalating to an ATWS event, there is no reason why the A2 ARI will not be effective in inserting the CRs, and from that point on, the transient will be same as those considered in Attachment H of Ref. 39. I therefore have no concerns about the UK ABWR's engineering provision for providing cooling for these events, and my observation that the fault schedule is only claiming the A1 ECCS is a minor, presentational issue.

4.3.10.2 High level adequacy of the ATWS systems

363. While PCSR Chapter 12 (Ref. 33) provides design descriptions of some of the SSCs claimed for ATWS events in the fault schedule, and PCSR Chapter 24 gives a brief description (supplemented with tables and a figure) of the ATWS SSCs, the best description I have found for the individual ATWS SSCs / functions and how they act together as single ATWS system is in Ref. 93.

364. First of all, Ref. 93 is clear about the objectives and requirements for the C&I delivering the ATWS functions:

- the ATWS system is a backup system for the A1 main shutdown system (the reactor trip protection system portion of the SSLC), and should be independent, isolated and diverse from it;
- the system is categorised as A2;
- it utilises the hardwired technology of the HWBS. This meets the A2 requirement and is diverse from the complex digital technology of the SSLC; and
- the power source for the HWBS and the other parts of the ATWS system is the Class 2 B/B power suppy.

365. It identifies four functions that need to be delivered (in the design basis safety case) in response to an ATWS event:

- ATWS Recirculation pump trip function (ATWS-RPT)
- Alternate rod insertion function (ARI)
- Standby liquid control system (SLCS) initiation function
- Feedwater stop function (FDWSTP)

366. It also states that as a backup to the ARI function, the ATWS system also prompts the FMCRD to run in the CRs. However, the FMCRDs are C3 SSCs and this provision is not claimed in the safety case.

367. It defines the SSCs which make up the ATWS system:

- detectors for reactor water level low (Level-2 and Level-3) and reactor pressure high,
- ATWS logic circuit panels,
- manual ARI operation buttons,
- ARI exhaust valves,
- ATWS-RPT circuit breakers
- feedwater stop valves,
- the SLCS.

368. It states that when the ATWS function activation conditions are satisfied (low water level, high reactor pressure, and high power despite a scram signal, or manual activation), the ATWS logic circuit panel sends signals to the RIP power supply circuit breaker, RIP adjustable speed drives, and the ARI exhaust valves to activate the ATWS-RPT and the ARI. Additionally, signals are also sent to SLCS and FDW with appropriate time delay. A non-claimed signal is sent to RCIS to activate the FMCRD run-in.

369. It formalises these requirements with safety functional claims and provides specific details on functional requirements, response times, C&I logic etc for each SSC.

370. As a result of my review of Ref. 93, I am satisfied that the fundamental role and requirements of the SSCs which make up the ATWS system are clearly defined. The A2 classification, the role of the HWBS and the independence of the power supplies

etc are all consistent with my expectations. It should be noted that this document, which I consider to be vital to my assessment, does not feature prominently in the safety case. I could not find any references to it directly from the PCSR or Ref. 39. I was able to eventually establish a link (PCSR Chapter 12 references a basis of safety case report for the CR drive system, and that references Ref. 93) so I am ultimately content that it is part of the UK ABWR safety case.

4.3.10.3 Requirements on the SLCS

371. The ARI is effectively just an alternative way of initiating the same CRs as assumed in a 'normal' scram, and therefore the requirements to deliver the FSF-1 function are well established. The SLCS uses very different means to take the reactor sub-critical, but it is likely it will never be used in the operational life of a UK ABWR (or any other operating ABWR). Therefore, gaining an appreciation of Hitachi-GE's evidence to support its claims on the effectiveness of the SLCS was a key objective for my ATWS assessment. In addition, a feature of the UK ABWR, as with other BWRs, is that the CRs insert from the bottom of the RPV against gravity. While PCSR Chapter 12 (Ref. 33) and its supporting references set out to justify the effectiveness of the hydraulic insertion and the fail-safe nature of the CRs (the assessment of these engineering features is beyond the scope of this fault studies report), confidence in the alternative means of providing shutdown margin to the 'novel' (at least for the UK) primary method has the potential to provide extra reassurance to interested parties.

372. Hitachi-GE has produced a basis of safety case report for the SLCS (Ref. 94) which does the following:

- summarises the function and role of the SLCS (largely in isolation and without reference to the other ATWS SSCs it needs to operate in conjunction with to achieve the necessary outcomes);
- identifies a long-list of safety case documents which are relevant to the SLCS;
- systematically lists all the formal safety functional claims placed on the SLCS in the safety case;
- systematically discusses all the safety property claims made on the SLCS, arguing why it meets all the applicable requirements on redundancy, single failure tolerance, protection from internal hazards etc;
- provides a description of the SLCS, its components, support systems and how it is operated;
- specifies performance requirements, operational temperatures and pressures, boron concentration levels etc;
- identifies significant qualification tests, commissioning tests, maintenance requirements, technical specification controls and surveillance tests etc; and
- illustrates the architecture and configuration of the system with piping and instrument diagrams (P&ID).

373. From a mechanical engineering and C&I perspective, the information supplied is consistent with what is supplied for other major systems in basis of safety case reports. It provides useful details on what the SLCS is and demonstrates how it meets engineering requirements. However, it does not clearly discuss or provide a link to (reactor physics) evidence that shows why the system it describes will be effective in taking an ATWS transient on the UK ABWR sub-critical.

374. There is a single reference in Ref. 94 to a physics-related report (Ref. 95), which is given as the source of a minimum injection rate for the SLC. Inspection of this report shows that it is summarising the results of steady-state reactivity calculations performed with the TGBLA06 and PANACEA computer codes as part of the broader UK ABWR core analysis (Refs. 96 and 97). The stated aim of this analysis is to show that the minimum levels of boron concentration identified in Ref. 94 are sufficient to bring the reactor, at any time in a cycle, from full power and minimum CR insertions

(which is defined to be at the peak of the xenon transient) to a sub-critical condition with the reactor in the most reactive xenon-free state.

375. The source references for the UK ABWR core analysis (Refs. 96 and 97) are outside the scope of this fault studies assessment (ONR fuel and core specialists have considered them as part of their assessment, Ref. 71). However, I am satisfied that they show that the assumed amount of boron, thoroughly mixed in a reactor cooled by the RHR, will take and keep the reactor sub-critical. However, they do not demonstrate why the SLCS will be effective in transporting the boron into the core during the initial stages of a very challenging transient.

376. To supplement the physics calculations, Ref. 95 introduces boron mixing tests performed in the early 1980s to demonstrate boron mixing performance of SLCS. These tests were performed with a 1/6-scale 3D model of a BWR/5 (a predecessor design of the UK ABWR). Hitachi-GE conceded that there were some differences between the test arrangement and the UK ABWR design, notably the test-rig simulated a boron solution being injected by two different routes: from a core-plate differential pressure measurement standpipe and from a high pressure core spray with a 360°coverage sparger located above the core (with operating coolant pumps and forced circulation). In the UK ABWR, the boron solution is injected by the HPCF with a 90°coverage sparger located above the core, accompanied by a trip of the RIPs and a feedwater stop. Despite these differences, Ref. 95 claimed that these results supported a claim that the boron solution will be mixed sufficiently with the UK ABWR's HPCF and 90°coverage, even at low core flow.

377. I was initially not satisfied that this limited and non-prototypic evidence fully supported the UK ABWR design and analysis. Through a number of meetings and RQs in GDA Step 4, I asked Hitachi-GE to provide additional information on how the UK ABWR's SLC is designed to work and to give assurances on why it believes it will be effective (Refs. 98, 99 and 100).

378. Through the RQ responses, Hitachi-GE has provided considerably more additional information than was originally available. In Ref. 99, the following has been provided:

- A description of how the SLCS is designed to work in an ATWS event.
- Confirmation of the major requirements and LCOs for the SLCS
- A statement that a SLCS has never been used in an operating plant
- A description of the limited tests that will be performed during commissioning and during the operational life of a UK ABWR to show that the SLCS will be operable.
- A statement that the UK ABWR SLCS is effectively the same design as the equivalent systems on the Japanese reference plants, except that the UK ABWR SLCS has automatic initiation (note, this is consistent with US NRC's requirements for an automatic SLCS on BWRs).
- A description of how the boron solution will get into the UK ABWR core during an ATWS event. It states that the boron solution is injected through the HPCF sparger located at the upper plenum and mixed, from where it flows through two paths into the core:
  - Through the steam separator, the downcomer, the RIP deck plate, the lower plenum, and then enters the in-channel area from the bottom
  - Down the bypass between channels, from where it enters the in-channel area from the bottom.
- In the absence of any UK ABWR tests, the validation evidence to support the ODYN code used to model ATWS events is discussed. It states that the second flow path is not considered by ODYN which is argued to result in conservative mixing. The claim is that benchmark testing shows that ODYN's one dimensional (1D) boron mixing model is conservative when compared with 3D boron mixing tests.

379. More detail is provided in Ref. 100 on the adequacy of the boron mixing model in ODYN. A review of applicability of all boron mixing test work performed up to 1983 is also included. Again, it is conceded that many aspects of the historic test work is not prototypic for the UK ABWR, but it does provide a basis for validating the computer codes used to model UK ABWR transients. Notably, Ref. 100 expands the applicability of the validation to the more sophisticated TRACG computer code, and identifies a need to develop a multi-azimuthal TRAGG model to demonstrate that the asymmetric injection of the UK ABWR is not a significant challenge to mixing and takes the reactor sub-critical (ultimately provided in an Appendix to Attachment E of Ref. 39).

380. I will return to the issue of modelling in the following subsections but my interim observation is that Hitachi-GE does have the information support the design of the SLCS. However, much of the evidence is dated, not directly applicable to the UK ABWR, and not discussed in the main safety case documentation. While the safety case documentation, notably the applicable basis of safety case report (Ref. 94), does identify some commissioning and surveillance tests to verify that the SLCS will function correctly, these will only provide limited evidence that that UK ABWR SLCS will be effective in taking the reactor sub-critical.

4.3.10.4 ATWS transient analysis

381. The main analysis to show that applicable (infrequent fault) acceptance criteria can be met following a design basis frequent fault with a failure of the A1 scram is provided in Attachment E of Ref. 39. The seven events identified in the fault schedule as prompting an automatic ATWS response have all be analysed with the ODYN code:

- MSIV closure fault
- short-term LOOP (< 2hours) fault
- pressure regulator failure open fault – maximum steam demand
- load rejection with no-bypass fault
- loss of condenser vacuum fault
- recirculation flow controller failure at maximum demand fault
- feedwater controller failure at maximum demand fault.

382. Conservative assumptions have been made in the analysis, consistent with those made in other DBA cases. The analysis has also been repeated with the slightly less onerous assumptions made in US / Japanese practice, to further illustrate the conservatism in the UK analysis compared to how the plant is expected to respond. I am generally satisfied with the appropriateness of the analysis assumptions but it is important to note that they are conservative with respect to the considered acceptance criteria (peak cladding temperature, RPV pressure, S/P temperature etc) and not necessarily conservative for boron mixing. Significantly, the analysis assumes that RPV water level is kept above the top of active fuel (TAF) by an operator action within 30 minutes from the event initiation (the ATWS system FDW stop having automatically terminated flow early in all the transients). This is stated to result in higher core flows, an increased reactor power, more steam flow, and therefore a conservative S/P response. However, it also keeps the ODYN code within its range of applicability.

383. For all seven cases, Attachment E of Ref. 39 shows acceptance criteria are met. For the majority of parameters of concern (maximum and average neutron flux, RPV pressure and peak cladding temperature), the challenging part of the transient is over within tens of seconds. PCV pressure and S/P temperatures generally peak at 30 minutes, after which time the RHR in S/P cooling mode is assumed to start removing heat from the containment. An exception is the analysis for the short-term LOOP fault, which shows S/P temperatures continuing to rise beyond 30 minutes. However, this is not a limiting ATWS transient (assuming the ECCS maintains water level) because the LOOP itself causes a rapid loss of flow and circulation before any A2 C&I response.

384. Another exception is the feedwater controller failure at maximum demand. Attachment E of Ref. 39 characterises this as the most severe ATWS transient analysed and therefore I have examined it in more detail. The malfunction causes the feedwater flow to increase. This is accompanied by a gradual power rise. When the high RPV water 'Level-8' is reached, the MSVs are assumed to close, prompting scram signals. For some reason, the scram is assumed to fail. The MSV closure causes a sharp pressure rise and an accompanying power peak (on top of the gradual rise that had been occurring). In a 'real' event, MSV closure would prompt four of the ten RIPs to trip (C3) and the SRVs would open at their lower C3 setpoints but these are ignored in the analysis. Instead, it is left to the A2 ATWS system to detect high pressure, trip four of the RIPs, and signal a FDW stop. After a 30 second delay, the remaining six RIPs are also tripped. The effects of the RIP trip and FDW stop reduce the power generation, and therefore limit the pressure increase and steam discharge to the S/P. The ATWS high pressure signal also initiates an ARI signal and SLCS injection (on a time delay). Conservatively ignoring the ARI insertion of the CRs, the analysis shows the added boron bringing the reactor down to hot shutdown.

385. The peak cladding temperature is predicted to be 791°C which is beneath the 1200°C limit (similar temperatures are predicted for the other transients modelled). Although the peak in S/P temperature is not predicted until circa 1.5 hours into the transient, the initiation of RHR heat exchanger on 30 minutes is effective in limiting S/P temperatures and PCV pressures to well within design limits.

386. Taking this limiting fault to be representative of all the ATWS events considered, I am satisfied that Hitachi-GE has performed appropriate analysis, within the limitations of its main computer codes, to show that the UK ABWR is tolerant to the conditions experienced during an ATWS event. It provides a valuable insight into how the A2 ATWS C&I system and the plant (thermal hydraulically) responds during the transients. However, on its own, it does not provide me with all the information I was seeking on the effectiveness of the SLCS.

387. As part of the contract I placed with GRS, I requested analysis of a limited number of ATWS events using its modern computer techniques. GRS modelled two of the ATWS events identified by Hitachi-GE:

- recirculation flow controller failure at maximum demand fault
- feedwater controller failure at maximum demand fault.

388. In a first 'pass', both events were modelled by standalone ATHLET calculations using a point kinetics model. In a second pass, the same transients were modelled in a coupled ATHLET / QUABOX-CUBBOX 3D physics model (Ref. 27). In all its analysis, GRS extended the examination of the transient beyond the challenging initial tens of seconds to examine long-term behaviour, including the effect of water level (assuming it initially falls due to the A2 FDW stop, but subsequently recovers due to A1 ECCS injection) and recirculatory flow on boron mixing and core sub-criticality.

389. For the recirculation flow controller failure fault, GRS's short-term results with both its point kinetics and 3D modelling were in good agreement with Hitachi-GE's. Reassuringly, it also predicted that relevant acceptance criteria would be met. In the long-term, the analysis predicts that the only route for boron into the core is down the bypass to the bottom of the core (with a collapsed water level following tripping of the flow and not making Hitachi-GE's ODYN assumption on the operators restoring feedwater, there is no boron recirculation route through the steam separator and downcomer). In the 3D model, the analysis shows the reactor in a stable, but not completely shutdown power level (ie above decay heat power levels) from the point at which ECCS injection starts (around 250 seconds into the transient, at RPV 'Level 2' and 'Level 1.5') to when it recovers the water level enough for recirculation to start (around 2000 seconds). Recirculation causes an initial drop in boron concentration,

before it starts to build up again and take the reactor to a steady power level (around 10% of rated power).

390. For the feedwater controller failure fault, GRS struggled to match some aspects of Hitachi-GE's modelling but did show that appropriate short-term acceptance criteria were met. It was unable to show that a sufficient concentration of boron would be mixed in the core to take the plant sub-critical.

391. I supplied GRS's final report detailing its ATWS analysis (Ref. 27) to Hitachi-GE and invited comment (Ref. 101). I fully recognise that although GRS's computer codes have appropriate validation, its newly-developed UK ABWR models do not have the many years of development time, validation evidence and regulatory scrutiny of Hitachi-GE's computer models (and those of its sister-company, GE-Hitachi). Significantly, Hitachi-GE pointed out in its feedback to me on the GRS analysis (Ref. 101) that GRS used a single channel for the bypass region. This does not allow parallel flow paths for gravity driven mixing. Referencing information supplied in Ref. 100, Hitachi-GE states that buoyancy driven mixing was found to be important in the 1980s physical tests. It postulates that GRS's analysis does not provide a natural circulation path for the boron solution to travel down at the same time as less dense liquid flows upwards.

392. I judge Ref. 101 to be a robust response to GRS's analysis. There was not time in GDA Step 4 to commission additional analyses from GRS, taking cognisance of Hitachi-GE's feedback. However, this is not necessary because ultimately the judgement of the adequacy on the UK ABWR safety case has to be made on Hitachi-GE's submissions and analysis, and not ONR's commissioned work. Computer modelling of the complex behaviour of boron in these situations is inevitably difficult, and Hitachi-GE's established analysis, which is benchmarked to validation evidence, is not invalidated by the newly commissioned GRS calculations.

393. There was sufficient time for Hitachi-GE to undertake additional analysis to address some of GRS's comments. This is discussed in the next section.

4.3.10.5 TRACG Modelling

394. In addition to providing a written response to GRS's observations from the independent confirmatory analysis, Hitachi-GE supplemented its ODYN reference calculations with some TRACG sensitivity cases and included them as Appendices to Attachment E of Ref. 39.

395. Firstly, it analysed the impact of not assuming the operators restarted the FDW injection by allowing the RPV level to fall to 'Level-2' and 'Level 1.5' before the RCIC and HPCF are respectively started to restore water levels. Hitachi-GE states that this analysis shows that the ODYN analysis is conservative, as the FDW restart assumptions increase the S/P temperatures and PCV pressure, while not impacting on the peak cladding temperature evaluation.

396. Secondly, to investigate the potential impact of the UK ABWR just having a 90° sparger supplied from one HPCF line, it performed a range of sensitivities using a 10-theta TRACG model (ie an azimuthal core sector for each RIP) considering:

- injection into the two HPCF lines, increasing the injection coverage into the core;
- delaying the injection of the SLCS by approximately 12 minutes as a way of simulating less effective mixing than is assumed in the standard analysis.

397. In all cases, the 10-theta TRACG analyses demonstrated that the S/P water temperature (the key longer-term acceptance criterion) showed little sensitivity to the varied parameters, and was bounded by the ODYN prediction of the same parameter.

398. I welcome both Hitachi-GE's responsiveness to undertake this additional analysis with new techniques to support the long-established ODYN methodology, and the results it predicts. I consider the approach taken to be sensible. When taken together with other responses provided by Hitachi-GE, it significantly strengthens Hitachi-GE's ATWS safety case.

4.3.10.6 ATWS Conclusion

399. I am satisfied that Hitachi-GE has demonstrated that the UK ABWR is protected against the consequences of a failure of an A1 scram following a frequent fault. Key to this is the A2 ATWS system which responds by tripping the RIPs, at the same time as prompting the ARI to terminate the transient. If this fails, the SLCS is designed to shut the reactor down by diverse means to the CRs.

400. To reach this judgment, it has been necessary for me to ask for a significant amount of additional evidence and information, especially on the SLCS. This extra information, mainly obtained through RQ responses, should be consolidated together more prominently in the UK ABWR safety case documentation, with a clear narrative and trail from high-level claims through the detailed evidence. While the ODYN analysis remains at the centre of the safety case demonstration of adequacy, it has its limitations. These have proved to be surmountable, but they do need to be recognised and discussed. The final version of PCSR Chapter 24 (Ref. 29) provides some more discussion to link the analysis to the engineered provision, but does little to draw in the detailed RQ responses and Hitachi-GE TRACG sensitivity cases into the safety case.

401. At the end of my assessment, it is not clear to me what future operator procedures should say about managing RPV water level and restarting FDW during an ATWS event. Hitachi-GE's analysis predicts that this may be conservative for the S/P water temperature to maintain a high RPV water level. GRS's analysis suggests that this could be detrimental to boron mixing. Further analysis, new experimental work, and enhanced commissioning tests could resolve these uncertainties.

402. Bringing these points together, I have raised the following assessment finding:

- AF-ABWR-FS-09: Hitachi-GE's arguments and analyses for anticipated transients without scram (ATWS) faults are distributed across multiple documents, severely limiting their ability to support safety case claims and inform future safe operations of the UK ABWR. The licensee shall review the available evidence for ATWS faults and consolidate it in future versions of the UK ABWR safety case, such that it is able to demonstrate it fully understands the design requirements for the ATWS systems, it can identify appropriate testing requirements for the standby liquid control system (SLCS), and can implement operator procedures which reduce risks to ALARP.

4.3.11 ATWS instability events.

403. PCSR Chapter 24 (Ref. 29) states that during the 1980s, there were a number of incidents reported in BWRs in Europe and the USA where power oscillations in the core led to unexpected reactor trips. These oscillations were traced to instabilities caused by coupling of density fluctuations in the coolant with the neutronic response of the fuel.

404. ABWRs are designed and operated to avoid regions where these instabilities may occur. This is discussed in PCSR Chapter 11 (Ref. 32) and its supporting references,

and has been assessed outside of this report by ONR fuel and core specialists (Ref. 71). However, some fault transients also have the potential to move the reactor into a low flow / high power region of the operating envelope where such instabilities may occur. If the reactor fails to scram, power and flow oscillations could occur.

405. Attachment E of Ref. 39 presents analysis for two limiting events using the TRACG code:

- turbine trip with bypass fault
- three RIP trip fault.

406. Neither of these faults result in difficult transients if an oscillation is not initiated by thermal hydraulic instability and / or a successful reactor scram is performed. To make the transient non-trivial, an ATWS is assumed and no credit is taken for the A2 ARI. Instead the SLCS is assumed to bring the core to safe shutdown conditions.

407. The acceptance criterion of concern is peak cladding temperature. For both faults, TRACG predicts temperature below 600°C.

408. As part of the GRS contract, I commissioned independent analysis of the three RIP trip fault (Ref. 27). Using its point kinetics ATHLET model, it managed to achieve good agreement with Hitachi-GE' s results on the oscillatory behaviour however its peak cladding temperature predictions were much lower, only managing to predict slight increases by a few degrees above normal operating temperatures. It did not predict conditions severe enough for the ATWS system to initiate SLCS injection.

409. With its coupled ATHLET / QUABOX-CUBBOX 3D physics model, it was unable to generate any oscillations, even allowing the plant to stay in a low flow / high power state for an extended period of time.

410. Primarily based upon Hitachi-GE's submissions, I am satisfied the UK ABWR design and safety case has appropriately considered ATWS instability events within the design basis, and shown that fault acceptance criteria will not be challenged if power / flow oscillations were established. I have no concerns about the use of TRACG for this analysis and I take additional reassurance from the output of GRS's independent analysis which supports this conclusion. Although there is an assumption that the SLCS will be effective in terminating these events, these faults do not introduce any additional concerns to those discussed in the general discussion on ATWS faults.

4.3.12 Conclusion on the adequacy of design basis reactor transient analysis

411. From a detailed review of Hitachi-GE's design basis reactor transient analysis provided in Ref. 39 and supporting references, I am satisfied that:

- appropriate faults have been analysed;
- appropriate conservative assumptions have been made for DBA;
- appropriate acceptance criteria have been considered for both frequent and infrequent faults; and
- appropriate A1 and A2 SSCs have been modelled and shown to be effective in meeting the identified acceptance criteria in accordance with SAPs ERC.1 and FA.7.

412. There are some weaknesses in the level of explanatory detail and the provisions of links to safety case arguments in Ref. 39 but I have obtained enough information during the course of GDA Step 4 to understand what has been modelled and to conclude that it is appropriate.

413. The analysis shows that an inherent feature of the UK ABWR, which follows from the turbine being directly connected to the reactor, is that many isolation fault transients involve a pressure wave travelling down the steam line. This can result in a spike in neutron flux which is a potential challenge to SAP ERC.3. However, I am satisfied that Hitachi-GE has demonstrated that the resulting spike in reactivity is not uncontrollable (the A1 SSCs have been shown to be effective in preventing fuel damage) and if credit is taken for C3 features within the design, the reactor can be kept within MCPR limits.

414. Five assessment findings (AF-ABWR-FS-05 to AF-ABWR-FS-09) have been identified for a future licensee to address but the matters arising from these findings are no challenge to decision to be made in GDA about the adequacy of the UK ABWR design.

415. As a result of my review, I have the following positive observations about the UK ABWR design:

- The correct operation of the claimed A1 and A2 SSCs in response to design basis events is effective in preventing consequential damage to fuel.
- The correct operation of the claimed A1 and A2 SSCs in response to design basis events is effective in protecting the integrity of the PCV. This means that for many design basis events, the off-site dose will be negligible (below the BSO).
- Venting is an effective way of meeting applicable acceptance criteria in extended SBO events and a diverse means of providing the FSF-3 long term cooling function.
- The UK ABWR has A2 SSCs which have been shown to be effective in ensuring acceptance criteria are met in the A1 scram fails following a frequent initiating event.

416. While the specific plans of future licensee to perform maintenance on SSCs designed to deliver importance safety functions while the reactor is at power are not known during GDA, Hitachi-GE's systematic consideration of single failures and planned maintenance within ECCS divisions as part of the LOCA analysis does indicate that the UK ABWR design provides greater flexibility to the operator than the Japanese reference plants. The SBO analysis does establish constraints on the availability of the RCIC throughout power operations; however this does not necessarily prohibit all maintenance on the Division I A1 SSCs.

417. I will discuss the acceptability of the UK ABWR's safety case for the small number of events which are associated with an off-site radiological release in Section 4.9.3

4.4 Shutdown reactor faults

4.4.1 Assessment overview and priorities

418. In GDA Step 2, I observed that Hitachi-GE's preliminary safety submissions did not provide any DBA for shutdown reactor states (Ref. 2). As an overarching high level observation, this shortfall has been addressed, in the final safety case submissions available at the end of GDA Step 4:

- Ref. 38 systematically identifies design basis initiating events in shutdown modes (see Section 4.2.4);
- the fault schedule included in Ref. 38 demonstrably considers faults in shutdown operating states;
- Attachment J of Ref. 39 includes extensive analysis of reactor faults in shutdown operating states, with comparisons made against appropriate acceptance criteria.

419. The analysis presented in Attachment J of Ref. 39 is generally more basic than the approach followed for at-power reactor faults. Greater use is made of simple energy and mass conservation techniques, heat-up and drain-down calculations etc, with less of reliance on sophisticated computer codes. I judge this to be acceptable for GDA. For most faults, the simple objective is to keep the fuel covered in water. Ideally, this will be achieved through active cooling but even if this is not available, the basic provision of makeup water to compensate for evaporative losses should be sufficient to protect the fuel. There are, however, several important factors that are more significant or relevant in shutdown modes which have shaped the assessment I have undertaken:

- The RPV and PCV are extensively reconfigured into different configurations during an outage. In addition, key safety systems are either completely or partially taken out of service (either for maintenance or as a consequence of the configuration of the plant). It is important that these configurations are taken into account in the DBA (SAP FA.6) and / or DBA is used to identify when safety systems can be taken out of service (SAP FA.9).
- Many faults which are potentially challenging when the reactor is at rated power either do not occur or are trivial several hours into shutdown. However, the fuel still retains a significant quantity of decay heat throughout an outage, and therefore faults which could challenge the provision of the cooling safety function need to be considered.
- In many of the shutdown operating states, the PCV is open and de-inerted. In addition, during refuelling, the top of the PCV and RPV is open to the operating deck. This is an obvious challenge for providing confinement safety functions.
- Outages will inevitable involve workers being in areas they would not be in during power operations or performing activities that can only be done when the reactor is shutdown. There are greater demands on them following an event to initiate protective actions, and they are also more likely to be the limiting group of people at risk from the radiological consequences of the event (compared to an off-site population).
- A LOCA event has the potential to both uncover fuel (reducing both cooling and shielding) and to cause consequential flooding. With PCV hatches open for access, there is the potential for barriers protecting safety systems from internal hazards such as flooding to be challenged.
- During a refuelling outage, the CRs continue to be vital for keeping the reactor subcritical. This is in contrast to PWRs where the reactor circuit is heavily borated during refuelling outages. However, as fuel is being actively removed, the CRs need to be withdrawn out of the bottom of the core to prevent them leaning (normally the surrounding FAs provide support to the CRs). This means that the B3 RCIS is ‘live’ when fuel is in the core and therefore is a potential initiator of a criticality fault.

420. These considerations are reflected in the sub-sections below.

4.4.2 Operating states and analysis assumptions

421. As stated in Section 4.2.2, I am content with the five reactor Operating State C sub-states used throughout the fault studies and PSA GDA documentation.[27] Attachment J of Ref. 39 builds upon these defined states, usefully presenting:

- a typical outage schedule showing what equipment is expected to be available in each sub-state;
- diagrams illustrating the configuration of the reactor, SFP, water level and gates in each sub-state;

[27] *Operating C-6 involves all the fuel being transferred out of the reactor and into an isolated spent fuel pool – it is therefore a limiting scenario for the fuel route safety case but a trivial one for the reactor safety case.*

- a table showing the minimum elapsed time from shutdown to enter a specific sub-state, the maximum decay heat assumed in both the RPV and SFP in each sub-state, and the initial water level and volume in RPV and SFP (noting that in sub-state C-3, the RPV and SFP are one contiguous volume of water).

422. For each fault it considers, the assumed pre-fault SSCs operating are identified (in contrast to when the reactor is at power where they are on standby, some A1 SSCs and their essential support systems will be providing a cooling function as part of normal shutdown operation), along with the assumptions made on unavailability as a consequence of the initiating event, maintenance, and single failures. This approach appears to be both systematic and auditable. As a result, if the subsequent analysis can show that applicable acceptance criteria are met, I judge it to be acceptable for demonstrating when maintenance can be performed on safety significant SSCs during outages, and for showing the UK ABWR has adequate levels of redundancy within the available SSCs.

4.4.3 Completeness of faults analysed and acceptance criteria

423. Attachment J of Ref. 39 analyses bounding events from Ref. 38, grouping them into six categories:[28]

- loss of decay heat removal (loss of RHR)
- LOOP (including SBO)
- loss of reactor coolant (including LOCAs)
- CCF of C&I systems (spurious initiation of ECCS, FLSS and ADS)
- CCF of electrical power supply systems
- CCF of essential services and support systems (cooling chain and HVAC).

424. These fault groups are consistent with my expectations.

425. The faults within each group have been categorised as either frequent or infrequent, on the basis of the safety classification of SSCs and as discussed in Section 4.2.4. The attributed frequency categories are consistent with my expectations. Of particular note, LOCA faults involving a physical break in a line are categorised as infrequent, while leaks due to maintenance errors are categorised as frequent.

426. The frequency category is used to determine whether one or two independent means of delivering safety functions are required. Consistent with my expectations, the fault schedule identifies which SSCs are being claimed as the A1 and A2 means of delivering the major safety functions and the analysis in Attachment J of Ref. 39 provides additional discussion and substantiation.

427. In some very limited cases involving CCFs of A1 SSCs and assumed maintenance on one division of the A2 FLSS, Hitachi-GE has stated that the A3 FLSR and the fire protection system (FP) can be considered as being equivalent to an A2 system, and therefore have claimed them on the fault schedule. In the specific cases where Hitachi-GE has done this, I judge this to be a reasonable approach to take in the context of ALARP:

- Maintenance has to be performed at some point on the FLSS, and if the initiating event involves a CCF in A1 SSCs during such occasions, the availability of high classification SSCs will inevitably be challenged.
- The safety function that is required is very basic: the provision of makeup water. The FLSR and FP are both capable of providing the necessary amount of water and engineered routes for directing the water to the necessary areas are already provided in the design.

[28] *The fault schedule (Ref. 38) also identifies control rod withdrawal faults in shutdown modes however the analysis for these faults is presented in Attachment B of Ref. 39.*

- The faults involved have hours of 'grace time' to allow the claimed systems to be readied for operation.[29]
- Ref. 42 defines a requirement for future technical specifications to establish that simultaneous maintenance will not be performed on a division of RHR and FLSS without confirmation of the availability and preparation for rapid connection of the FLSR or another suitable Class 3 system.

428. It is normal practice for the frequency category to also determine the applicable acceptance criteria considered in DBA. However, in the case of shutdown faults, Hitachi-GE has specified the same acceptance criteria for both frequent and infrequent faults:

- RPV water level shall be maintained above the TAF in the reactor and for handled fuel to prevent the fuel being uncovered and heating up;
- SFP water level shall be maintained above the TAF to prevent irradiated fuel being uncovered and heating up.

429. I judge these acceptance criteria to be sensible and appropriate for all design basis events.

430. In addition to the above criteria which are about protecting the integrity of the fuel, Attachment J of Ref. 39 also identifies BSO and BSL dose / frequency targets for demonstrating that the radiological consequences of design basis shutdown faults to workers and the public are acceptable. The BSO and BSL values are identical to those established in Numerical Target 4 of SAPs (Ref. 5) and are therefore fully in line with my expectations.

4.4.4 Steam generation and secondary containment

431. The protection identified for most shutdown reactor faults initiating from (or resulting in) a loss of active cooling is the provision of makeup water to compensate for generated steam. As reflected in the acceptance criteria, as long as the water level remains above TAF, the fuel will remain adequately cooled. During power operation (Operating State A) or the early and end phases of a shutdown (Operating State B) the RPV and PCV are 'intact'. A fault occurring during these phases of operation will result in any generated steam being discharged into the S/P and retained within the PCV. However, in those operating states where the RPV and PCV are open (Operating State C), any steam generated in a fault condition will be released into the secondary containment.

432. In all operating modes, there is the potential for a loss of active cooling fault involving the SFP to also result in steam being released into the secondary containment.

433. The UK ABWR's secondary containment is designed to provide mitigation against any potential radiological releases outside of the PCV. However, it is not a leak-tight structure (in contrast to the PCV). During normal operation and most fault conditions, the secondary containment is maintained at a negative pressure relative to the environment by the Class 3 R/B HVAC in normal operation and the Class 2 standby gas treatment system (SGTS) in fault conditions. Through these means, the secondary containment is designed to ensure a leak rate of less than 50% volume per day. However, neither system is formally claimed by Hitachi-GE in the safety case as being an effective means to manage the consequences of design basis events involving a steam release from the RPV or the SFP. For many reactor or SFP events, the two systems will be unavailable by the very nature of the fault (for example loss of cooling chain or ac power). In addition, Hitachi-GE has stated that the amount of steam that is generated in a loss of active cooling event involving either the reactor or the SFP will

[29] *In the limiting Operating State C-4 cases, assuming 30 minutes for the operators in the main control to become aware of a fault, 30 minutes to establish that the front-line systems are not effective, and eight hours to line up the FLSR, Hitachi-GE's analysis shows margin to fuel uncovery.*

be beyond the capacity of the SGTS (the Class 3 HVAC having been automatically isolated in a fault condition).

434. I established during early interactions with Hitachi-GE that the design proposal and analysis assumption for the UK ABWR is that a blowout panel (above the operating deck in the side of the secondary containment) opens following a fault condition involving a large release of steam, resulting in a discharge direct to atmosphere.

435. Although consequential fuel damage is not predicted for design basis SFP and shutdown reactor events, this approach will result in quantities of radionuclides entrained in steam and aerosols being released, with the potential for public and worker dose uptake.

436. SAP ECV.1 states that radioactive material should be contained and the generation of radioactive waste through the spread of contamination by leakage should be prevented. SAP ECV.2 states that containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions. SAP FA.7 states that, so far as is reasonably practicable, the correct performance of claimed passive and active safety systems ensures that at least one barrier preventing the release of radioactive should remain intact in a design basis fault condition, there should be no release of radioactivity, and no person receives a significant dose of radiation.

437. Following this guidance, I challenged Hitachi-GE during GDA to account for the radiological consequences of the operation of its proposed engineering features in the safety case and demonstrate why the design is ALARP. In addition to design basis faults, I also asked it to take into account severe accidents in its ALARP considerations. These can generate significantly greater quantities of radionuclides (notably, fission products) and hydrogen. Although severe accidents are beyond the scope of this report, the early stages of a severe accident in shutdown modes or involving the SFP will almost certainly start out as a variation of a design basis fault and result in the release of large amounts of steam into the secondary containment. If the blowout panel is designed to open to atmosphere for design basis levels of steam generation, it will almost certainly be providing an unconstrained route to atmosphere during a severe accident.

438. Hitachi-GE responded to this challenge by initiating an extensive optioneering process and ALARP review (Refs. 102 and 103) for ways of responding to a seven day loss of active cooling fault. I will not repeat all the arguments contained in these two references but I consider the following extracted aspects to be significant for my assessment judgements:

- The estimated off-site consequences for the bounding design basis event, assuming the blowout panel design, are stated to be in the region of 0.6 mSv. This is below the BSLs established by Numerical Target 4 in the SAPs (Ref. 5) but above the BSO (0.01 mSv). This indicates the baseline design proposal is not totally unacceptable if it can be shown to be ALARP. It provides the context for considering the merits and disadvantages of other options. It should be noted that although the release is not large in absolute terms, it is higher than the mitigated off-site doses predicted for design basis reactor faults at power such as LOCAs and MS line break faults outside of containment (see Section 4.9.3).
- Hitachi-GE has highlighted several design changes it has already made to the UK ABWR (relative to the Japanese reference plant) to reduce the likelihood of a loss of active cooling fault:
    - The FPC has been upgraded from a Class 3, two-train systems with common piping to a Class 1 separated two-train system,

        - A reserve ultimate heat sink (RUHS) has been added to the design (see Section 4.11.3). This initiates automatically when reactor building service water (RSW) is lost. Cooling can therefore be maintained to the SFP and RPV in the event of a loss of the ultimate heat sink.
        - The outage schedule has been modified to control and improve RHR availability.
        - The way the steam dryer and separator are handled in Operating State C-2 has been modified (for other reasons), greatly reducing the time spent in a high decay heat plant state with reduced water volume levels.
    - A comprehensive review of both additional measures to further reduce the likelihood of a loss of active cooling fault and to mitigate the public dose from steam generation has been performed. Following initial consideration of a wide range of options, a detailed review of a smaller set of viable options was performed. Amongst the options considered were:
        - venting the steam through a demister and filter fitted to the existing blowout panel;
        - venting the steam through a demister and filter fitted to an additional blowout panel; and
        - connection of the operating deck to the main stack via additional ducting (no filtration or active condensation but dose mitigation is achieved by releasing the steam at height).
    - An argument is made that severe accidents involving the SFP and the reactor at shutdown have been practically eliminated (Ref. 104). The implications for severe accident management of each of the options have been considered, but the practical elimination argument provides a context for weighing the potentially conflicting requirements and implications for severe accident management against design basis aspects.

439. Ultimately, Hitachi-GE concluded that the extant design is the appropriate ALARP option. From both my interactions with Hitachi-GE while it was undertaking its review and the documentary evidence provided in Ref. 103, I am satisfied with the scope and rigour of the work undertaken, as well as the final conclusion reached. An important factor for my acceptance of Hitachi-GE's conclusion is that the secondary containment is not a leak-tight pressure containment. Even without the blowout panel open, when it is pressurised by steam rather than being actively maintained in a slightly depressurised state, it cannot be claimed to be a robust barrier for confining radioactivity. However, in my judgement it would be grossly disproportionate to build a second leak tight containment around the PCV for slow developing faults occurring in time-limited operating states (ie outages) and with consequences slightly above the BSO.

440. Having confirmed its design choice in Refs 102 and 103, as part of its DBA for shutdown reactor faults in Attachment J of Ref. 39, Hitachi-GE has demonstrated that fuel can be kept covered by water, calculated the timing for the onset of boiling for different faults in the various operating states, and estimated the off-site doses assuming an open blowout panel. This is all fully consistent with my expectations, and I am satisfied that the predicted radiological consequences meet the expectations of SAP FA.7 and Numerical Target 4 (Ref. 5), when accompanied by the ALARP arguments provided.

441. While Hitachi-GE has made a conservative (radiological consequences) analysis assumption that the blowout panel will be open for these events, it has not linked the setpoint at which it will open during a real event to any fault analysis (DBA or severe accident analysis). I have no objections to this for GDA. However, it is my understanding that the original reason for providing the blowout panel was to provide secondary containment pressure relief in the event of a high energy steam pipe break (ensuring that safety boundaries such as concrete walls and slabs are protected). No

details are provided on when the blowout panel would be expected to open during a SFP or RPV steam generating fault, for example if it will open soon after the onset of boiling or towards the end of the assumed seven day event. Assuming the specific pressure setpoint for opening can be modified by either the UK ABWR designers or operators, in accordance with SAP FA.9 I would expect analysis to be used to inform its value. I have therefore raised the following assessment finding:

- AF-ABWR-FS-10: The UK ABWR secondary containment is provided with a blowout panel to protect the civil structure from high pressure steam releases. However, over the course of GDA the number of claims on this panel has expanded from the original design intent. The licensee shall review and optimise the opening setpoint of the secondary containment blowout panel, cognisant of the safety requirements for high pressure piping ruptures, spent fuel pool (SFP) and reactor design basis loss of active cooling events resulting in steam generation, and the management of radioactivity and hydrogen in severe accidents.

4.4.5 Worker dose considerations

442. Hitachi-GE has recognised in Attachment J of Ref. 39 that it needs to consider the radiological consequences to workers from shutdown faults, and identify any claims on evacuations from an area in order for dose targets to be met.

443. The assumptions made in the worker dose analyses are clearly established at the start of Attachment J of Ref. 39. Crucially, it states that workers are assumed to start evacuating an area as soon as they recognise coolant boiling in the reactor well, a drop in water level due to draindown or a LOCA event, or coolant spilling over from the reactor following a spurious initiation of water injection sources. The time to evacuate is generally only a few minutes, however Hitachi-GE has included the bases for its time estimates (including initial location of workers, the location of exit, the speed on ladders and moving through floodwater) in the submission.

444. The requirement for a rapid evacuation following a fault (for both nuclear safety and conventional safety reasons) is a challenging issue to accept with a design basis safety case. In the relatively calm and controlled environment of the main control room, it is usually assumed that an operator will take 30 minutes to identify a course of action and execute it. In contrast, in these scenarios an immediate response is required to an unexpected event that the worker has never experienced before. However, without a complete redesign of the UK ABWR and its outage operations (it would no longer be an ABWR), workers will need to be in vulnerable areas doing essential work during shutdown operating states, and there is no way to avoid a need for rapid evacuations for the most limiting faults.

445. I also consider the following points to be relevant to accepting the safety case claims on operators for GDA:

- By systematically analysing these shutdown events with conservative DBA methods, the most onerous fault, operating states and worker locations / activities have been identified. This will help a future licensee manage and understand the risks from its plant.
- For both nuclear safety and conventional safety reasons, a future licensee will need to plan its outages and perform risk assessments to demonstrate ALARP (for example, limit number of staff in vulnerable areas or identify the need to perform pre-job briefs on ensure workers know how to response in the event of an emergency etc). This should minimise residual risks that are inherent to the UK ABWR design and operation.

446. As a result, I am satisfied for GDA with the scope of the analysis undertaken in Attachment J of Ref. 39, the transparency and traceability of the claims made on workers to evacuate, the adequacy of the predicted doses against Numerical Target 4 of the SAPs, and the insights the analysis provides into the risks from outage operations.

4.4.6 Additional claims for LOCA faults

447. Hitachi-GE has systematically considered the consequences of the LOCA faults occurring in shutdown operating states in in Attachment J of Ref. 39. However, what it has provided within the scope of the submission has evolved over GDA Step 4. Its initial analysis focused solely on the short term requirements of detecting a drop in water level and providing adequate makeup water to ensure no fuel damage occurs. It subsequently added information on the risk to workers from the loss of shielding between them and the fuel / reactor internals. However, this still did not meet all of my expectations for a design basis safety case, in particular with regard to SAP FA.8 which states that safety measures should be shown to be capable of bringing the facility to a stable, safe state following any design basis fault.

448. My specific concern was that early safety case submissions did not identify any claims on operators to close open containment hatches and personnel airlocks, either to enable a draindown event to be terminated (ie to avoid a need for makeup water to be provided indefinitely to compensate for the losses) or to ensure that SSCs initially operating in response to the fault are not later lost due to flooding in the R/B basement. If closing hatches is a requirement of the design basis safety case, I was looking for assurances that rising floodwater or dose concerns would not challenge the completion of all necessary actions.

449. In response to this challenge, Hitachi-GE has added Appendix C to Attachment J of Ref. 39 and provided additional text into PCSR Chapter 24 (Ref. 29).

450. Appendix C starts off by detailing all the openings in the PCV, and then discusses how long it would take (and with how many workers) to close individual hatches in an emergency situation. In the case of the limiting lower D/W equipment hatch, it is estimated that it will take four to five workers 2.2 hours to perform the necessary actions. Allowing time for fault detection, preparation and getting people and equipment to the correct areas, it has generally been assumed it will take up to 3.5 hours to get an equipment hatch closed from the initiating LOCA event occurring.

451. Appendix C then systematically reviews each of the events considered in the main part of Attachment J of Ref. 39 to identify if a closure operation is needed to either terminate the event or to protect operating SSCs. The analysis shows that the situations and requirements are not straight forward. Depending on the location of the break and the shutdown operating state of the reactor, there may or may not be a safety case requirement to close hatches and airlocks, and the available time to get the hatches closed varies. However, in a ‘real’ event, workers evacuating from an area are unlikely to know the location and severity of the accident, the time available to close hatches, or whether it is an event where hatch closure is required.

452. In an interim revision of Ref. 39, Hitachi-GE considered a guillotine break of the bottom drain line as the limiting event below TAF which requires hatch closure for a stable, safe state to be reached. However, the rate at which this event filled the lower D/W was too high to allow the hatches to be closed before water reached their level. Hitachi-GE argued it would still be physically possible to close the hatches in this condition, and that the amount of over-topped flood water in the R/B basement would not be sufficient to challenge safety systems (by the time the hatches were closed).

453. While I take some comfort from these assertions for extreme scenarios, I stated to Hitachi-GE that I did not consider the levels of reliability that are usually required for design basis measures could ever be claimed for such 'heroic' operator actions in the likely conditions. As a result, Hitachi-GE re-evaluated it safety case approach, and in the final version of Attachment J of Ref. 39 it has argued that a guillotine break of the bottom drain line in shutdown modes is an excessively conservative assumption because the pressures and temperatures involved are much lower than they are during at-power operations (for which a guillotine break has still been assumed). Given that the line is made of corrosion resistant steel and wall thinning is expected to be negligibly small, it has assumed that a slit break is an appropriate scenario for a design basis fault in short-duration Operating State C-3. I judge this to be a reasonable argument to make to inform ALARP judgements on potential improvements to hatch closure response times, and certainly one that I consider to have a stronger basis than claims of closing hatches in the presence of flood water.

454. As a consequence of this change in break size, the time available to close the hatches increases significantly (up to a day) and the bottom drain line break ceases to be the limiting fault. In the final safety case, the largest loss of coolant fault in shutdown modes with open hatches is identified as being a procedural error during outage operations to replace in-core monitoring equipment. It is estimated in Appendix C that it will take 3.9 hours for the lower D/W to be flooded following this event, which is sufficient time for operators to evacuate and close hatches, even allowing a 30 minute preparation time. Similar drain down faults caused by other errors during maintenance operations result in smaller flows and therefore they allow a greater time window for closing hatches.

455. It is my judgement that Hitachi-GE has done sufficient work on the requirements for closing hatches in GDA, and it has documented its analysis and assumptions adequately in Attachment J of Ref. 39 and the PCSR. More will need to be done by the licensee to substantiate the claims made and ensure that the identified actions can be performed in accordance with the requirements of the safety case. It may be possible to gain extra time through the deployment of temporary flood barriers or pumps. However, these options cannot be explored significantly further until the licensee has developed plans for how it wants to perform outages and written appropriate procedures. Therefore, the following assessment finding is raised:

- AF-ABWR-FS-11: Hitachi-GE has shown in GDA the importance of closing primary containment vessel (PCV) hatches and airlocks following a loss of coolant accident (LOCA) in certain shutdown operating states. However, a full demonstration that the necessary actions can be completed with an adequate time margin cannot be made until the UK ABWR design and outage strategies are further developed. The licensee shall review its detailed design, outage plans and procedures to ensure that everything reasonably practicable has been done to ensure that hatches and airlocks in the PCV can be closed in a shutdown fault condition in accordance with the reactor safety case requirements, without the safety of workers being compromised to an unacceptable level.

4.4.7 Reactivity faults during shutdown

456. Alongside consideration of CR withdrawal faults while the reactor is at power (Operational State A) or in startup (Operational State B), Attachment B of Ref. 39 provides discussion on the need for analysis of CR withdrawal fault during shutdown modes (Operational State C). It explains that when the Class 3 RCIS control system is put into its 'REFUEL' mode, no more than two CRs (a CR pair sharing the same HCU) can be withdrawn from the core. However, it recognises that a spurious failure of the RCIS could cause the withdrawal of more than two CRs, leading to a criticality event.

457. Attachment B does not provide any new analysis specifically for shutdown faults. Instead it references analysis for startup faults to make the following arguments:

- The unmitigated consequences can be assumed to be bounded by the results of the startup fault analysis. This shows that even if the A1 scram is not credited (first line of protection for the frequent fault), the enthalpy rise from a reactivity insertion will not be sufficient to cause fuel failures.
- On the basis that there will be no fuel failures, the unmitigated consequences on-site will be less than 200 mSv. According to Hitachi-GE's categorisation and classification scheme (Ref. 54), a frequent fault with these unmitigated consequences requires a single A2 SSC to provide the necessary FSF-1 safety function.
- Protection is actually provided by the A1 SRNM prompting a scram (the hydraulic insertion of all the CRs overriding the mechanical withdrawal of CRs).
- The effectiveness of the scram in Operating State C is assumed to be shown by the results of the startup fault analysis demonstrating the same aspects in Operating State B.
- The RCIS includes an interlock which blocks more than two CRs being withdrawn when it is in 'REFUEL' mode but no credit is taken for this in the analysis.

458. The fault schedule (Ref. 38) appears to be putting forward different arguments to Attachment B of Ref. 39. It firstly considers as a frequent fault the incorrect withdrawal of a single CR (the incorrect withdrawal of a CR surrounded by fuel rather than the correct CR that has just had the adjacent FAs removed by the refuelling operations). It then considers the incorrect withdrawal of a pair of CRs. For both faults, no design basis protection is claimed to be necessary. My interpretation of this entry is that credit is being taken for UK ABWR cores being designed to have sufficient shutdown margin with the pair of CRs with the highest worth not credited. However this not stated in the fault schedule. The fault schedule does state that faults of greater severity are limited by the Class 3 RCIS 'REFUEL' rod block interlock.

459. I have a number of concerns with the adequacy of the safety case, as presented:

- The fault schedule is inconsistent with Attachment B of Ref. 39.
- During a rod withdrawal fault during startup, the RPV and PCV are intact. In many of the Operating C sub-states, notably C-3 when refuelling is being performed, the RPV and PCV are open. Therefore the unmitigated consequences to workers from an unplanned criticality cannot be assumed to be the same (at least not without extensive supporting discussion and analysis).
- The RCIS is a Class 3 C&I system that is live throughout refuelling operations and it has the capability to withdraw any number of CRs in a postulated failure. Although the rod block in 'REFUEL' mode will make a valuable contribution to safety and limit the severity of operator errors or RCIS failures, it is not independent of the RCIS and its correct operation cannot be credited if the fault is initiated in the RCIS (see SAP FA.6).

460. Separate from my concerns, Hitachi-GE has also identified its own issues with the safety case for these faults. In Ref. 102, Hitachi-GE presents an ALARP review of the risks of a criticality event during refuelling. This review was undertaken before the end of GDA Step 4, with a design assumption that the RCIS would be safety class B2 rather than the final B3 designation declared for GDA. The review started with the premise that the key safety case claim is a B2 rod block within the RCIS which will limit the severity of any rod withdrawal fault (ie consistent with the extant fault schedule). The concern identified by Hitachi-GE that prompted it to undertake the review was that the RCIS interfaces with the C3 control system of fuel handling machine (FHM) and this has the capability of overriding the RCIS rod block. It was therefore postulated that

a failure in the low integrity FHM control systems together with an operator could cause an unplanned criticality.

461. The review looked at multiple options to remove the vulnerability introduced by the FHM's control system (including upgrading its safety classification and reliability). It also looked at diverse means ensuring the control of reactivity, independent of the FHM and RCIS. The ALARP option it ultimately settled on was to retain the FHM's control systems as a monitoring system but change the way refuelling operations are performed so that the CRs do not need to be withdrawn.

462. In the Japanese reference plants, the process for removing fuel in a four assembly cell around a CR is as follows:

- Initially all CRs are inserted.
- Two FAs in a diagonal around a CR are removed by the FHM (ie in a checkerboard pattern). The two remain FAs provide support to the cruciform CR, preventing it from leaning.
- Double blade guides (DBGs) are inserted into the two empty cells. These are effectively dummy assembly boxes the same size as a FA.
- The two remaining FAs are removed. The DBGs provide support to the CR.
- The CR is withdrawn through the bottom of the core by the RCIS.
- The DBGs are removed by the FHM and the process moves onto the next four assembly cell.

463. The process is reversed during fuel loading. If a CR is to be removed from the core or maintenance, it is removed by the FHM out of the top of the RPV from an initially withdrawn position.

464. Ref. 102 states that Japanese plants have 10 DBGs to allow them to manage their refuelling operations. The ALARP design change it proposes for the UK ABWR is to utilise 205 DBGs (ie one for every CR) so that CRs can be supported in the inserted position, thereby removing the need for CRs to be withdrawn and the potential vulnerability from a RCIS failure.

465. If this change was adopted, it could go a significant way to addressing my concerns. For example, if CRs withdrawals are not needed for operational reasons, the simple but highly effective measure of removing power to the CR drive mechanisms during part or all of refuelling operations could significantly or completely remove the threat of a spurious or erroneous withdrawal.

466. Ref. 102 has not resulted in any confirmed changes to the UK ABWR GDA design or safety case. It states the further controls on the withdrawal of CRs will be incorporated in site licensing. In a late addendum, it goes on to recommend the future licensee reviews again the optioneering and proposed design changes for these events, speculating that following the re-designation of the RCIS as B3, the weakness it first observed (a failure in the lower class FHM control system resulting in a vulnerability in the RCIS) may no longer be there.

467. I disagree with this final piece of speculation in Ref. 102. It is my judgement that the risks of a design basis fault during refuelling with an 'active' B3 RCIS remains, regardless of its classification relative to the FHM control system. I do agree that this whole area needs to be looked at again during site licensing. I am not satisfied that Hitachi-GE has demonstrated the adequacy of either its design or safety case in this area. However, I believe it is appropriate for this to be addressed outside of GDA because:

- Hitachi-GE has stated in Ref. 102 that more work needs to be done after GDA to resolve this matter;

- the detailed design of the RCIS and FHM control system is beyond the scope of GDA, and therefore has not been considered in ONR's Step 4 C&I assessment (Ref. 79);
- it is not known how future licensees will undertake their refuelling outages.

468. I have therefore raised the following assessment finding:

- AF-ABWR-FS-12: As a result of ONR's GDA Step 4 assessment establishing that the Class 3 rod control and information system (RCIS) is active during refuelling operations, the licensee shall review its design and safety case to ensure that the risks from an uncontrolled criticality caused by an erroneous control rod(s) withdrawal event are reduced so far is reasonably practicable. It is assumed this will require a greater appreciation of the detailed design of fuel route control systems and likely refuelling strategies than is available in GDA.

4.4.8 Conclusions on adequacy of the shutdown reactor safety case

469. Noting that at the start of GDA the available safety case submissions contained minimal consideration of faults not at rated power, I am now satisfied that Hitachi-GE has comprehensively and systematically addressed reactor faults in shutdown operating states.

470. Shutdown events are identified in the fault schedule (Ref. 38), and the claims made on availability and effectiveness of SSCs are supported by DBA in Attachment J of Ref. 39. I attach particular importance to the substantiation of maintenance assumptions in the outage schedule, and acknowledge that changes have been made as a result of the analysis undertaken.

471. I had initial concerns about the acceptability of releasing steam generated during loss of active cooling faults into the secondary containment and then unfiltered to the atmosphere through a blowout panel. However, I am satisfied that Hitachi-GE has performed a rigorous ALARP review of this aspect of the design, and I am content with its final conclusion on the adequacy of the extant design.

472. Hitachi-GE has expanded its consideration of the consequences of faults from just reactor acceptance criteria on the fuel, RPV and PCV to include the potential doses to workers. To meet dose targets, many faults require workers to evacuate areas rapidly. However, Hitachi-GE has justified the assumptions it has made, and its analysis helps to inform me (and future licensees) which events are the most challenging.

473. In Appendix C to Attachment J, Hitachi-GE has considered the requirements to close equipment hatches to allow LOCA faults to be terminated and to protect SSCs in the R/B basement. I am satisfied that Hitachi-GE has done sufficient work for GDA to establish what actions can be credibly completed in the available time, but this will need to be substantiated and reflected in future outage procedures.

474. I am not satisfied that Hitachi-GE has demonstrated the adequacy of either its design or safety case for CR withdrawal faults during refuelling. With the detailed design of the RCIS and FHM control system currently not available, and plans for how future licensees would plan to undertake refuelling outages yet to be developed, it has not been possible to resolve this issue during GDA. However, it will need to be addressed in site licensing.

475. Three assessment findings have been raised on shutdown faults:

- AF-ABWR-FS-10 on the opening setpoint of the secondary containment blowout panel;
- AF-ABWR-FS-11 on the plans and procedures for closing PCV hatches;

- AF-ABWR-FS-12 on the risks of an unplanned criticality during refuelling.

476. In addition, the need for AF-ABWR-FS-01 on the need for the shutdown states used in the technical specifications to be consistent with the DBA and fault schedule is reiterated.

4.5 Fuel Route

477. For any nuclear power plant, there is rightly a considerable amount of safety case attention focused on the reactor. However, there is usually a larger inventory of irradiated nuclear fuel in the SFP than there is in the reactor. In addition, fuel handling operations are amongst the most challenging routine tasks performed on a nuclear power plant site. If FAs are dropped or involved in a collision during handling, there is a high likelihood of the cladding being damaged and fission products being released into the local area. It is therefore very important that the UK ABWR has a robust design basis safety case for fuel route faults.

478. I have already stated in Section 4.2.4 that I am satisfied with how Hitachi-GE has identified fuel route faults in Ref. 44. In this section I have detailed my assessment of Hitachi-GE's analysis presented in Ref. 45 which aims to demonstrate the effectiveness of safety measures claimed to protect against the identified faults.

479. I have separated my assessment into two parts. Firstly, I have looked at the analysis for the SFP and the measures which ensure the safety of the bulk inventory of irradiated fuel. Secondly, I have looked at the analysis for faults during routine FA and reactor component handling operations, where the main safety concern is the risk to workers rather than integrity of all the fuel.

480. During normal power operations, the reactor is a separate system to the SFP. Once the reactor is shutdown, depressurised and the RPV / PCV open, it too is effectively just another storage pool. During Operating State C-3 (refuelling operations), the reactor and SFP are a single contiguous system. Consistent with the approach taken by Hitachi-GE, my SFP assessment below has considered the SFP when it is isolated from the reactor. Operations in State C-3 with the SFP gate open are assumed to be covered in the shutdown reactor safety case. My assessment of FA and reactor component handling operations covers all Operating States (including C-3).

481. I have excluded consideration of fuel export operations from the spent fuel pool (these have been reviewed by radioactive waste management colleagues) although many of the SSCs involved and safety case arguments made for these operations are the same as those I have considered here.

4.5.1 Spent fuel pool

482. The SFP is a seismically qualified Class 1 structure made of reinforced concrete lined with stainless steel plate. It has capacity to store a total of 300% of one full core's fuel load. This is sufficient space to store the spent fuel from 10 years of operation and a full core offload. The water in the SFP is not borated. Criticality is prevented even in the most severe fault conditions by the spacing of FAs in the racks and the borated stainless steel the racks are made with.

483. The SFP is cooled by the FPC system. It takes overtopped SFP water from two skimmer surge tanks, puts it through heat exchangers and returns it to the SFP. The FPC on the UK ABWR has been modified from the equivalent system on the Japanese reference plants to improve its redundancy and segregation. These changes have allowed Hitachi-GE to classify the FPC on the UK ABWR as A1.

484. In the event of a leak from the SFP (or an extended loss of active cooling, with associated evaporative loses), the A2 FLSS is the major SSC claimed. It is designed to provide sufficient makeup water to ensure that the fuel in the SFP remains covered and therefore adequately cooled for up to seven days.

485. In Ref. 45, Hitachi-GE has presented analysis for the following limiting infrequent basis events:

- loss of all FPC pumps
- medium term (up to 24 hours) SBO
- SFP (small) liner leak.

486. Several frequent faults are identified on the fault schedule however they generally involve the failure of just a part of a redundant A1 SSC or are trivial from an analysis perspective (for example, SFP cooling can be maintained during an extended LOOP through the operation of the EDGs). I therefore judge the scope of the SFP DBA presented in Ref. 45 to be appropriate.

4.5.1.1 Loss of all FPC Pumps

487. Hitachi-GE has analysed two limiting heat loading scenarios for the SFP that bound all operational states when the SFP gate is closed:

- a ‘normal’ heat load assuming the SFP is at 200% capacity plus quarter of the reactor core’s FAs (3.35 MW);
- a rare maximum heat load scenario when the SFP is at 200% capacity and the entire core is offloaded (9.75 MW).

488. In both cases, a 17 month period of power operation has been assumed, and the SFP gate has just been closed 16 days into a 30 day outage, upon completion of fuel handling operations. To pessimise the analysis, the initial water temperatures have been assumed to be the maximum design temperatures permitted by the technical specifications. These assumptions are adequately explained and are consistent with my expectations.

489. The analysis shows that for the ‘normal’ case, it would take 27 hours for the SFP water to start boiling, and a further six hours for the water level to reach the ‘SFP water level low’ setpoint which initiates an alarm in the main control room. It is assumed the operator starts the FLSS 30 minutes after receiving the alarm, preventing further reductions and subsequently restoring water levels.

490. For the maximum off-load case (Operating State C-6), boiling is predicted within seven hours and the ‘SFP water level low’ setpoint is reached two hours later. Again, the operator is assumed to respond after 30 minutes by starting the FLSS and restoring the water levels.

491. Through detection of low water levels and starting the FLSS, it is claimed that the fuel will be adequately cooled throughout the assumed seven day transient.

492. I judge this analysis, and the conclusions, to be appropriate. In reality, the operators would know long before boiling and the SFP ‘water level low’ setpoint is reached that action is needed. However, even with the conservative assumptions made, there is always a considerable amount of water above the fuel.

493. It is noteworthy that the claimed protection for this fault is limited to the provision of makeup water by the FLSS. The UK ABWR safety case is not based upon having an alternative means of providing active cooling and avoiding boiling. I am content with this for the following reasons:

- Fuel in the SFP is adequately cooled as long as it remains covered, even if the water is boiling.
- The safety classification of the FPC has been increased to A1 (which is reflected in the architecture of the piping, redundancy in pumps, safety classification of control and support systems etc) such that a total loss of active cooling is an infrequent event.
- A RUHS has been added to the UK ABWR, protecting against some causes of a complete loss of heat sink and therefore some causes of a total loss of FPC.
- In some shutdown states, the FPC is supplemented by the RHR to keep the SFP water temperature within technical specification limits for normal operation. In limiting conditions, a single division of RHR would not be able to keep the SFP water temperature within normal operational temperatures but it would be able to prevent boiling.
- The RHR is not available to support SFP cooling when the reactor is at power (a design change compared to the Japanese reference plants, made to ensure there is adequate provision for reactor faults assuming planned maintenance and single failures). However, the heat loading in the SFP is lower during normal power operations than it is in the two analysed situations, and therefore the time available to restore active cooling is increased.

494. Hitachi-GE's safety case guidance (Ref. 54) allows for A2 protection (in this case, the FLSS) to be the sole protection for an infrequent design basis fault, if the initiating event is associated with a CCF in an A1 system (in this case, the normally operating FPC). Given the simplicity of the demand placed on the FLSS (the provision of makeup water after many hours), the diversity of the FLSS's control system (HWBS) from the FP C&I, and recognising that there are several additional defence-in-depth measure available to provide the same function (the FLSR, the FP, the makeup water condensate system (MUWC), and the suppression pool clean-up system), I do not see any safety benefits in increasing the safety classification of the FLSS further. As a result, I agree with Hitachi-GE that the A2 FLSS provides appropriate protection for this fault.

495. As with shutdown faults with the PCV open (see Section 4.4.4), there remains the challenge of dealing with the (slightly) activated steam that is generated in the fault condition if active cooling cannot be restored before the water starts to boil. Hitachi-GE's ALARP review discussed in Section 4.3.15 (Ref. 103) included the steam generated from the SFP (both in isolation and in combination with a reactor fault) in its deliberations. I am satisfied that Hitachi-GE has demonstrated that the radiological consequences of releasing the generated steam out of the secondary containment are acceptable, and that the addition of filters or upgrading the HVAC system would be grossly disproportionate.

496. Hitachi-GE claims that workers will not remain in the vicinity of the SFP if the water is boiling, and therefore will not receive a dose from this fault (from either radioactivity carried in the steam or from a reduction in water shielding). I judge this to be a credible claim to make, noting that the FLSS will be operated from the main control room.

4.5.1.2 Medium term SBO fault

497. Hitachi-GE has effectively bounded LOOP events (for which EDGs are available for up to seven days) with SBO events where a CCF of the EDGs has occurred. A two hour SBO fault has been bounded by 24 hour medium term SBO event. No new analysis has been performed for the limiting SBO event because the fault sequence and protection is virtually the same as that assumed for the loss of all FPC pumps (the FLSS remains available even with the EDGs unavailable).

498. I am satisfied with this approach, and note that even without specific analysis, the analysis conditions and claims of SSCs for this fault (and the faults it bounds) are clearly stated in Ref. 45.

499. One important point of detail that I welcome is a recognition in the acceptance criteria that the SFP water level not only needs to be maintained above the TAF, but also needs to be above any fuel being handled above the racks. Ref. 44 states that the FHM is not supplied by the EDGs, and therefore in either a LOOP or a SBO, any assemblies being moved will be stranded above the rest of the fuel. The analysis (loss of all FPC, assumed to applicable for SBO faults) shows that there is not a challenge to stranded fuel but it is appropriate that this is recognised as the first safety concern that occurs before TAF is threatened.

4.5.1.3 SFP liner leak

500. In both Refs 44 and 45, Hitachi-GE is clear that the primary SSCs for maintaining SFP water level are the A1 SFP structural concrete, the stainless steel liner and the pool gate. Protections against internal and external hazards for these SSCs are included in the design and safety case, consistent with their A1 safety classification. The adequacy of the civil engineering and hazards safety case claims are matters for ONR colleagues who specialise in these areas and beyond the scope of this report. However, if an adequate safety case is made in these areas, it can be assumed that a catastrophic drain down from the main pool structure is not a design basis event.

501. The gate is a potential source of failure but Hitachi-GE has recognised this by classifying it as A1. The engineering and inspection requirements that follow from the gate being classified that A1 are beyond the scope of this fault studies report, however I do note that Ref. 45 does identify a need to periodically inspect and replace the seal on the gate to ensure its integrity. I also note that the bottom of the SFP gate is above the TAF in the SFP, so even a catastrophic gate failure will not result in the immediate uncovery of fuel in the racks. In operating states when fuel is being handled above the racks, there is either a second gate in place (Operating State A), or the reactor well is flooded up to the same level as the SFP (Operating State C-3).

502. Given that there are no other penetrations in the SFP structure, Hitachi-GE has stated that the limiting design basis event it has assumed is a failure of welding line on the bottom of the SFP, resulting in a maximum flow rate of 10 m^3/hour.[30]

503. Before accepting this as a limiting fault scenario, I sought additional assurances on breaks in the FPC not being a further threat to SFP water inventory. While the FPC's intake is water overtopping weirs at the normal operating level for the SFP into the skimmer surge tanks, it returns water through submerged pipes. Meetings with Hitachi-GE during GDA Step 4 and accompanying RQs resulted in Refs. 105 and 106 being submitted to ONR supplying additional information on the FPC.

504. In Ref. 105, Hitachi-GE stated that the FPC discharge lines go down 11 m below the normal SFP water level (about 0.4 m from the bottom of the SFP and a long way beneath TAF for FAs in the racks). As a result, the unmitigated consequences of a limiting break in a FPC line could result in much larger volumes of water being siphoned out of the SFP than is assumed for the weld liner leaks (beyond the capacity of the FLSS). However, Ref. 105 goes on to state that the FPC discharge line is protected by both an A1 siphon breaker and an A1 check valve.

505. I was immediately satisfied that these two simple and reliable measures should be effective in protecting against the risks of water being siphoned out through the FPC discharge lines but I challenged Hitachi-GE to explain why it is consistent with showing

[30] *The justification for this assumed flow rate is set out in Ref. 147. Analysis in early drafts of Ref. 45 showed that a leakage rate of 30 m^3/hour (assuming a failure of all welds in the liner) is within the makeup capacity of the FLSS.*

that risks are ALARP to have discharge lines so deep into the SFP. Even if the safety benefits of having the lines terminate higher (for example, above TAF) are likely to be small, there would be limited financial detriment with such a change. In Ref. 106, Hitachi-GE responded that the design choice of locating the discharge lines deep into the SFP had evolved from many years of operational experience on Japanese BWR plants. The deep location was found to encourage mixing between hot and cold regions of water and minimise water surface variations. Both of these factors were found to aid SFP visibility for normal operations, and as a result all Japanese plants (including ABWRs) have adopted similar designs.

506. Ref. 106 goes on to provide an extended ALARP justification for the extant design, presenting both deterministic and probabilistic arguments for keeping the FPC return pipes low in the SFP. I judge some of the arguments put forward to be stronger than others, but ultimately I am content that the likelihood of a catastrophic draindown through the FPC is very low, while I am happy to take accept the operational experience from Japan that there are operational advantages to the design.

507. Ref. 105 states that the FLSS / FLSR lines are not submerged beneath the water, and therefore I accept that these are not additional siphoning risk.

508. On the basis of the extra information supplied in Refs 105 and 106, I am content with the liner leak being the specified as the limiting design basis loss of water inventory fault.[31]

509. The analysis of the limiting fault in Ref. 45 shows the water level reaching the 'SFP water level low' setpoint within approximately three hours. Assuming 30 minutes for the operator to respond with FLSS injection, there is never less than 11 m of water in the SFP, and normal water levels are recovered within four hours of the event occurring. The recovery of normal water levels facilitates the restoration of active cooling by the FPC via overtopped water to the skimmer surge tanks. Fuel being handled (or in the racks) is never uncovered, steam is not generated, and the drop in water level is not sufficient to cause workers to receive an abnormal dose due to a significant loss of water shielding.

510. I am therefore satisfied that Hitachi-GE has demonstrated the effectiveness of the FLSS and its associated water level setpoint for manual initiation, and I judge the presented design basis safety case for this fault to be adequate.

4.5.2 FA and equipment handling

511. The UK ABWR fuel route routinely handles FAs and reactor components, consistent with the fuel routes on most light water reactors. Dropping or over-raising a FA will almost certainly be associated with radiological consequences, as would dropping a heavy component onto FAs. These risks are inherent to fuel route operations on all BWRs and I have no expectations that Hitachi-GE will depart from relevant good practice and develop novel fuel route techniques that have evaded other reactor vendors.

512. The most important factor for nuclear safety is to minimise such events occurring, rather than trying to mitigate the consequences. Hitachi-GE has recognised this, and has declared the design provision of the FHM and reactor building overhead crane (RBC) to be safety class A1. The adequacy with which the UK ABWR fuel route systems meet the design requirements for an A1 crane is beyond the scope of this fault studies assessment. However, I am taking it to be a fundamental assumption that any additional actions or safety measures required to prevent significant radiological consequences are only needed after a failure of an A1 measure on the FHM or RBC.

[31] *The final version of Ref. 45 received during GDA Step 4 was updated to summarise the key arguments made in Refs 105 and 106, clearly establishing the check valves and siphon breakers as A1 SSCs with an important role in the SFP safety case.*

513. In Ref. 45, Hitachi-GE has considered as frequent faults:

- over-raises of irradiated fuel or equipment;

and as infrequent faults:

- fuel drop during irradiated fuel handling between the SFP rack and the core;
- drop of heavy equipment onto the core or the spent fuel rack.

514. In the following sub-sections, I have assessed the design basis safety case for each in turn.

4.5.2.1 Over-raises of irradiated fuel or equipment

515. Ref. 45 identifies a number of items which need to be moved by either the RBC or the FHM. The bounding components chosen for analysis are:

- separator (RBC main hoist)
- irradiated fuel (FHM main hoist)
- CR (FHM auxiliary hoist)
- RIP impeller (FHM RIP inspection hoist).

516. I judge this selection of bounding events to be appropriate for the UK ABWR.

517. Normal operations on both the RBC and FHM are controlled by a C3 programmable logic controller (PLC). I therefore agree with Hitachi-GE that a malfunction in a PLC resulting in an over-raise event should be treated as a frequent fault.

518. To support a decision on the number of protective measures required, Attachment C of Ref. 45 presents analysis of the unmitigated consequences to workers for the bounding over-raise faults. Unsurprisingly, the radiological consequences of over-raising irradiated fuel or a CR are large and therefore A1 and A2 protection is required according to Hitachi-GE's categorisation and classification scheme. The unmitigated consequences for over-raising the separator and the RIP impeller (as well as other RIP-related components) are less serious and only a single A2 measure is stated to be necessary. I agree with the logic behind these conclusions and consider the outcomes for the design to be reasonable.

519. As a result, the following protection is identified:

- A1 height detectors (limit switches) to prevent over-raise events on the FHM, with diverse A2 height detectors provided for fuel and CR faults;
- A2 height detectors on the RBC to protect against separator over-raise events.

520. Ref. 45 goes on to present dose analysis (shielding calculations) to show the effectiveness of the protection in limiting the dose to workers in the vicinity of the over-raised components while fuel route operations are being performed.

521. In an early revision of Ref. 45, in the absence of detailed design information for the UK ABWR, setpoints for the height detectors were taken from Japanese reference plants, and used in combination with an assumption of an immediate rapid evacuation by workers (similar to the assumptions made in the shutdown safety case discussed in Section 4.4.5 and will be mentioned in the next section on fuel drops). In the case of the separator, the combination of these assumptions resulted in a dose to workers close to the Numerical Target 4 BSO (0.1 mSv). This established to me that both the height detector and a rapid evacuation are needed to minimise doses to expected levels. However, for the FHM-related over-raise faults, doses several orders of magnitude smaller than the BSO were predicted. Ideally, the engineered protection would be shown to be effective with setpoints established such that a rapid evacuation

is not necessary. As originally presented, the dose information was not demonstrating this.

522. In response to a RQ, Hitachi-GE addressed this feedback in Ref. 107. A table was supplied, summarising all identified SFP and fuel route faults and giving the following information:

- The unmitigated radiological consequences to workers calculated for each fault, assuming no engineered protection or a rapid evacuation.
- The mitigated consequences for each fault crediting the engineered protection but not assuming a rapid evacuation of workers.
- The mitigated consequences crediting the engineered protection and assuming the workers evacuate immediately in accordance with procedures.

523. The final version of Ref. 45 has been updated to reflect the final results of Ref. 107. I welcome this but also consider the format and tabular style of Ref. 107 to be an informative supplement to the main fuel route safety case documentation. It shows that for the FA, CR and RIP impeller over-raise faults, the BSO can be met without a rapid evacuation, assuming the height detectors are set at, or below, the setpoints used on the Japanese reference plants.

524. The procedure for removing the separator during a routine outage has been recognised as a relatively high dose activity and has therefore been subject to significant regulatory attention during GDA, notably in the mechanical engineering topic area (Ref. 108). In the UK-context of demonstrating that risks have been reduced to be ALARP, changes have been made to the procedures for the operation (compared to Japanese practice), so that the water level in the reactor well and DSP is flooding up at the same time as the RBC is lifting the separator. Refs. 107 and 45 show that if a malfunction on the C3 RBC PLC results in the separator being lifted above the increasing water level, doses above the BSO could occur (but would remain below the BSL), even with engineered over-raise protection and a rapid evacuation. This is not ideal, however given that the unmitigated consequences of this fault condition are consistent with those permitted for normal outage operations in Japan (ie a UK fault condition is similar to Japanese normal activities), and because the whole operation has been subject to a detailed ALARP review in the mechanical engineering topic area, I am satisfied that the expectations of SAP FA.7 and Numerical Target 4 (Ref. 5) have been met.

4.5.2.2 Fuel drop during irradiated fuel handling between the SFP rack and the core

525. In my opinion, the most important aspect of the design basis safety case for a fuel drop is the protection included within the A1 FHM provided to ensure a drop does not occur. If a drop does occur, there are no additional measures that can be put in place to stop the FA being damaged on impact and / or rapidly relocate it to a safe position. All that can be done are actions to mitigate the consequences to the workers (by evacuation) and the public (confining or filtering the release). The adequacy of the A1 protection on the FHM is beyond the scope of this GDA fault studies report but it is crucial context for my assessment.

526. Ref. 45 has considered FA drops in both in SFP and at the reactor well. Most of the presented analysis is based on drops at the reactor well because the fall distance into the core is larger than the maximum drop height in the SFP. However, a demonstration for a limiting criticality scenario is presented involving a dropped FA in the SFP lying horizontally on top of assemblies in the SFP racks. It is illustrated that the design and geometry of the FAs is such that the dropped FA is always a distance away from the TAF of the fuel in racks that exceeds the neutron mean free path. I am content with this simple demonstration, recognising that the potential for such a fault has long been factored into the design of BWR fuel and storage racks.

527. Three scenarios have been considered for drops at the reactor well:

- A drop into the core, resulting in damage to both the dropped FA and in-situ fuel.
- A drop into the reactor well (but not into the core), causing an additional radiation risk to workers performing outage tasks in the upper D/W.
- A drop into the RPV bottom between the inner surface of the RPV and the outer surface of the core shroud. This could cause an additional radiation risk to workers performing outage tasks in the lower D/W.

528. For the first scenario, Hitachi-GE has estimated in Attachment B of Ref. 45 that the kinetic energy of the dropped FA is sufficient to damage approximately 45 rods in impacted assemblies, in addition to all rods in the dropped FA being damaged. This has been rounded up to be two FAs, or 0.2% damage to the total core inventory (given that there are 872 FA in the UK ABWR core). I am content with this assumption, noting that it is clearly explained and is auditable in the document

529. Following an ONR RQ (Ref. 109), Hitachi-GE has acknowledged that it is relevant good practice on many operating BWRs to minimise the risks to workers during fuel handling operations by putting in place temporary shielding or a fuel transfer chute.[32] For the second scenario, Hitachi-GE has taken credit for currently unspecified temporary shielding to protect workers in the upper D/W, stating that a detailed ALARP assessment will be performed during the site specific phase of UK ABWR development to determine what options can and should be implemented. I have no objections to this assumption for GDA.

530. Refs. 107 and 45 show that the dose to the workers for the first and third scenarios are greater than 100 mSv if no credit is taken for a rapid evacuation (the provision of temporary shielding for the second scenario is shown to result in worker doses of 5 mSv). Although they are below the Numerical Target 4 BSL for infrequent faults (200 mSv), they are high. A rapid evacuation is shown to be effective in reducing the worker dose by an order of magnitude for the first scenario and by nearly two orders of magnitude for the second and third scenarios.

531. In my opinion, the mitigated worker doses in fault conditions remain high (when for example compared with design basis reactor faults in Operating State A) and it is difficult to substantiate claims on the effective, rapid evacuation of teams of workers prompted by local area or personal alarms to the levels normally expected for design basis measures. However, as stated at the start this section on FA and equipment handling, while the operations involve risks, they are an inherent part of UK ABWR operations and cannot be totally eliminated. As part of 'normal business', I would expect a future UK ABWR licensee to recognise this, and make sure its fuel route procedures and emergency arrangements do everything that is reasonably practicable to minimise these risks (including the installation of temporary shielding and other examples of international relevant good practice). Allying this expectation with the recognition that that the RBC and FHM will have A1 safety classifications, I judge the safety case presented by Hitachi-GE for these faults to be acceptable for GDA.

532. Note, the off-site consequences of dropped FA into the core is a 'standard' evaluation for a nuclear power plant safety case, and is usually taken to be the limiting design basis fuel route fault considered because of the associated fuel damage. Attachment D of Ref. 45 summarises the analysis performed and the results. A dose of 0.017 mSv is

[32] *US NRC Regulatory Guide 8.38 Revision 1 "Control of access to high and very high radiation areas in nuclear power plants" identifies a number of fuel route scenarios and examples where adequate controls on access are required. It also identifies the results of a review into overexposure scenarios relating to fuel assemblies and fuel route transfer anomalies. As part of the review of the radiological controls for BWR drywells during spent fuel movements, examples of the use of temporary shielding for spent fuel transfer to the storage pool, operational considerations (eg, restricting access to the upper drywell or evacuation procedures for the drywell during fuel movement), and enhanced employee training are all identified.*

predicted, effectively just at the BSO level. I will discuss this result, alongside other dose discussions, in Section 4.9.

4.5.2.3 Drop of heavy equipment into the core or the spent fuel rack.

533. In Attachment B of Ref. 45, Hitachi-GE has reviewed all the components handled by the RBC and FHM which could potentially be dropped into the SFP or reactor well, and considered their mass and maximum drop height to determine the limiting fault scenario (in terms of damaged fuel pins in either the reactor core or SFP racks). It concludes that the limiting event is a drop of the RIP impeller shaft (with the FHM grapple attached) into the reactor core. This is assumed to result in damage to all the pins in three FAs.

534. In my opinion, Attachment B is clear, systematic and auditable. It supports Hitachi-GE's decision to take the RIP impeller drop forward for detailed analysis and I therefore consider its selection to be appropriate.

535. The assumption of three damaged FAs results in a prediction of off-site and on-site consequences similar, but slightly larger, than those predicted for a FA drop at the reactor (for which less than two FAs were assumed to be damaged). My assessment conclusion are therefore also similar:

- the need for a rapid evacuation to mitigate high worker doses (but below the Numerical Target 4 BSL) down to a few tens of mSv (still above the BSO) is less than ideal because it is difficult to substantiate such actions to the level of reliability expected for DBA;
- however, the most important measures for nuclear safety are those taken which prevent a drop occurring in the first place.

536. Therefore, I am content with the design basis safety case for these drop faults for GDA, on the basis that the protection measures on the FHM and RBC are classified A1 and making an assumption that a future licensee will recognise the need to do everything reasonably practicable in terms of procedures and emergency procedures to minimise the likelihood of a drop and maximise the efficiency of any necessary evacuations.

4.6 Non-reactor faults

537. I have deliberately limited the scope of my assessment of non-reactor faults. Non-reactor SSCs have been subject to detailed assessment in other topic areas, notably in the management of radioactive waste topic area (Ref. 60). The objective for my fault studies GDA interactions in this area has been to establish that the building blocks of a safety case are in place to facilitate a targeted and proportionate assessment by specialists in other topic areas (in both parallel GDA assessments and in later phases of the UK ABWR project). Specifically, I have looked at:

- the identification of initiating faults (SAP FA.5);
- the identification of appropriate fault sequences (SAP FA.6);
- analysis of the consequences of fault sequences (SAP FA.7);
- the identification of suitable and sufficient safety measures, and their collation on a fault schedule (SAP FA.8).

538. In Section 4.2.4, I have already stated that I am satisfied with how Hitachi-GE has systematically identified non-reactor design basis initiating faults in Ref. 38.

539. In Section 4.2.3, I stated that I consider the UK ABWR categorisation and classification scheme set out in PCSR Chapter 5 (Ref. 31) to be appropriate for non-reactor faults.

540. Inspection of the fault schedule included in Ref. 38 shows that it lists all the bounding design basis events identified through the FMEA detailed in the same report, along with the claimed design basis safety measures (and their safety classification). Defence-in-depth measures that protect against the faults but are not credited in dose analysis are also listed for information. This is consistent with my expectations for a fault schedule, as established by SAPs ESS.11 and FA.8.

541. The choice to only present bounding design basis non-reactor faults on the fault schedule is consistent with the approach Hitachi-GE has followed for reactor faults (notably for external hazards). Given that it has included the most challenging non-reactor faults for the plant, it provides me with the confidence I am looking for that the risks from the UK ABWR away from the reactor can be appropriately managed. It does mean that the fault schedule is potentially not identifying every SSC that could end up having a role in the design basis safety case (some non-bounding faults may place unique claims on safety-classified SSCs that are not required for the bounding faults). However, there is a lot more detailed design and safety case development work to be done before the UK ABWR is constructed, operated and maintained, especially for the radioactive waste systems. I therefore see little value in trying to get an exhaustive list of SSCs claimed in the design basis safety case at this point in time. Making what I consider to be a reasonable assumption that the fault schedule will be kept under review during all phases of UK ABWR development and operation, I am content to leave it to the future licensee to ensure it has a comprehensive list of all claimed SSCs (and what they are claimed for), either in the fault schedule or through other equivalent means.

542. Hitachi-GE's analysis for the limiting non-reactor faults included on the fault schedule is presented in Attachment L of Ref. 39. The following events are considered:

- Off-Gas Radioactive Waste Systems
  - Off-gas treatment system failure
- Liquid Radioactive Waste Systems
  - Liquid radioactive waste system leak or failure
  - Resin transfer pipe rupture
  - Spread of containment due to maintenance failure
  - Catastrophic failure of powder resin storage tank
- Other Systems
  - Loss of clean up water function
  - Radiation dose increase in reactor building cooling water system (RCW)
  - Evaporator failure
  - Fuel assembly failure due to dropped load (equipment such as the irradiated fuel inspection machine falling into the SFP)
- Maintenance Faults
  - CUW Pump Inspection and Maintenance
  - FMCRD Replacement - Overhaul

543. The analysis is largely radiological (rather than thermal hydraulic or reactor physics). The SSC suffering the fault is described, the initiating event is discussed, and then the unmitigated consequences for the fault are detailed. The unmitigated consequences are used to confirm the appropriateness of the number of safety measures and the safety classification attributed to them on the fault schedule.

544. In most cases, the protection recommended by Hitachi-GE's guidance is lower than would be provided for a design basis reactor fault of a similar frequency because the unmitigated consequences are reduced. In several cases, Hitachi-GE has applied time limits in the unmitigated analysis to how long a worker could be expected to be in a vulnerable area, or for how long a leak will go undetected before routine surveillances identify a problem. In my opinion, the assumptions made in Attachment L are clearly

identified and appear to be reasonable, recognising that detailed procedures and surveillance requirements are not available during GDA.

545. As a final step, Attachment L of Ref. 39 provides mitigated radiological consequences analysis for both worker doses and off-site doses, and compares the fault sequence results (assuming the correct operation of the identified protective SSCs) with BSL and BSO targets defined in Ref. 53. This approach is fully consistent with my expectations, SAP FA.7 and Numerical Target 4 (Ref. 5).

546. For most of the considered faults, the mitigated on-site and off-site doses are below the BSO, or at least considerably beneath the BSL limit. Within the scope limitations of my assessment, I judge the extent of the analysis and the conclusions to be adequate for GDA. My assessment strategy is to leave judgements on how the designs compare against relevant good practice or whether risks could be reduced further to specialist ONR colleagues outside of fault studies.

547. The only faults that I do consider merit closer fault studies attention are those associated with the off-gas treatment system. On most power generating plants (conventional or nuclear) it is necessary to have a system to remove non-condensable gases from the main condenser to keep it at vacuum during electricity generation operations. However, on a direct cycle plant such as the UK ABWR, the vacuum system has to additionally deal with hydrogen and oxygen created by radiolysis, and provide abatement for radioactive species in the steam / condensate. The off-gas treatment system on the UK ABWR is therefore a much more important system from a nuclear safety perspective than equivalent systems on other reactor designs.

548. The management of the risks from hydrogen has been considered in detail by colleagues specialising in reactor chemistry and radioactive waste (Refs 110 and 60). However, the unmitigated radiological consequences of a rupture in the off-gas system are shown in Attachment L of Ref. 39 to meet the criteria for a design basis fault. Given its novelty from a UK-perspective, I judged it appropriate to look at it in some more detail as part of this fault studies assessment.

549. Attachment L considers representative fault scenarios which could result in a radioactive release. The first scenario is a guillotine pipe break in a pressurised, up-stream portion of the off-gas system, resulting in radioactivity from the reactor circuit being discharged direct to the local environment. The second scenario is a break in the down-stream charcoal adsorber which is holding-up short-lived fission-products and noble gases prior to discharge. The break is assumed to result in an instantaneous release of the radioactivity stored in the adsorber.

550. Assuming that an unmitigated release to the atmosphere could continue for eight hours, and that a field worker could be in the vicinity of a HVAC duct transporting activity from an off-gas room for up to one hour, Attachment L states the following:

- an off-gas rupture is an infrequent fault with unmitigated consequences between 1 mSv and 10 mSv off-site, and less than 20 mSv to workers;
- an adsorber break is an infrequent fault with unmitigated consequences between 10 mSv and 100 mSv off-site, and less than 20 mSv to workers.

551. This information has been used to establish that the consequences of both scenarios need to be protected against by a single B2 system. As previously stated in a general sense for non-reactor faults, I judge the justifications of the assumptions made, and the conclusions reached from applying Hitachi-GE's categorisation and classification scheme to be reasonable and adequately explained in Ref. 39.

552. The claimed protection is a B2 radiation high alarm in the rooms containing the break.[33] This prompts the automatic closure of B2 isolation valves upstream of the break, stopping further releases from the reactor circuit. As an analysis assumption, it is assumed the automatic isolation occurs within 16 minutes of the break first opening. The provision of automatic isolation is a design change compared to the Japanese reference plants which rely on manual isolation of the off-gas system in such circumstances.[34]

553. The mitigated consequences of the adsorber break bound those from the upstream off-gas system rupture. A 7 mSv off-site dose and a 2 mSv dose to workers local to the break area are predicted. While these are much lower than the Numerical Target 4 BSLs for infrequent faults (100 mSv off-site, 500 mSV on-site for initiating event frequencies less than $1x10^{-4}$ per year), they are high. Significantly, they are higher than the mitigated consequences of any reactor or SFP design basis fault.

554. I consider this to be an important point to be recognised about the UK ABWR, but not an unacceptable one. The potential unmitigated radiological consequences of a reactor fault with 872 FAs, or from SFP faults with three cores' worth of FAs are of course significantly higher than could occur from any fault involving the off-gas system. However, the reactor and SFP are provided with A1 and A2 safety systems which have been shown to be very effective in mitigating the consequences of any design basis fault. The B2 safety systems provided for the off-gas system do reduce the consequences of a fault, but not as dramatically as the reactor safety systems.

555. Hitachi-GE's approach of categorising safety functions based on the unmitigated consequences of an event (not the mitigated consequences), and then classifying SSCs based on their importance in delivering the identified safety functions is fully consistent with SAPs ECS.2 and ECS.3 (Ref. 5). The mitigated consequences may be comparatively high, but they are beneath the BSL. They are therefore acceptable if Hitachi-GE can demonstrate that it has reduced risks to be ALARP. To that end, Hitachi-GE has written a comprehensive topic report dedicated to showing just that (Ref. 111).

556. The scope of Ref. 111, initially supplied in response to an RO (Ref. 112) to address issues raised outside of the fault studies topic area, includes consideration of the extant design and whether improvements are reasonably practicable for benefit of safety in normal operations (beyond the scope of this report) and fault conditions. It includes a review of international relevant good practice and operational experience with off-gas systems on BWRs, notably on the causes of historic off-gas system failures. It observes that a pressure boundary failure could result from either a random failure or from a hydrogen combustion event. To reduce the likelihood of such a failure, it highlights the following features on the reference Japanese design:

- a welded design to minimise the number of flanges
- double isolations valves for branch pipes
- low pressure / negative pressure operation
- combustion proof design.

557. Ref. 111 reviews several additional measures for consideration in the UK ABWR design, identifying the following improvements as being reasonably practicable (in addition to automatic isolation and B2 area radiation and temperature monitors already discussed):

[33] *As additional defence-in-depth measures, additional protection in the form of B2 off-gas area temperature high alarms, C3 process monitor alarms and C3 radiation monitors on the stack are also identified.*
[34] *The closure of the off-gas system isolation valves will eventually cause an automatic turbine trip due to loss of condenser vacuum, followed by a consequential scram of the reactor. However, I am satisfied that there is an adequate reactor safety case for such an event (see Section 4.3.4) and therefore the radiological consequences of concern for the fault are all associated with the off-gas system (and not from failing to cool fuel in the core).*

- Upgrading C3 hydrogen detectors which prompt manual isolation to B2 hydrogen detectors and an automatic isolation of the off-gas system;
- Improving the quality assurance level of the design and adopting the 'ASME III' design code.

558. The proposals for additional improvements have been reviewed in more detail in the radioactive waste management topic area (Ref. 60) but from a fault studies perspective, I am satisfied that the scope and rigour of the ALARP review provided in Ref. 111 are consistent with my expectations and those set out in paragraph 698 of the SAPs (Ref. 5), given predicted the radiological consequences. Taking this into account, along with level of engineered protection provided should a breach occur, I judge the safety case for design basis faults associated with the off-gas system to be acceptable for GDA.

4.7 Beyond design basis faults

4.7.1 Reactor at-power BDBA

559. Ref. 46 summarises the transient analysis results for the 12 beyond design basis events identified in Ref. 38 (for SBO events, Ref. 46 references out to the dedicated topic report on SBOs, Ref. 40, for the relevant analysis). See Table 6.

560. To model the reactor thermal hydraulic transient, Hitachi-GE has generally used the SAFER code. To model containment pressures and temperatures during extended transients, the MAAP code has generally been used. The exception to this approach is the medium break LOCA with a failure to scram fault (a challenging ATWS event) for which TRACG has been used to model reactor behaviour and SHEX has been used to model the containment behaviour.

561. I have no objections to the use of these codes. With the exception of the MAAP, I have accepted the use of the same codes for DBA. The objective of the analyses performed in Ref. 46 is to show that the events will not escalate to a severe accident. Assuming that this is demonstrated, the reactor codes do not need extra functionality to model potential severe accident phenomena, and they should remain within their range of applicability.

562. The MAAP code has been used extensively to model containment behaviour during severe accidents and in support of the PSA, and judged to be appropriate (Refs 16 and 59). I judge the use of this internationally recognised code for modelling containment behaviour to be appropriate for BDBA.

563. The analysis with these codes has been performed with a reduced the level of conservatism when compared to the equivalent assumptions made in DBA. Typical of the assumptions made are:

- the reactor is operating at normal rated power and pressure prior to the fault;
- an industry standard decay heat curve is applied (which bounds a UK ABWR specific best-estimate decay heat curve) but without additional two-sigma uncertainties;
- no additional single failures in safety systems (most of the events are associated with at least one CCF in a major A1 SSC);
- SRVs open at their Class 3 automatic pneumatic actuation setpoints.

564. These assumptions are consistent with my expectations for BDBA as established by SAP FA.15 (Ref. 5) and Ref. 14. Both of these references state that best-estimate analysis should be performed for events outside of the design basis.

565. In principle, limited fuel damage is tolerable for beyond design basis events, as long as it is not associated with a major degradation of the core and numerical targets can be met. Hitachi-GE's declared strategy is to apply its infrequent (design basis) fault criteria for the fuel, RPV and PCV to beyond design basis faults, allowing it to claim that the mitigated consequences are no worse than those of the most onerous design basis events, and hence it is showing no 'cliff-edge'. I consider this to be a robust and welcome approach.

566. To come to judgements on the acceptability of the predicted radiological consequences for design basis events, the SAPs (Ref. 5) identify Numerical Target 4 as an appropriate benchmark for ONR assessors to use. However, Numerical Target 4 is explicitly for DBA and therefore does not apply for BDBA.

567. Hitachi-GE has recognised this and looked to Numerical Target 8 as the source of the off-site dose target for the deterministic consideration of beyond design basis events. Numerical Target 8 is primarily used by PSA to compare the aggregated frequencies from groups of sequences with similar consequences to the BSO and BSL frequency targets (ie the frequencies of sequences within a dose band are summated and compared to the targets). However, the text that accompanies Numerical Target 8 states that the risk from a facility should be balanced so that no single class of accident makes a disproportionate contribution to the overall risk. It is suggested that this can be shown by demonstrating that no single accident contributes more than about 10% of the frequency target for each dose band. Hitachi-GE has used this advice to apply a 10% factor to its own frequency limits given in Ref. 53 for 'Level 1' PSA and apply them as deterministic targets for the off-site consequences for beyond design basis events. I judge this to be a reasonable approach to adopt, noting that many of the at-power events do not result in a release outside of PCV and therefore an off-site dose calculation has not been performed.

568. Across the 12 events considered, Ref. 46 shows that the currently supplied engineered provision is sufficient to demonstrate compliance with the identified acceptance criteria, and therefore, in my opinion, it is adequately demonstrating the expectation that there should be no 'cliff-edge' just beyond the design basis region. Key to demonstrating this on the UK ABWR are:

- being able to depressurise the RPV to allow low pressure injection;
- the FLSS being available (due to physical separation and its own power supplies) to provide low pressure injection in the event of CCFs in the ECCS;
- the capability to vent the PCV, either manually or passively via the COPS.

569. As with some of the more challenging DBA transients, the BDBA for some extended transients shows PCV temperatures exceeding the 'traditional' design limits set out in Table 4 of this report. However, Hitachi-GE has justified the acceptability of these predictions by discussing the margin to the expected failure conditions for the PCV. I accept the arguments presented, although it reinforces the need for the assessment finding AF-ABWR-FS-07 to be addressed by a future licensee. I also observe that the best-estimate behaviour of the PCV in severe accidents has been considered in some detail in the parallel Step 4 assessments on PSA and severe accidents (Refs. 59 and 16), considering equivalent and more challenging accident sequences.

570. Ultimately, I am satisfied that through Ref. 46 Hitachi-GE has demonstrated the resilience of the UK ABWR to beyond design basis events, in accordance with post-Fukushima relevant good practice.

571. Set against the context of learning lessons from Fukushima, I consider it appropriate to discuss in more detail the resilience of the UK ABWR design to extended SBO events, in addition to the general observations above. In Ref. 40, Hitachi-GE has considered with BDBA the following events:

- a long term SBO (LOOP lasting up to seven days with a CCF of the EDGs);
- a long term SBO with an additional CCF of the B/B air-cooled diesel generators.[35]

572. From a modelling perspective, the first scenario is little different from the medium term SBO considered in the design basis. FLSS injection, and subsequently PCV venting, are both initiated within the first 24 hours, and therefore the controlled state reached in the medium term SBO (with falling pressures and temperatures) can be maintained for as long as FLSS water stocks last (seven days). The radiological consequences of venting are dominated by the initial release from opening the route from the PCV, and the extra mass of steam that is released over subsequent days in the long term event has a limited effect. This powerfully demonstrates that there is no cliff-edge (a key objective of BDBA) associated with the duration of either the SBO or venting operations).[36]

573. From a safety case and engineering perspective, Hitachi-GE states in Ref. 40 and Ref. 113 that after 24 hours the RDCF SRVs, which have been keeping the RPV depressurised, will close because their accumulators will have emptied. To address this, four of the seven RDCF SRVs are provided with 'switching valves' which allow them to be kept open by manually supplying nitrogen from a dedicated set of cylinders located outside the PCV. During Step 4 interactions, Hitachi-GE explained that this capability has always been included within the UK ABWR, but as a result of the formal deterministic consideration of this event, the functional requirements and safety case claims on this capability are clearly established and included (for example) on the fault schedule. I welcome this clarity on the safety case and engineering requirements for this extended event, and I am satisfied this requirement for switching valves is appropriately cascaded into documentation outside of the fault studies topic area.

574. I recognise that the second scenario is very extreme, however, I welcome its consideration as a means of demonstrating the resilience of the UK ABWR. The B/B is a significant addition to the UK ABWR design which provides a permanent engineered capability for Fukushima-type extreme events, and assuming it has failed, in addition to the redundant A1 EDGs, constitutes an onerous 'stress test' for the plant, well beyond the design basis. What Ref. 40 shows is that through the operation of:

- the RCIC for up to eight hours
- the manual opening of SRVs on eight hours via the switching valve capability
- the mobile FLSR after eight hours
- PCV venting.

a severe accident can be avoided (indeed, minimal differences in mitigated consequences are predicted compared to a design basis event), even if no ac power is available for seven days. Although this would not be the primary way of responding to an extended LOOP, I do believe the safety case is strengthened by including this analysis which demonstrates the UK ABWR's defence-in-depth. The analysis should also inform the sizing and deployment requirements for the FLSR.

4.7.2 Multiple line breaks

575. Within the fault studies safety case documentation, a design basis LOCA event is assumed to be restricted to the pipe with the initiating break. Consequential failures due to pipe whip or jet impingement are assumed to be prevented by distance, barriers or pipe restraints. In limited locations where this is not possible, the pipework is

[35] *The sequence frequency for SBOs with a CCF of the B/B diesel generators is below the 5 x 10^{-9} per year cut-off applied by Hitachi-GE in Ref. 46 for BDBA but the event was analysed deterministically at ONR's request as part of the response to RO-ABWR-009 (Ref. 49).*
[36] *As a result of the reduction in uncertainties in the modelling of the beyond design basis long term SBO, a lower dose is artificially predicted in Ref. 40 for the extended seven day SBO than is predicted by DBA methods for the 24 hour SBO.*

classified as ‘very high integrity’ with design and inspection requirements greater than those applied to ‘normal’ Class 1 pipework. These arguments are substantiated in the structural integrity and internal hazards portions of the UK ABWR safety case and are beyond the scope of this fault studies assessment.

576. In a late Step 4 addition to the UK ABWR safety case, Hitachi-GE has presented some deterministic thermal hydraulic analysis for two limiting LOCA cases (Ref. 114). The stated objective of the analysis is to support the structural integrity safety classification applied to two welds, such that if they did fail and result in more damage than has been assumed in the design basis safety case, there are no cliff-edge consequences to be considered.

577. The cases identified are:

- Case 1: A break in a weld point in FDW(A) with consequential damage to the HPCF and RHR in Division III;
- Case 2: A break in a weld point in FDW(A) with consequential damage to a MS Line and the RHR in Division I.

578. The analysis has used the SAFER code to model the long term reactor consequences of the fault sequences. The analysis has made conservative assumptions about decay heat and SRV setpoints etc consistent with design basis LOCA analyses (see Section 4.3.7), but it has not assumed any ECCS unavailability due to single failures or planned maintenance. The results have been compared to the same infrequent fault acceptance criteria as applied to other reactor beyond design basis faults. All fuel acceptance criteria are met.

579. To demonstrate the resilience of the PCV, the short term response of containment has been analysed for the bounding Case 2 with the M3CPT code, consistent with the approach for design basis LOCA faults (see Section 4.3.7.3). While most of the predicted temperatures and pressures are below the design values shown in Table 4, the D/W pressure does peak at 451 kPa(gauge) compared to a design value of 310 kPa(gauge). This is still below the COPS setpoint and limiting pressure for the PCV of 620 kPa(gauge), and is predicted to fall back to design levels within tens of seconds.

580. The identification of the two bounding cases is beyond the scope of this fault studies assessment report. However, I am satisfied that they represent events which are significantly more severe than have previously been considered as part of the design basis. I judge Hitachi-GE’s analysis methods to be appropriate for its stated objectives. I recognise the general conservatism included in its methods, and at the same time consider it reasonable that single failures and maintenance have been discounted for these beyond design basis considerations. Significantly, no fuel failures are predicted, which supports Hitachi-GE’s claim that there is no cliff-edge in terms of consequences if the assumed weld failures result in more damage to surrounding pipework than expected.

581. I am not unduly concerned about the short-lived high PCV pressures, noting that if for some reason the PCV did fail (or more likely the COPS opened), there would not be any significant off-site radiological consequences given that the fuel has been shown to remain intact.

582. These cases and the resulting analysis are not integrated into the wider beyond design basis safety case documentation established by PCSR Chapter 26 (Ref. 30) and Ref. 46 (these are mainly characterised by CCFs of protective SSCs in addition to an initiating event). Whether they should be will depend on the final outcomes of safety case decisions in the structural integrity and internal hazards topic areas, but for the purposes of GDA and considering the adequacy of the UK ABWR design, I have no concerns about the reactor’s resilience to the identified sequences.

4.7.3 Shutdown reactor BDBA

583. Ref. 46 summarises the transient analysis results for the nine beyond design basis events occurring in a range of applicable and / or limiting Operating State C sub-states. See Table 6.

584. For most of the events, the objective of the analysis is to show that a single source of makeup water can be provided to RPV and SFP before fuel is uncovered due to coolant boil-off (for LOCA faults, inventory losses through breaks also have to be compensated for). Which systems are available to provide makeup water, and the 'grace time' to initiate them, is a function of the CCFs assumed in the beyond design basis scenario, the permitted maintenance allowed in the sub-state being considered, the starting volume of water in each sub-state, and the assumed decay heat at the start of each sub-state. I have found these assumptions to be clearly set out in Ref. 46.

585. More so than for at-power beyond design basis events, claims are made on the mobile B3 FLSR to ensure adequate makeup water is provided. Additional claims and arguments are also made on C3 FP and C3 MUWC. Given that Hitachi-GE allows additional time for these systems to be initiated (as a conservative starting assumption, eight hours to line up the FLSR and FP, and a further hour to start injection), and the simplicity of the engineering requirement (the addition of makeup water), I am content with this.

586. In general the analysis in Ref. 46 shows that the available measures, with appropriate assumptions made for their initiation, can prevent fuel being uncovered. In the case of a loss of the operating RHR faults, with a CCF of all ECCS and FLSS, occurring in Operating State C-1 (the sub-state with highest decay heat), an assumption of nine hours for the FLSR and FP is too late to prevent fuel being uncovered. Hitachi-GE argues that it should be possible to initiate the FLSR and FP within five hours to prevent uncovery, and the MUWC could be available to provide more time. I am comfortable with these arguments, to which I make the additional observations:

- The beyond design basis event is considering the failure of two engineered A1 and A2 SSCs designed to protect against the loss of the operating RHR. I view providing further (third) permanent engineered means delivering makeup water (the most credible way of speeding up the supply of water) for a vulnerable state that only exists for a short-period of time to be grossly disproportionate.
- The strength of the BDBA for this event is that it emphasises the importance of design basis controls in the technical specifications on ECCS and FLSS availability in Operating State C-1.

587. Ref. 46 has also looked at the requirements for closing PCV hatches and airlocks following a beyond design basis event. In a 'real' emergency, workers evacuating from the containment will not be aware whether they are experiencing a design basis event or a beyond design basis event, and it would be reasonable to assume they follow the same procedures for closing hatches as they would for a design basis event. What Ref. 46 usefully shows is whether there is sufficient time to close hatches if the identified operations need to be successful for a long-term stable state to be reached. I am satisfied by the extent to which these considerations have been developed for GDA, but beyond design basis events in shutdown modes should also be taken into account by the future licensee when addressing AF-ABWR-FS-11 on outage plans and procedures for PCV evacuation.

588. Looking across the totality of what has been provided in Ref. 46 for beyond design basis shutdown faults, I am satisfied that Hitachi-GE has adequately illustrated the defence-in-depth provision included in the UK ABWR design, and shown that there is no cliff-edge just outside of the design basis. In some cases, margins are shown to be

tight however this is valuable for informing both availability controls in normal outage operations and the emergency procedures to be followed if an accident occurs.

4.7.4 SFP and fuel route BDBA

589. Five fuel route-related beyond design basis events are considered in Ref. 46 (see Table 6). Three are directly associated with the challenge of keeping fuel in the SFP adequately cooled, one is associated with a failure of the design basis protection on the FHM provided to stop an over-raise of an irradiated FA, while the final event considers the drop of a loaded transfer cask into the SFP.

590. The SFP cooling analysis is straight forward. For two of the events:

- loss of all FPC pumps with failure of FLSS;
- small leak of SFP with failure of the FPC and FLSS

the presented analysis shows that there is sufficient time, even with extended preparation time, to start providing makeup water via the FLSR before fuel becomes uncovered.

591. The third event considers the consequences of a seven day SBO on the SFP. No additional analysis is provided to that given for shorter duration design basis SBO events, in recognition of the fact that the FLSS is designed with sufficient capacity to provide adequate makeup water for seven days (in addition to any simultaneous reactor requirements).

592. I am content with the analysis for all three events. It should be noted that there is an additional defence-in-depth feature for cooling the bulk SFP FA inventory that is not credited in this analysis. Should a catastrophic drain down event occur from leak significantly larger than the liner failure assumed in the DBA and BDBA, the FLSS and FLSR makeup water is provided in the form of a spray. This spray is claimed in the PSA modelling to be effective in mitigating the consequences of a SFP severe accident, and in some circumstances preventing extensive fuel damage (this claim and the supporting analysis has been assessed by ONR colleagues specialising the PSA and fuel topic areas in Refs 59 and 71).

593. For the over-raise fault, Ref. 46 provides the results of a radiological consequences analysis, assuming the handled FA is raised to the physical limit permitted by the FHM (ignoring the C&I over-raise protection) and that local workers evacuate within four minutes of local area or personal alarms sounding. Unsurprisingly, even with the rapid evacuation, the predicted dose to a worker from a partially shielded irradiated FA is large (660 mSv). However, Hitachi-GE has compared this with a frequency / worker dose target from Ref. 53 that is based on Numerical Target 6 in the SAPs (Ref. 5). This states that the frequency BSO for a single accident with consequences to a worker on site in the band 200 to 2000 mSv is 1×10^{-5} per year. Hitachi-GE's estimated frequency for this event given in Ref. 44 is 1×10^{-8} per year, and therefore it claims that the relevant criterion has been met.

594. While this result does not provide any additional insights into the UK ABWR (it is to be expected that evacuation alone will not be very effective in preventing a large dose being received from an unshielded FA), I do welcome the fact that Hitachi-GE has followed a systematic and logical process which has resulted in this event being identified and subsequently analysed for comparison with a dose targets. In my opinion, the most significant point the analysis illustrates is the importance to nuclear safety of the engineered over-raise protection.

595. The conclusions to be drawn from the analysis of the cask drop into the SFP are similar. It is estimated that 220 FA in the racks will be damaged, resulting in mobile

fission products being released into the water and subsequently into the local environment. A dose of 2.3 mSv is predicted off-site, which is no challenge to the Numerical Target 8 BSO for a fault with consequences in the 1 to 10 mSv range. A dose > 200 mSv is predicted to workers on the operating deck (assuming they evacuate the area in approximately three minutes), which again is no challenge to the Numerical Target 6 BSO. While these positive comparisons against appropriate targets are welcomed, the main insights I take from the analysis are the limitations of evacuation in preventing a larger worker dose, and the importance of design basis measures which stop the drop occurring in the first place.

596. Hitachi-GE provides very limited discussion on why it believes it is not reasonably practicable to provide additional engineered protection on the basis of these BDBA results, and therefore why the extant provision is adequate. However, I observe that the challenges the UK ABWR faces with over-raise faults and drops of heavy loads into the SFP are the same as those faced on many nuclear facilities. I have already judged the design basis measures (A1 crane protection systems, A1 + A2 over-raise protection) to be adequate and consistent with relevant good practice, and given the positive comparison made against numerical targets for these very low frequency sequences, I believe it would be grossly disproportionate for more to be done. For SFP cooling, the main requirement is to provide makeup water, and Hitachi-GE has demonstrated there are multiple ways of supplying that water.

597. In conclusion, I welcome the systematic approach to considering beyond design basis events which has resulted in SFP and fuel route faults being considered in addition to reactor-based events. I am satisfied that appropriate criteria have been met and no additional engineered measures are required.

4.8 Computer codes and methods

4.8.1 Assessment strategy for computer codes and methods

598. Hitachi-GE's fault studies safety case makes extensive use of the results of computer codes and models. My assessment judgements and conclusions presented in the preceding sections of this report have largely assumed that the analysis results reported, for example, in PCSR Chapter 24 (Ref. 29) and Ref. 39 are appropriate. In this section, I will detail the assessment I have undertaken on Hitachi-GE's codes and methods that has allowed this approach to be taken.

599. The AV series of SAPs provide guidance on what should be considered when seeking assurances on the validity of data and models (Ref. 5). Informed by this guidance, I have considered if Hitachi-GE's models:

- adequately represent the UK ABWR design (SAP AV.1);
- models adequately represent the relevant physical phenomena (SAP AV.2);
- use valid data (SAP AV.3);
- are subject to adequate quality management (SAP AV.4);
- have been used to perform sensitivity studies so that uncertainties and variations in data are understood (SAP AV.6);
- are adequately documented to allow external review (SAP AV.5).

600. IAEA guidance is also available for reactor transient analysis (Ref. 17), and this has also informed my assessment.

601. The computer codes and calculation routes used by Hitachi-GE for DBA and BDBA are summarised at the start of PCSR Chapters 24 and 26 respectively (Refs 29 and 30) as well as their main supporting references (Refs 39 and 46). I have also included a summary in Table 5 of this report, linking the various codes used to applicable parts of my assessment.

602. I have adopted a sampling approach to gain confidence in the totality of Hitachi-GE's methods and associated quality management systems, looking in some detail at four 'work-horse' computer codes used for by Hitachi-GE for the bulk of its reactor (at-power) transient analysis:

- ODYN
- SAFER
- SHEX
- LAMB.

603. I have also looked at the general adequacy of the TRACG code with a focus on the reactor physics modelling utilised for ATWS and CR reactivity faults. My assessment is set out in Section 4.8.2.5 below.

604. The core physics simulator PANCEA (extensively used as part of Hitachi-GE's calculation route for CR reactivity faults) has been assessed outside of this fault studies report by ONR fuel and core specialists (Ref. 71). The MAAP code used for BDBA modelling has been considered in Step 4 assessment reports on both severe accidents (Ref. 16) and the PSA (Ref. 59). I have therefore excluded these codes from my sample.

605. In earlier sections of this report, I have explained how I have used independent transient analysis to reanalyse the behaviour and consequences of specific faults predicted by Hitachi-GE's methods. In addition to giving confidence in the resilience of the UK ABWR to individual faults and benchmarking Hitachi-GE's methods against GRS's state-of-the-art modern codes, the process of developing these independent models has provided me with insights into Hitachi-GE's available documentation, its controls on the UK ABWR design and the availability of data. These insights are set out in Section 4.8.3 below.

606. For shutdown faults, Hitachi-GE has made extensive use of spreadsheets to predict the consequences of reactor faults in shutdown modes and faults involving the SFP. Given that these lack the track record and documentary evidence of traditional codes, I have chosen to sample their use to gain confidence in their adequacy for the faults they have been applied to. My findings from this review are in Section 4.8.4 below.

607. Finally, in Section 4.8.5, I have looked at how Hitachi-GE and its contractors have controlled its analysis.

608. Note, my assessment of the adequacy of Hitachi-GE's methods for determining the radiological consequences of faults is detailed separately in Section 4.9, as part of wider review of UK ABWR dose analysis.

4.8.2 Codes and methods for reactor DBA (at-power)

609. As set out in my Step 4 assessment plan (Ref. 1), my principal method of gaining assurance in the validation status and applicability of Hitachi-GE's main computer codes for the modelled reactor transients was to commission experts working for ONR's TSC GRS to review ODYN, SAFER, LAMB, and SHEX against the expectations of the SAPs, applicable TAGs, and international relevant good practice (including Ref. 17).

610. GRS's findings are reported in Ref. 20 and are summarised below as part of my wider assessment of each code. The targeted assessment of TRACG was beyond the scope of the GRS contract and therefore reflects my own review, informed by expert advice from ONR fuel and core specialist colleagues (Ref. 115).

4.8.2.1 ODYN

611. Hitachi-GE analyses short-term transients with symmetric neutron flux using an ODYN-ISCOR-TASC calculation chain developed by its sister-company (and contractor for the UK ABWR GDA) GE-Hitachi.

612. ODYN simulates the transient response and drives the single channel model TASC, which determines if boiling transition in the limiting core channel occurs and calculates the resulting peak cladding temperature. ODYN uses a 1D model for both the neutron kinetics and thermal hydraulic behaviour of the reactor.

613. GRS concluded that:

- ODYN is adequate for modelling transients without strong asymmetries in the neutron flux and without core uncovery for the UK ABWR.
- ODYN's 1D approximation is suitable for fast-acting transients where the shape of the core radial flow and/or power distributions remain close to their nominal shapes prior to scram. This is not the case for design basis faults with strong asymmetric distortions of core flow prior to scram.
- ODYN has been successfully validated against relevant single effect and integral test cases and benchmark problems. The validation evidence shows that the main output parameters for DBA such as peak cladding temperature, RPV pressure and RPV water level are predicted with sufficient accuracy within ODYN's applicability range. While overcooling transients are not covered by specific validation results, the pressure-wave void collapse transients are well validated and bounding for DBA.
- ODYN has been successfully validated to model the effects of boron injection under the conditions found in the 1980s BWR test rigs.
- The documentation of ODYN and its models is sufficient for a technical review.

614. In addition to GRS's findings, I take additional assurance in the adequacy of ODYN for ABWR DBA because it has been accepted by US NRC as a licensing code (Ref. 116) and has been subject to repeated regulatory review and validation by it. Moreover, the development and maintenance of the code follows the respective quality control requirements of US NRC.

615. As discussed in Section 4.3.10, I had some initial concerns about the conservatism included in the ODYN ATWS analysis, given that Hitachi-GE was assuming a restart of feedwater (tripped earlier in the transient by the A2 ATWS system) to keep the RPV water level within the scope of ODYN's capabilities. However, I am satisfied that the sensitivities performed by Hitachi-GE with the more sophisticated 3D TRACG model have shown that the base-case ODYN results are adequate.

616. Across a wider tranche of DBA faults, I am also reassured by the observation that predictions by the ODYN-ISCOR-TASC calculation chain for short-term parameters such as peak cladding temperature or RPV pressure bound the equivalent results from the more realistic TRACG code. I attribute this to the significant conservatisms implemented in the ODYN-ISCOR-TASC calculation chain, particularly for the determination of a violation of the MCPR safety limit and the simulation of peak cladding temperatures.

617. There are of course some uncertainties in any code prediction but I am satisfied that these are covered by pessimistic initial and boundary conditions and the inherent conservatisms in the code. For example, the ODYN calculation chain assumes that boiling transition occurs when the MCPR limit of 1.06 is reached while assuming a starting critical power ratio at the operational limit, irrespective of the specific conditions of the fault.

618. In summary, informed by GRS's findings, I judge ODYN to be an adequate DBA tool for UK ABWR transients within its range of applicability, and I am satisfied its results can be used to support Hitachi-GE's relevant safety case claims for GDA.

4.8.2.2 LAMB

619. Hitachi-GE uses the GE-Hitachi code LAMB for predicting boiling transition in the core during the initial depressurisation phase of a LOCA fault. LAMB has been validated against applicable LOCA tests and shows acceptable agreement with test results for the relevant test phases (Ref. 117).

620. The review by GRS (Ref. 20) has concluded that LAMB is applicable to the UK ABWR and can simulate the initial depressurisation phase of a LOCA fault until onset of lower plenum flashing. This is adequately supported by validation evidence. Uncertainties are covered by conservative initial and boundary conditions.

621. On that basis, I am satisfied that the LAMB code, and how Hitachi-GE has utilised it in support of the UK ABWR LOCA safety case, is adequate for GDA.

4.8.2.3 SAFER

622. Hitachi-GE uses the GE-Hitachi developed SAFER code to simulate RPV inventory and important core safety parameters as part of a longer-term consideration of LOCA transients. SAFER is also used to demonstrate the effectiveness of diverse protection systems delivering FSF-2 functions.

623. SAFER uses a simple nodalisation of the RPV and connecting systems are represented by boundary conditions (Ref. 118). SAFER includes models for core uncovery and core heat-up with cladding oxidation and cladding rupture. SAFER is also provided with models to simulate the re-flooding of the core by the ECCS, as well as FLSS injection. It uses simple representations for calculating heat transfer by nucleate boiling, transition boiling, film boiling, steam cooling and mist cooling. SAFER has been validated against a wide range of conditions and for the key events in LOCA scenarios for BWR designs with both jet and internal pumps (earlier BWRs had jet pumps instead of the RIPs provided on the UK ABWR).

624. GRS has reviewed the available evidence on SAFER against the SAPs and concluded the following (Ref. 20):

- SAFER is suitable for calculating the long-term RPV inventory and important parameters like peak cladding temperatures for LOCA faults and transients. The models adequately represent the relevant phenomena.
- SAFER has been successfully validated against relevant single phenomena and integral tests. The main output parameters like RPV pressures, RPV water levels, core mass flow and peak cladding temperatures are covered by the validation tests.
- SAFER is applicable for the UK ABWR and produces sufficiently accurate results. SAFER predictions for peak cladding temperatures are bounding for experimental values and SAFER predicts faster core uncovery and later re-flooding than observed in test data.
- Uncertainties in data and assumptions are enveloped by conservative initial and boundary conditions as well as inherent conservatisms within SAFER.
- The available evidence supports an external technical review.

625. My own judgements on SAFER are informed by that fact that it, and its precursor codes SAFE, CHASTE and REFLOOD, and the calculation chain it is part of, have been subject to review by the US NRC (Ref. 119) and have been accepted for licensing applications.

626. I am aware that Hitachi-GE has used SAFER to support the derivation of success criteria for the PSA Level 1 (Ref. 120). While I have not reviewed these calculations in detail, I am content that SAFER has been used within its range of applicability.

627. I conclude that SAFER is applicable to the UK ABWR and, within its range of applicability, adequately represents the relevant phenomena and processes. I am satisfied that SAFER provides conservatively bounding results for important parameters like RPV pressure, RPV water level and peak cladding temperature, and I judge its use for LOCA faults and other extended transients to be adequate for GDA.

4.8.2.4 SHEX

628. Hitachi-GE uses the GE-Hitachi code SHEX for analysis of long-term containment behaviour during design basis faults including LOCAs and SBOs. SHEX was originally developed for GE-Hitachi's Mark III BWR containment (Ref. 121). Energy balances and state equations are used to compute the pressures and average gas space temperatures in the PCV. Specific models for heat transfer and condensation phenomena in the containment and also vent line clearing are provided. SHEX contains a simple RPV model which drives the thermodynamic source term for the PCV.

629. GRS has reviewed the available documentation for SHEX against the SAPs and other sources of guidance, and concluded the following:

- The available documentation and validation evidence applies to SHEX-03 and not SHEX-06P, the version actually used for UK ABWR DBA. Consequently, GRS could not positively assess the validation status of SHEX.
- The significant differences between the UK ABWR PCV and the Mark III containment limit the representativeness of SHEX.
- The lumped-parameter approach in SHEX is not in line with the state-of-the-art for containment analysis codes.
- SHEX could over-predict the efficiency of heat removal from the PCV in the long-term phase from break mass flow ('cold' ECCS injection spilling out of the reactor circuit through a line break).
- Important parameters in SHEX are user inputs and the results depend on the adequacy of these inputs.

630. I discussed these observations with Hitachi-GE in a routine GDA Step 4 meeting (Ref. 122). It responded by bringing to my attention the following points that were not made in the review documentation supplied to GRS:

- SHEX has been routinely used by GE-Hitachi in licensing applications to US NRC and other international regulators.
- SHEX has been successfully benchmarked against other containment codes, including GOTHIC.

631. I have identified other reasons that support Hitachi-GE's claim that SHEX is suitable and adequately conservative for DBA:

- Hitachi-GE is artificially transferring non-condensable gases from the D/W to the W/W in the initial phase of a LOCA fault (Ref. 39). I consider this to be a substantial conservatism in the modelling of the short and medium term pressures in the PCV.
- During extended transients, assuming thermal equilibrium has been reached, average containment pressures and temperatures will be largely determined by energy and mass balances between major containment compartments. This is what is implemented and output by SHEX, and in many cases a more sophisticated model is not needed.

- GRS's independent confirmatory calculations with COCOSYS generally support the conclusion that SHEX long-term average predications are sufficient for DBA.
- Hitachi-GE has undertaken containment performance analysis with a UK ABWR MAAP model to the support the PSA (Ref. 120). Inspection shows that the MAAP results are generally consistent with, but bounded by, the equivalent SHEX results.

632. Considering all these observations, in my opinion, SHEX is a limited code that is not accompanied by the level of documentation and validation evidence available for Hitachi-GE's other DBA codes. The transient analysis for the immediate PCV conditions following a LOCA (see Section 4.3.7.3) and the long-term PCV conditions during a SBO (see Section 4.3.8) show that its results cannot be compared in a simple way to acceptance criteria. Additional justifications and off-line calculations have been required. I would encourage any future licensee to review the use of SHEX, and through assessment finding AF-ABWR-FS-07, I have already asked for improvements and clarifications in the acceptance criteria its outputs are compared against. However, I am ultimately satisfied that Hitachi-GE's design basis safety case for the PCV is suitably conservative and therefore adequate. The SHEX results are a major part of that safety case. I am therefore content with SHEX's use for GDA and even its potential use beyond GDA, as long as its weaknesses are understood, managed and improved upon.

4.8.2.5 TRACG

633. TRACG is a best estimate transient calculation code for BWR systems. It can model a wide range of transients from simple operational transients to LOCAs, ATWS faults and instability transients (Ref. 29). It is therefore much more flexible and capable than Hitachi-GE's other analysis codes. Neutron kinetics calculations of BWR reactor core, thermal hydraulic calculations for two-phase flow, fuel rod and structure temperature calculations, and control system calculations can all be coupled with each other to evaluate a BWR's transient response.

634. TRACG has the following characteristics (Ref. 123):

- a modular structure for basic thermal hydraulic components with flexibility for the detailed nodalisation;
- a multi-dimensional two-fluid model for the reactor thermal hydraulics;
- Specific models for flow regime, choked flow, counter current flow limitation, friction, form losses, and special geometries;
- a 3D neutron kinetics model;
- a sophisticated heat transfer package

635. TRACG's 3D neutron kinetics model is consistent with the BWR core simulator PANACEA used for the core design of the UK ABWR (see Ref. 71).

636. The use of a best estimate code, in combination with a suitable treatment of uncertainty is fully in line with modern relevant good practice (see for example Ref. 14), and therefore I have no concerns, in principle, about its use for DBA.

637. As part of my review of its thermal hydraulic capability, I have sampled the calculation of pressure losses, dry surface heat transfer, interfacial heat transfer, and condensation models. I found no major weaknesses and I am satisfied that the implemented models allow an accurate representation of the UK ABWR (Ref. 115).

638. TRACG and its individual models have been extensively validated against single effect tests, integral tests, benchmark problems and full scale BWR plant data. I am satisfied with the validation evidence presented in Ref. 123. My review of the results for integral

tests simulating plant transients has found good agreement. In my judgement, there are not any alternative codes available that are likely to improve on TRACG predictions.

639. As a general observation, I am impressed by the quality of the documentation which is available for TRACG.

640. The use of TRACG has been somewhat limited in GDA; it has mainly been used to support the conclusions reached by the older, more limited but conservative calculation routes. If greater use is made of it in the future to support the UK ABWR safety case and operation, I would expect to see improved discussion and sensitivity studies on the nodalisation adopted and the uncertainties applied in accompanying documentation. However, I judge both the code and its use to be consistent with my expectations (as established by the SAPs) and I have no issues with its appropriateness for the UK ABWR GDA.

4.8.3 Insights from independent confirmatory calculations

641. In addition to providing assurance and insights for individual fault transient, the independent confirmatory analysis performed GRS has also informed my more general opinions on strengths, weaknesses, and levels of conservatism in Hitachi-GE's methods.

642. Hitachi-GE's DBA calculation chains for the ODYN and SAFER use conservative codes and pessimistic assumptions. The containment analysis codes, like SHEX, are run decoupled from the transient analysis in the RPV and are geared towards pessimistic results as well. They have been shown to be long-established approaches that have supported the licensing and continued operation of multiple BWRs around the world, and have been subject to a significant amount of regulatory attention over the years. However, apart from TRACG, I do not consider them to represent the state-of-the-art. They were developed at a time when computing power and time was significantly more constrained than it is now.

643. In contrast, GRS's code ATHLET is intended to produce realistic results. Its model of the RPV and its connecting systems is more detailed than Hitachi-GE's models and includes non-safety systems. It is less constrained in the phenomena it can predict and the parts of a transient it can model. It can also be coupled to a reactor physics package (QUABOX/CUBBOX) and a containment analysis code (COCOSYS) to better model the combination of phenomena and the feedback effects that would occur in a real transient. A bounding, conservative approach remains a fundamental requirement for DBA, but this can be achieved applying appropriate uncertainties, pessimising systems' performances, and assuming limiting boundary conditions. This combination of best estimate codes with conservative boundary conditions is a more modern approach that is good practice in the UK and internationally.

644. From the small sample of the totality of the Hitachi-GE fault sequence transient analysis independently repeated by GRS, I have formed a view that Hitachi-GE's less modern tools are adequate in characterising the progression of a fault sequence as well as plant parameters for safety acceptance criteria, timings for operator actions and demonstrating the effectiveness of safety systems. In some cases, Hitachi-GE already knew it needed to fall-back on its more capable TRACG code to support or enhance its traditional methods. In other cases, it reverted to TRACG (or other methods) to provide further substantiation retrospectively in response to GRS-informed challenges I put to it. Ultimately though, while I would encourage future licensees to consider modernising some of its methods, GRS's analyses do not undermine Hitachi-GE's claims about the appropriateness of its methods.

645. In order for GRS to develop its independent UK ABWR models, it needed a considerable amount of design detail from Hitachi-GE. A valuable secondary outcome of requesting this information for GRS was that it gave me confidence in Hitachi-GE's knowledge, levels of documentary evidence, and ownership of both its design and the modelling assumptions in its own analysis. While I observed some minor weaknesses, generally the design detail was readily available and Hitachi-GE could explain how it was used in its own analysis. This is important for my assessment against SAPs. AV.1, AV.3 and AV.5, but it also suggests that an effective knowledge transfer should be possible with future licensees.

4.8.4 Codes and methods used for shutdown and SFP faults

646. I established during the course of GDA Step 4 that Hitachi-GE was making extensive use of spreadsheet calculations for the open RPV and SFP safety case. I considered it very important to gain confidence in both the technical basis of the spreadsheets and the quality management system controlling the calculations. However, not unreasonably, the spreadsheets and quality management documentation was in Japanese.

647. To facilitate to my review, Hitachi-GE produced a detailed description (in English) of its spreadsheet tool (Ref. 124), alongside one example of the Japanese spreadsheet being applied to a design basis fault. Aided by Ref. 121, I have established that the spreadsheet tool has the following characteristics:

- it calculates the energy and mass balance for an ideally mixed pool open to atmosphere at standard pressures under thermal equilibrium conditions;
- properties of water and steam are implemented by their enthalpies at operating conditions and the boiling point only;
- the decay heat from the core or in the SFP at the start of a fault condition is based on a 'May-Witt' decay heat model with an additional allowance to compensate for uncertainty and is conservatively assumed to remain constant until normal water level is re-gained;[37]
- heat losses and heat transfers to structures are neglected;
- interaction with the R/B air space is neglected;
- elevations and water volumes in the RPV, reactor well, DSP and SFP are based on UK ABWR dimensions;
- LOCA mass flow rates are calculated with Toricelli's law;
- injections from the ECCS and FLSS are considered at their nominal enthalpy values.

648. My assessment as led me to the following judgements (Ref. 125):

- Hitachi-GE has adequately demonstrated that the May-Witt decay heat curve is bounding for shutdown faults and the SFP (see Refs. 65 and 66). Assuming a constant decay heat for the transient part of a fault introduces a substantial amount of conservatism.
- Plant characteristics and performance parameters of the ECCS and FLSS in the model are representative for the UK ABWR.
- The implementation of the enthalpy and mass balances is adequate and simplifications generally lead to conservative results for RPV water level and temperature. Neglecting heat losses and evaporation below the boiling point introduces considerable conservatism.
- The calculated LOCA mass flows are demonstrably bounding.
- The tool optimistically neglects that swell levels due to boiling in the RPV would lead to leakages from a break location even if the water level has dropped

[37] *May-Witt is a GE-Hitachi decay-heat model which considers contributions from both fission products and heavy-element decay energy.*

below the break location. However, this is enveloped by the other conservatism in the tool and does not change safety case conclusions.
- The analysis method has been implemented correctly in the calculation sheets.
- Although Hitachi-GE has not carried out an investigation of sensitivities, I am satisfied that the conservative approach produces enveloping results.
- While Hitachi-GE's documentation for the spreadsheet tool could be improved, it is sufficient for my purposes in GDA.
- There is no attempt to provide any validation evidence for its results, as would be expected by SAP AV.2 and is done as a matter of routine for Hitachi-GE's computer codes for at-power faults.

649. Hitachi-GE has performed severe accident calculations for the shutdown reactor with the MAAP code (Ref. 126). Considering the differences in assumptions and starting conditions, these results give me additional confidence that the spreadsheet produces enveloping results for RPV and SFP water level. I have also performed some limited independent calculations of my own using GRS's ATHLET code which suggest that Hitachi-GE's spreadsheet tool is conservative in its predictions RPV and SFP water levels (Ref. 125).

650. In conclusion, I am satisfied for the purposes of GDA that Hitachi-GE's methods support its safety case conclusions for shutdown operations and the SFP. However, I do not consider a Japanese spreadsheet tool, with limited documentation and verification / validation evidence, to be sufficient to support an operational safety case 'owned' by a UK licensee. As a minimum, a future UK licensee will need to demonstrate it has confidence in both the technical content and controls on Hitachi-GE's spreadsheet tool. A version of the tool in English that would allow a UK licensee to check and have confidence in the results of a potentially Japanese supply chain for its analysis could be an easily achievable outcome.

651. I also recommend that a UK licensee considers the conservatisms inherent in Hitachi-GE's spreadsheet tool, and whether a best-estimate state-of-the-art computer code could better predict reductions in water levels, times to boiling and R/B pressures that could inform the development of emergency arrangements, evacuation requirements, setpoints for blowout panel etc. An alternative computer code could also be accompanied by superior documentation and quality controls.

652. I have therefore raised the following assessment finding:

- AF-ABWR-FS-13: Hitachi-GE has made acceptable use of spreadsheets and hand calculations to support its safety case for shutdown faults and the spent fuel pool (SFP). However, these are not supported by the same level of validation evidence as the computer codes extensively used for at-power fault analysis and the accompanying verification records are in Japanese. As a result, the licensee shall review its design basis tools (DBA) tools and methods for shutdown faults and faults in the SFP to ensure it has confidence in the available verification and validation evidence, while also demonstrably understanding and owning the predicted results.

4.8.5 Quality assurance and configuration control of analysis models

653. SAP AV.4 establishes a vital expectation that computer models and data used to support the safety case should be developed, maintained and applied in accordance with quality management procedures.

654. To gain an appreciation of processes Hitachi-GE has followed, I undertook two targeted inspections at its Japanese offices through the course of GDA (Refs 127 and 128). I established the following:

- The majority of the computer codes and models used by Hitachi-GE to support its design basis safety case were developed and remain actively maintained by its sister company GE-Hitachi.
- The computer codes and models are stored and run from servers operated by GE-Hitachi. Changes to the models are subject to strict controls and verification, defined by GE-Hitachi procedures and policies. These procedures and policies are used to support operating BWRs in the US, and are therefore subject to regulatory attention and approval from US NRC.
- Hitachi-GE has appropriate controls (paper-based and in Japanese) for identifying the requirements for individual calculations, identifying necessary changes to controlled models, and checking that changes have been made.
- The bulk of the transient analysis has been performed by GE-Hitachi under contract to Hitachi-GE. I am satisfied with how Hitachi-GE specifies the requirements for analysis, GE-Hitachi updates it reference models accordingly, and then supplies the results back to Hitachi-GE.
- Hitachi-GE performs appropriate checks and then accepts GE-Hitachi results, through controlled processes and interfaces.

655. Through the course of GDA, I have had no reason to doubt the level of qualification and experience of Hitachi-GE's personnel specifying and accepting the analysis results, or the GE-Hitachi personnel performing the analysis.

656. SAP AV.1 defines an expectation that theoretical models should adequately represent the facility being considered. An advantage that the UK ABWR has over other new reactor types is that the basic design is mature and Japanese reference plants have been built. As a result, Hitachi-GE had access to well-developed ABWR models from the start of the project (under strict version control by GE-Hitachi) and there is a sound basis for the majority of the modelling assumptions on, for example, volumes, pipe lengths, control system responses etc. There have been design changes during the course of GDA, but I am content that few have influenced major parameters like the RPV or PCV volumes. The small number of changes which could influence the analysis results were identified by Hitachi-GE and incorporated into GE-Hitachi's models following the established process (for example, the increase in RHR heat exchanger capacity).

657. I therefore have no concerns for the quality assurance procedures followed by Hitachi-GE and its contractors, and I am satisfied the analysis models adequately reflect the UK ABWR design declared for GDA.

658. Looking past GDA, I would expect the pace and volume of design changes to increase as site-specific and detailed design work in undertaken. It will be impossible to update all the UK ABWR DBA after every design change (or even demonstrate definitively the impact of a proposed design change on the DBA), and therefore it will be important that the following is done:

- the design at any point in time needs to be clearly defined;
- any changes to the design need to be controlled through appropriate arrangements which include consideration of potential impact on safety analysis modelling;
- computer models and generations of analyses need to be linked to a design reference point, with visibility of what modifications have been included since the last update was performed, and what modifications should be included in future updates.

659. I am confident that the first two controls will be put in place by a UK licensee as a fundamental part of its Licence Condition 20 arrangements (Ref. 129). However, at the moment, the control of the various input decks against the declared GDA design reference point is based upon expert judgement by Hitachi-GE engineers, and the

internal procedures of GE-Hitachi. I cannot see any 'line-of-sight' between the design that will be under the control of the future licensee after GDA, and the models residing on GE-Hitachi's servers. Eventually, the licensee may take ownership of the computer models, or even develop its own independent methods, but I am assuming the bulk of the fault studies analysis work supporting safety case submissions in the next few years will be based largely on what was done in GDA. I have therefore raised the following assessment finding:

- AF-ABWR-FS-14: Given that the control of many of the computer models which support the UK ABWR safety case is ensured by the knowledge and processes of a third party (GE-Hitachi), the licensee shall put in place version controls and change management processes to ensure that there are clear links between the latest generations of the fault studies analyses (and the computer models which generated them), and the changing UK ABWR design reference it is controlling through its normal arrangements.

4.8.6 Conclusions

660. Overall, I judge that Hitachi-GE's methods and tools that support the DBA safety case are sufficient for GDA. The models are representative of the UK ABWR and its phenomena and processes, and are based on valid data.

661. While large parts of the methodologies employed do not represent the state-of-the-art, they have a long-established pedigree, are well documented, well controlled, and subject to international regulatory attention. Crucially for DBA, they have been shown to be conservative in almost all cases examined.

662. For shutdown and SFP faults, Hitachi-GE has made use of spreadsheets rather than established computer codes. While I am content that these spreadsheets have been subject to appropriate quality assurance and are predicting conservative results that support the GDA safety case, the expectations of the AV series of SAPs are not complied with to the level that is achieved with the main reactor analysis codes. It will be much more difficult for a licensee to demonstrate ownership and control of the safety case in those areas where a spreadsheet in Japanese is providing the bases for claims and arguments, and therefore I have raised assessment finding AF-ABWR-FS-13 for the use of these tools to be reviewed.

663. I have gained confidence through the course of GDA Step 4 in how Hitachi-GE and its contractor has controlled and managed the large volume of analysis undertaken. This achieved by a robust interface and procedures between Hitachi-GE and GE-Hitachi. However, it is unclear to me how after the GDA the link between an evolving design (under the control of the licensee) and the DBA models (effectively under the control of a third-party) will be ensured, so a further assessment finding (AF-ABWR-FS-14) has been raised for appropriate controls to be put in place.

4.9 Radiological consequences

664. A fundamental objective of fault studies is to show through the use of appropriate tools and techniques, on a conservative basis, that the consequences of fault sequences are ALARP (SAP FA.7). Judgements on whether the consequences are ALARP have to be informed by an appreciation of the radiological consequences of faults to people (on and off-site), and by comparing those predicted consequences with targets that represent relevant good practice (or, in some cases, legal requirements). For design basis faults, the applicable targets are provided by Numerical Target 4 in the SAPs (Ref. 5). For beyond design basis faults, Numerical Targets 6 and 8 are applicable.

665. In some cases, detailed radiological consequences analysis is not necessary. For many reactor faults, calculations are not necessary to demonstrate that the

unmitigated consequences are very severe. There are also faults where it is clear that if safety features operate correctly, there will be no additional radiological consequences beyond those expected in normal operations. In such circumstances, I have no expectation that radiological consequence calculations are performed.

666. However, some reactor or SFP faults, even with the correct operation of protective measures, will involve the loss of at least one physical barrier preventing the release of radioactive material (for example, MS line break fault outside of containment or a FA drop), and therefore a dose calculation is necessary, even if other acceptance criteria have been met.

667. Hitachi-GE's approach to dose calculations is consistent with these expectations and is appropriately integrated into its fault studies documentation:

- For many reactor faults analysed in Ref. 39, all identified acceptance criteria are met, so there are no challenges to any barriers and no radiological consequence analysis is presented.
- For those reactor faults which are directly associated with a break or bypass of a barrier, dose analysis has been presented in Attachment F of Ref. 39. However, the consequences are limited by the demonstration of acceptance criteria, notably no consequential damage to the fuel cladding and the PCV remains intact.
- Dose analysis has also been performed for those reactor events where the management of the transient involves a planned release of radioactive steam, notably PCV venting for SBOs and the diverse means of providing the FSF-3 function, and the release of steam from the secondary containment generated during shutdown and SFP faults. This radiological analysis is generally reported alongside the main sections detailing other aspects of the DBA for the fault in question.
- The DBA for fuel route faults involving mechanical damage to fuel assemblies (or a loss of shielding) is almost exclusively based on radiological consequence analysis (Ref. 45).
- The DBA for non-reactor faults is also almost exclusively radiological consequences focused analysis, and is consolidated together in Attachment L of Ref. 39.

668. A comparison of Hitachi-GE's predicted dose values against numerical targets in the SAPs in order to reach conclusions on ALARP for individual faults is my ultimate assessment goal in this area. However, before I could do that, I needed to establish confidence in the validity and appropriateness of Hitachi-GE's methods. I have achieved this by a sampling approach (targeting reactor faults), and by drawing upon the assessment conclusions of colleagues in other topic areas. This requirement is reflected in the reporting structure I have followed. In the following sub-sections, I will discuss:

- the assumed reactor source term (the types, quantities, and physical and chemical forms of the radionuclides present in a fault condition that will result in an exposure to radiation);
- the modelling of the transport, release, dispersion and uptake of the source term;
- the predicted results for reactor faults and the comparison against Numerical Target 4;
- observations on fuel route dose calculations; and
- observations on non-reactor fault dose calculations.

669. The radiological consequences for beyond design basis events are presented as appropriate in Ref. 46. Aside from what I have already discussed in Section 4.7 above, I have chosen not to look in detail at the results or sample the underlying methods

further in this section. In most cases the objective of the BDBA in Ref. 46 is to show there is no cliff-edge in terms of plant behaviour compared to related design basis events, and therefore the DBA radiological consequences predicted can be assumed to be broadly representative of any likely dose. It is appropriate to reduce some of the conservatism included in BDBA dose calculations compared to DBA calculations. However, in cases where the predicted doses are already very small (in the case of reactor faults) or dominated by evacuation times (in the case of fuel route faults), I judge there to be little benefit to be gained from further detailed examination of the modelling assumptions.

4.9.1 Reactor source term

670. Hitachi-GE has undertaken a significant amount of work during GDA to establish an appropriate reactor source term for the UK ABWR (for both normal operations and fault conditions), and this work and its output has been subject to extensive regulatory scrutiny, led by ONR reactor chemistry colleagues, as a result of regulatory issue RI-ABWR-0001 (Ref. 130).

671. A suite of documents was generated by Hitachi-GE to define and justify the source terms to be used in different circumstances, headed by a high level strategy report (Ref. 131). The strategy report introduces the concept a primary source term (PST). The PST is the level of activity at outlets of the RPV. It quantifies the concentration of each radionuclide present in the reactor water and reactor steam. Two versions of the PST have been identified :

- The best estimate PST is a representative condition that is a realistic and reasonable expectation of what could be present in the UK ABWR over a defined period. It is to be used for disposability assessments and routine discharges to ensure there is no over-specification of plant systems.
- The design basis PST is a conservative maximum value which is considered to be a bounding limit for the plant design. It is expected that this level would not be exceeded during operation, even if ‘expected events’ (see Table 1) such as fuel pin failures occur.

672. It is the design basis PST which has been used for the reactor DBA. In principle, I am content with this as an approach given Hitachi-GE has shown with thermal hydraulic and reactor physics analysis that no consequential fuel damage due to design basis faults needs to be considered.

673. Ref. 131 states that the PST has been developed from statistical analysis of operational data from existing BWRs plants, taking into account design and operational factors pertinent to the UK ABWR. Given that the operational data only includes a limited sub-set of radionuclides, the PST has been augmented with the results of computer models and supporting calculations. This derivation of the source terms has been assessed by reactor chemistry colleagues and judged to be adequate (Ref. 110). I have therefore not looked at it again, and I am making the assumption that it is appropriate for the UK ABWR.

674. Despite this interface with and reliance on the parallel reactor chemistry assessment, there are still fault studies judgements I need to make. The design basis PST forms the basis of a LCO on circuit activity to be complied with in normal operation. There are two questions to be considered when assessing the LCO:

- Is it sufficiently low to allow Numerical Target 4 to be met for the bounding reactor fault?
- Is it reasonably practicable to tighten the LCO to reduce further the consequences of design basis events?

675. I will comment on the first question in Section 4.9.3 below. On the second point, optimising the LCO will be a matter for the licensee after GDA. However, it is possible to form a view (from a fault studies perspective) if there is a strong need to drive for tighter limits. I will also comment on this Section 4.9.3. Colleagues in other topic areas have already considered Hitachi-GE's claim that the extant LCO will not be prohibitive for normal operations

4.9.2 Radiological consequences methods and assumptions

676. As with any piece of modelling that supports a safety case, radiological consequences analysis needs to meet the fundamental expectations set out in the AV series of SAPs, notably:

- theoretical models should adequately represent the facility and the site (AV.1);
- calculation methods should adequately represent the physical and chemical processes taking place (AV.2);
- the data used in the analysis should be valid and it uncertainty exists, an appropriate safety margin applied (AV.3);
- models and datasets should be developed, maintained and applied in accordance with quality management procedures (AV.4);
- documentation should be provided to review the adequacy of the analytical models and data (AV.5).

677. In addition to the expectations above, it also needs to be established that the level of conservatism included in the modelling is consistent with that assumed for the numerical targets being compared with. It is not appropriate to compare a verified and validated, well documented, best-estimate calculation with a limit defined for conservative analysis.

678. Evidence and assurance on these points has been pursued during GDA Step 4 by an ONR inspector who specialises in radiological consequences analyses, in support of this fault studies assessment. Full details of this specialist assessment are captured in Ref. 132 but of particular note are:

- As well as the activity levels present in normal operations, it is relevant good practice to consider a 'spike' release of activity in some fault conditions involving a depressurisation of the RPV. Early interactions with Hitachi-GE revealed some discrepancies in the spike activity assumed for some radioactive species however the ONR specialist was ultimately satisfied with the final assumptions made in the later revisions of Ref. 39.
- The means by which radionuclides generated in the core are transferred to a location where a person can receive a dose in a fault condition is usually through the release of steam. Hitachi-GE assumes in its analysis that only small fractions of the radionuclides, in particular iodine, are transferred. The data supporting this assumption were derived from at-power operations. The ONR specialist sought and received additional assurances that the assumed carry-over fractions remained applicable (and bounding) in circumstances where the steam flow is much lower (for example, during an SBO extended transient).
- For faults where the containment is intact and not bypassed by the fault or the accident management measures, containment leakage rates dominate the radiological consequence calculations. The assumed rates were investigated and challenged through RQs, and as a result the ONR specialist was satisfied with the rates assumed in the final versions of fault studies submissions.
- For faults where the release is via the R/B, Hitachi-GE claims that plate-out of radionuclides on surfaces is an important factor in determining the off-site consequences. The ONR specialist was satisfied that the R/B decontamination

factors assumed in the analysis are in reasonable agreement with the available test data.

- Dispersion modelling is an important factor for determining off-site releases. The Pasquill weather categories used in Hitachi-GE's analysis were investigated, challenged, and after revision, judged to be appropriately conservative for DBA.
- The initial assumptions made by Hitachi-GE to convert ground level deposition to an ingested dose in off-site calculations were challenged. During Step 4, a number of changes were made to Hitachi-GE's analysis. The ONR specialist was satisfied that the final assumptions included in the analysis presented in Ref. 39 are consistent with expectations and guidance for the UK.
- The groundshine assumptions made in the off-site calculations were assessed and judged to be appropriate in the later revisions of Ref. 39.
- Hitachi-GE has used the RADTRAD code to perform its radiological consequences calculations. It considers the source term, mitigation and dispersion to determine public and worker doses. It is a US code, primarily aimed at demonstrating compliance with US NRC's requirements for dose analysis. However, it has previously been used in support of GDA submissions for another reactor design, and assessed in that context by ONR (Ref. 133). Specifically for the UK ABWR GDA, the ONR specialist inspector reviewed some of available code documentation and performed some independent checks of the predicted releases. The code was judged to be generally adequate however a problem with how the code handles the build-up of daughter products was revealed by ONR's assessment. Hitachi-GE acknowledged this issue (Ref. 134), referred it to the third-party code maintainers, and put in place a technical work around and additional quality assurance checks to ensure the final results are acceptable. This approach was judged to be appropriate for GDA.
- The ONR specialist performed independent off-site radiological consequences calculations for four of the design basis faults considered by Hitachi-GE in Ref. 39. Reasonable agreement was found, providing additional assurance in Hitachi-GE's methods and the levels of conservatism assumed.

679. The final conclusion of the ONR assessment in Ref. 132 is that Hitachi-GE's analysis methods and assumptions are appropriate for meaningful comparisons to be made against Numerical Target 4. This finding has informed my assessment approach, and I have therefore assumed that Hitachi-GE's dose predictions for design basis faults can be used as the basis for regulatory judgements on the adequacy of the UK ABWR design and safety case.

4.9.3 Comparison of design basis reactor fault doses with Numerical Target 4

680. Attachment L of Ref. 39 presents evaluations of the on-site and off-site doses for four bounding design basis faults which involve the loss of at least one physical barrier (even with the correct operation of safety measures) and therefore could result in radiological consequences higher than those seen in normal operation:

- FDW line LOCA inside the PCV – 2.1 x 10^{-4} mSv off-site, 5.9 x 10^{-6} mSv on-site
- MS line break outside the PCV – 1.8 x 10^{-1} mSv off-site, 5.3 x 10^{-1} mSv on-site
- Reactor water cleanup line break outside of the PCV – 3.3 x 10^{-1} mSv off-site, 3.1 x 10^{-3} mSv on-site
- small line break outside of the PCV – 1.3 x 10^{-4} mSv off-site, 8.9 x 10^{-6} mSv on-site
- inadvertent MSIV closure fault – 2.2 x 10^{-4} mSv off-site, 1.9 x 10^{-4} mSv on-site.

681. Following a comparison of these results against Numerical Target 4, I have the following observations:

- If radioactivity is confined by the PCV, the predicted on-site and off-site doses for even the most onerous LOCA and non-LOCA design basis faults are well below the BSO limits. This is a significant and welcomed result that applies for the vast majority of the at-power reactor faults listed in the fault schedule. It also provides important context for ALARP judgements on whether further improvements to the UK ABWR should be sought.
- The MS line break outside the PCV results in on-site and off-site doses above the BSO limits, but significantly below the BSL limits which apply for infrequent faults. Given that a release of active steam outside of the PCV is inherent to this event, it is my view that it is unrealistic to expect the BSO to be met. Tightening the LCO would reduce the predicted results to closer to the BSO but only marginally when compared to the level of uncertainty and conservatism included within the calculation (for example, assuming a more realistic MSIV closure time will have a bigger impact on the predicted dose by reducing the mass of activated steam released). A future licensee will be required by law to demonstrate that it has done everything reasonably practicable to reduce risks, and as part of that duty I would expect it to review its LCO to see if they can be tightened further. However, for the purposes of GDA, I am content that the results predicted for this bounding fault are acceptable with the extant source term assumptions.
- The reactor water cleanup line break outside of the PCV is not a challenging LOCA for the fuel in the RPV, but as with the MS line break, the nature of the fault means that a bypass of the PCV is unavoidable. With conservative analysis, assuming a 32 second release before A1 isolation terminated the leak, doses higher than the BSO are being predicted. There remains considerable margin to the BSL limits. In the context of judging if Hitachi-GE has reduced risks to be ALARP, my main consideration is whether the reactor water cleanup system needs to be outside of the PCV. ONR reactor chemistry colleagues have assessed the system as part of their GDA Step 4 review (Ref. 110). They have advised me that the system is large and has been optimised (compared to other BWR designs) to minimise operator doses from routine activities. Therefore, moving the system within the PCV would be extremely difficult and costly, and would almost certainly result in higher operational doses. It is my judgement that the predicted off-site dose for a fault condition (<1 mSv) is not significant enough to warrant Hitachi-GE exploring any major design changes that could eliminate the vulnerability of a PCV bypass, and therefore I am content with the design and analysis results for GDA.

682. All frequent design basis reactor faults credit PCV venting as a diverse means of providing the long term FSF-3 cooling function. In addition, venting is claimed as the primary means of providing long term cooling in extended SBOs. Clearly this action provides a route for confined radioactivity to be released to the environment which needs to be considered.

683. The fault schedule identifies two means of venting for these design basis events; the hardened unfiltered route and the FCVS. Conservatively assuming the release is via the unfiltered route, Hitachi-GE has predicted the off-site consequences of venting in design basis events to be:

- medium term (24 hour) SBO – 2.9×10^{-3} mSv (Ref. 40)
- diverse long term cooling for frequent faults – 2×10^{-2} mSv (Ref. 39).

684. These results are close to, or below, the BSO for off-site doses. This is another significant conclusion for the UK ABWR safety case. It shows that if the reactor core can be scrammed and then kept sufficiently cooled so that fuel damage does not occur (the objectives demonstrated by the wider DBA), then venting is not a major radiological concern. The diverse long term cooling demonstration assumes venting is

not terminated until seven days after the initiating event. It illustrates that there is no radiological consequences 'cliff-edge' if venting is performed for an extended period of time. The analysis of the beyond design basis long term SBO in Ref. 40 which used less conservative analysis assumptions suggests that the expected consequences could be much less than is predicted by the DBA results.

685. Thermal hydraulic sensitivity cases for the medium term SBO showed that a lower mass of steam would be released if venting is delayed until 620 kPa (gauge). However the bounding radiological consequences shown above which assume venting is performed at 310 kPa (gauge) are not significant enough to suggest it is ALARP to delay venting until the COPS setpoint is reached (ie the predicted doses should not deter the operators from venting the containment to prevent the design pressure being exceeded).

686. Given that the FCVS route is also available to the operators to further mitigate the releases, venting is only performed following a CCF of a major A1 SSC, and venting can be terminated when power or active cooling is restored, I have no concerns about the claims made on venting in the design basis safety case.

687. I have already discussed in Section 4.4.4 the radiological consequences from shutdown reactor faults. As long as the fuel remains covered, consequential damage is not predicted. The remaining concern is therefore generated steam which, in operating states with an open PCV, will be released straight into the R/B, and from there to the local environment. Ref. 103 estimates for the bounding scenario (involving a simultaneous problem with the both reactor and SFP) the off-site dose to be 0.6 mSv. This is above the BSO, and is higher than any dose predicted for at-power faults and PCV venting operations. This highlights the relative significance of faults during shutdown. However, it is below the most restrictive BSL for any frequency of design basis event and has been accompanied with an extensive ALARP review. I am therefore satisfied that these radiological consequences are acceptable for GDA.

4.9.4 Fuel route dose calculations

688. The analysis that supports the fuel route safety case is dominated by radiological consequence calculations (for example, there is generally not a need for complex thermal hydraulic calculations). As a result, I have already discussed in Section 4.5 my assessment conclusions following comparisons against Numerical Target 4, assuming Hitachi-GE's dose analysis is adequate. However, a number of additional matters have been pursued during the course of the GDA Step 4 assessment to gain confidence in Hitachi-GE's analysis.

689. There are three main dose considerations in the fuel route safety case:

- Assuming sufficient makeup water is provided to keep FA in the SFP covered and therefore adequately cooled, the off-site dose from generated steam needs to be considered.
- In the case of over-raise faults or reductions in water level, the dose to workers from irradiated FAs and components with a loss of shielding needs to be considered.
- In the case of dropping FAs, or dropping heavy loads on FAs, the on-site and off-site dose from released fission products needs to be considered.

690. The specialist assessment of Hitachi-GE's radiological consequences analyses undertaken to support this fault studies assessment looked at the SFP steam calculation (Ref. 132). It observed that the radiological consequences from a boiling SFP are dominated by fission products and corrosion products from any failed fuel stored in the racks. Following a number of meetings and RQs, the ONR specialist was satisfied that final calculations reported by Hitachi-GE used an appropriate value for

the amount of fission product inventory in the clad / fuel gap that could be released into the water and out to the environment in a fault condition.

691. I have discussed the issue of evacuation times and over-raise setpoints in earlier sections for loss of shielding events. As part of the ONR specialist assessment, an independent calculation was performed to estimate the dose to a worker from FA with reduced water shielding (Ref. 132). Reasonably agreement was obtained with the worker doses reported in Ref. 45. This outcome provides me with valuable additional confidence in Hitachi-GE's methods.

692. For faults involving damage to a FA, a significant amount of noble gas and iodine can be released to the SFP. While noble gases will be readily released from the SFP, to the R/B and ultimately to the environment, the SFP water will provide some mitigation to iodine release. This mitigation, together with some claims on filtration, means that iodine only makes a small contribution to the radiological consequences predicted by Hitachi-GE when compared to noble gases. The ONR specialist judged this to be a reasonable assumption but investigated further the size of the iodine decontamination factor used in Hitachi-GE's analysis. Following some interactions and revisions to calculations, the specialist was ultimately satisfied that the final factor used in Ref. 45 is acceptable, and consistent with recommendations in Ref. 135.

4.9.5 Non-reactor fault dose calculations

693. As with fuel route faults, the analysis that supports the non-reactor SSC safety case is dominated by radiological consequences calculations, and I have already discussed the acceptability of the results against Numerical Target 4 and the design implications for required safety measures.

694. The ONR specialist radiological consequence assessment (Ref. 132) performed some independent calculations of the off-site dose from an off-gas system rupture and a liquid radioactive waste system leak. Reasonable agreement was obtained. This outcome adds to my confidence in Hitachi-GE's methods, and supports my approach of using Hitachi-GE's predicted doses as a basis for making judgements on the adequacy of the UK ABWR's design.

4.9.6 Numerical Targets 5 and 6

695. ONR's assessments of deterministic design basis safety cases are almost exclusively performed against Numerical Target 4 in the SAPs (Ref. 5). ONR specialists in the PSA topic area are interested in the probabilistic risks from initiating events and fault sequences, and, in the case of the UK ABWR GDA, they compare the off-site risks predicted by Hitachi-GE's PSA model to Numerical Targets 7, 8 and 9.

696. However, as part of my assessment strategy I was keen to gain an appreciation on whether the direct-cycle nature of the UK ABWR introduced some additional or different risks, in particular to workers, to those present on the operating UK nuclear fleet. Therefore, through RO-ABWR-037 (Ref. 52), I actioned Hitachi-GE to develop a methodology for comparing the risks to workers from accidents on the UK ABWR against the BSOs and BSLs of Numerical Targets 5 and 6. Given that exactly how operations will be performed cannot be known at this time, there was no expectation that this methodology could be comprehensively applied in GDA. But through the application of some clearly stated assumptions and scope limitations, Hitachi-GE was asked to apply its methodology in a limited way to provide some additional insights into the UK ABWR design.

697. Informed by advice from an ONR colleague who specialises in radiological consequences assessment, I am satisfied that both the methodology developed by Hitachi-GE (Ref. 136) and its application (Ref. 137) are adequate for GDA (Ref. 138).

698. The results are broadly consistent with the conclusions already reached in this assessment report. If design basis measures work effectively, there are no major risks to workers from reactor or SFP faults. The UK ABWR worker risks are therefore dominated by severe accidents or fuel handling faults, but even these are shown to be at, or below BSO levels.[38] Non-reactor faults, including those which are unique to or an inherent feature of BWRs, are all predicted to have consequences in the lowest Numerical Target 6 dose band and only make a small contribution to the summated frequency calculated for that band. Similarly, they only make a very small contribution to the overall calculated risk of worker death predicted by Hitachi-GE (which is below the Numerical Target 5 BSO).

699. I assume that when a future licensee knows how it will conduct operations and deploy workers, it will review and reapply the methods developed in GDA to assess the risks to its staff against relevant targets. However, the limited application in GDA Step 4 has been of value, validating the scope of my assessment and the review against other numerical targets. It has:

- illustrated the importance of demonstrating the effectiveness of design basis reactor safety measures, such that significant worker doses will only be received during a very unlikely severe accident;
- shown that fuel handling operations do have risks attached with them, so it is important the engineered protection that prevent faults occurring the first place are appropriately identified, classified, designed, operated and maintained; and
- not revealed any non-reactor faults with significant risks to workers that are inherent to the UK ABWR but novel to UK regulators which have been missed from ONR's assessment.

4.10 Safety case documentation

700. In the preceding sections, I have largely concentrated on the adequacy of Hitachi-GE's documentation to support specific claims about the UK ABWR design. In this section, I will comment on my overall impressions of Hitachi-GE's documentation as a collective suite of reports which establish the fault studies safety case and how they compare against the expectations from TAG NS-TAST-GD-051 (Ref. 13) listed in Section 2.1.2.

701. As a general observation against the expectations of Ref. 13 for a safety case to accurately represent the design intent, all the major submissions in the fault studies area have been generated specifically for the UK ABWR over the course of GDA. Although some methods and assumptions have origins predating GDA, all the analysis and accompanying safety case discussion has been newly produced and is directly applicable to the UK ABWR. There is minimal reliance on reports produced for other ABWRs or earlier reactor designs. This strong position has been achieved through a considerable amount of work by Hitachi-GE, which I commend.

702. Moving onto the adequacy of individual documents and portions of the safety case, I consider Ref. 38 to be an excellent report which provides a vital foundation for the fault studies safety case. It systematically and comprehensively explains the basis and origins of the faults included on the fault schedule. This is to the benefit of other parts of the UK ABWR safety case, my assessment, and importantly, future users of the safety case.

703. Ref. 38 includes the main fault schedule. It is another crucial part of the UK ABWR safety case that provides the links between the fault studies and the design

[38] *The only event predicted to have a risk to workers higher than the Numerical Target 6 BSO is a cask drop during fuel export operations with a failure of the canister. However, the frequency attributed to this event is low; beyond design basis for Numerical Target 4 and less than 1% of the Numerical Target 6 BSL frequency. Hitachi-GE has performed an extensive ALARP review during GDA for this event which has been accepted by ONR (Ref. 102).*

requirements for engineered safety systems. The scope, structure and contents are all consistent with my expectations. Of particular note, the fault schedule clearly identifies:

- the HLSF being delivered by each SSC claimed on the fault schedule;
- whether a claimed SSC is the primary design basis means of providing the HLSF, a diverse means for frequent faults, or a defence-in-depth measure which will contribute to nuclear safety but is not formally credited in the design basis;
- whether an SSC is actuated automatically (if so, by what parameter) or manually;
- the number of divisions of a SSC which are available for each specific fault in the considered operating state, and the number of divisions required to deliver a safety function.

704. The main fault schedule is also supplemented with a useful attachment which identifies the key support systems which facilitate the actuation and continued operation of the claimed A1 and A2 systems.

705. The analysis which identifies and substantiates the SSC requirements shown on the fault schedule is provided in Ref. 39. This is a long document, reporting the bulk of the transient analysis that supports the design basis safety case. It details most of the major assumptions, outlines the methods used (for example, the computer codes), and clearly states what the results of analyses are and how they compare against applicable acceptance criteria. However, it is limited and varying in the extent to which it explains how its results support the design basis safety case or substantiate the fault schedule. It also does not link the results to appropriate explanations on why risks have been reduced to be ALARP. In summary, it is a presentation of results, but it is not itself the (reactor) design basis safety case.

706. In the final revision of Ref. 39 submitted in GDA Step 4, references to individual Hitachi-GE ‘calculation sheets’ were added. This is consistent with my expectations as set out in Ref. 13 for all references and supporting information to be identified and accessible. An observation that I have made several times in this report, echoing a finding made by GRS when it was trying to independently replicate Hitachi-GE’s results, is that Ref. 39 does not provide all the information a reader may need to fully understand the methods applied and the reasons for certain parameters being used. The addition of references to the ‘calculation sheets’ came too late in Step 4 for them to be examined and therefore I do not know to what extent they can fill the gap in information and explanations that I have observed in Ref. 39.

707. Despite this observation, I am satisfied that Ref. 39 is sufficient for me to reach conclusions on the adequacy of Hitachi-GE’s DBA for GDA. A future licensee will probably require additional information and superior documentation to support future site-specific revisions of the UK ABWR safety case.

708. Hitachi-GE has identified the PCSR as the place to find the safety case structure and over-arching claims that are missing from Ref. 39. I have no objections to this but it does mean a safety case user needs to read and appreciate information across multiple PCSR chapters (aided by the fault schedule in Ref. 38) to form a picture of the design basis safety case for an individual reactor fault.

709. It is my judgement that there are many positive aspects to the PCSR, including:

- Chapter 5 (Ref. 31) provides an effective and valuable summary of the approach and principles adopted throughout the UK ABWR safety case.
- The engineering chapters 11, 12, 13 and 16 (Refs 32, 33, 34 and 35) not only provide adequate descriptions of individual SSCs but they also ensure there are traceable links between the HLSFs identified in the fault schedule and the

lower-level basis of safety case reports providing supporting evidence on each SSC. This is achieved through the use of SFCs. This approach achieves clarity on the requirements for individual SSCs, and a supporting evidence trail, that are superior in scale and ambition to anything I have seen in other top level reactor safety reports.

- Chapter 28 on ALARP (Ref. 37) provides an excellent summary of the evolutionary development of the UK ABWR (preceding and during GDA). It explains and justifies the origins of many of key design features which ensure safety, recognising that while the UK ABWR is new to the UK, BWRs have been designed and operated in other countries for decades.

710. Chapters 24 and 26 (Refs 29 and 30) were originally planned by Hitachi-GE to be summaries of the main fault studies topic reports (notably Refs. 38, 39 and 46). However, Hitachi-GE has responded to feedback given over the course of GDA Step 4 on the need for improvements by providing additional information and discussion in the chapters to help integrate the analysis in the fault studies topic reports into the broader safety case. Summaries of a subset of the analyses presented in Ref. 39 continue to be the bulk of Chapter 24 but also included in the final version are:

- objectives for the presented analysis and an overview of what will be shown in the chapter;
- clear links between the acceptance criteria demonstrated in the analysis and the SFCs made in the engineering chapters;
- clear links between the SSCs claimed in the DBA to deliver HLSFs and the supporting system descriptions in the engineering chapters of the PCSR;
- discussion and detail on what LCOs have been identified from the analysis;
- a global strategy for how ALARP is demonstrated for the design basis safety case, with conclusions provided for each group of faults saying how the reported analysis demonstrates ALARP consistent with that strategy.

711. Similar additions have been added to the beyond design basis portion of Chapter 26, although, entirely appropriately, it has fewer links back to engineering chapters. BDBA is primarily about demonstrating that there is no cliff-edge just outside of the design basis, and that the extant provision is effective in preventing fault escalation. By definition, it is the DBA that is driving design and engineering requirements for SSCs.

712. I still consider it a challenge to establish and follow the claims, arguments and evidence through the PCSR on a fault-by-fault basis. However, through the complementary information included in the final version, my understanding of the safety case developed through interactions with Hitachi-GE, and the overview provided by the fault schedule (not included in full in the PCSR), I am satisfied that the PCSR is adequate from a reactor fault studies perspective for GDA. The traceability of the claims, arguments and evidence on a SSC-by-SSC basis is excellent and consistent with the expectations of Ref. 13.

713. At the start of GDA, while there was a limited description of the fuel route, there was no formal fault studies safety case documentation for it and the associated activities. At the end of GDA Step 4, there is now a comprehensive and integrated fuel route safety case spread across many reports and technical areas, all brought together under a single topic report (Ref. 43). I judge this to be another significant achievement made by Hitachi-GE during the course of GDA. This safety case will need to be further developed in later phases of the UK ABWR project (for example, demonstrations the FHM and RBC meet all the requirements of A1 systems) but there is now a clear safety case intent and framework for undertaking that work.

714. The starting position for non-reactor SSCs associated with a significant nuclear hazard was similar. The available safety case documentation was initially centred on the risks to the fuel in the reactor, and not on the potential for radiological harm regardless of

source. The need to consider non-reactor faults is now fully integrated into the safety case, starting with the principles and objectives set out in PCSR Chapter 5 (Ref. 31). Ref. 38 identifies non-reactor initiating events for inclusion in the fault schedule, and Ref. 39 provides appropriate analysis. PCSR Chapter 24 (Ref. 29) incorporates these fault studies perspectives into the wider safety case, providing the necessary links between what the analysis shows and what the engineering can deliver. There will be further work to be done after GDA to continue to develop the safety case, but I consider what has been done (from a fault studies perspective) to be adequate for GDA.

715. A fundamental requirement for any UK safety case is the demonstration of ALARP. I am satisfied that the basic arguments for reactor DBA as set out in PCSR Chapter 24 (Ref. 29) are reasonable:

- There are often large margins between the predicted results of DBA and the corresponding parameters.
- The DBA is conservative so in a real event the margins to acceptance criteria would be much larger.
- The unclaimed lower class SSCs have been shown by the US / Japanese practice analysis to provide greater margins.

716. On that basis, Hitachi-GE argues that it is generally not ALARP to provide additional engineered provision. This is supported by the BDBA which demonstrates no cliff-edge effects for events just outside the DBA.

717. It is my judgement that Hitachi-GE's results support this conclusion.

718. As with a lot of the fault studies safety case, these ALARP arguments are decoupled from discussion on individual SSCs. Therefore, to gain a fuller picture of the ALARP case for a specific fault, the general fault studies arguments need to be read in conjunction ALARP discussions in PCSR chapters 11, 12, 13 and 16 (Refs 32, 33, 34 and 35). This makes it harder for the safety case user than it could be to appreciate the ALARP case, but I am content that adequate arguments are provided across the totality of the UK ABWR safety case documentation for GDA.

719. In response to specific challenges put to it during GDA Step 4 (see for example the fuel route safety case or Section 4.11 below), Hitachi-GE has performed systematic optioneering reviews to either substantiate the extant design or identify design changes. The final versions of these reviews provided to ONR in support of the fault studies safety case assessment have been adequate for GDA.

720. In conclusion, I am satisfied that the major submissions available at the end of GDA do adequately bring together the claims, arguments and evidence identified by Hitachi-GE to form an adequate fault studies safety case for the UK ABWR. Many of the expectations of Ref. 13 have been met, and any shortfalls or limitations that exist are not sufficient to prevent me reaching conclusions of the adequacy of the UK ABWR design.

4.11 Adequacy of specific UK ABWR engineering features

721. In general, I have excluded from the scope of this assessment report a detailed review of how individual SSCs meet the engineering standards and architecture requirements that follow from the safety classification applied to them in the fault schedule. Such a review is primarily a matter for other technical areas, for example mechanical engineering or internal hazards. However, as part of this fault studies assessment, I have asked Hitachi-GE to demonstrate the adequacy of its design in three areas for which questions arose as a result of considering DBA deterministic rules:

- the level of redundancy and diversity in the SRV design;
- the optimisation of the FLSS design;
- the resilience of the UK ABWR to biological fouling and the provision of a RUHS.

4.11.1 SRV redundancy and diversity

722. The SRVs are a crucial part of the UK ABWR design. They are claimed on the fault schedule to deliver several FSFs for most reactor design basis faults.

723. Analyses in Attachment A and Attachment E of Ref. 39 show that 15 out of the 16 SRVs are sufficient to provide overpressure protection for the limiting isolation transients and ATWS events. Few transients result in the staggered setpoints of all 16 SRVs being reached. Many transients without MSIV closure do not result in even the lowest overpressure setpoints being reached. Given that planned maintenance of a SRV inside the isolated and inerted PCV will not be possible while the reactor is at power, I am satisfied that this level of redundancy (N+1) is sufficient to meet the single failure criterion.[39]

724. As previously stated in Section 4.3.2, the applicable basis of safety case report (Ref. 68) sets out to demonstrate that the SRV design can provide 'N+2' redundancy, consistent with the general claim for a standby A1 SSC set out in Table 2 (it does go on to state that 'N+2' is not necessary because at power maintenance cannot be performed). Ref. 68 references analysis performed in support of PSA modelling to demonstrate that only 14 out of the 16 SRVs are required for overpressure protection. I have not looked at the referenced analysis, and as point of relevant good practice, I would expect conservative DBA (such as that presented in Ref. 39) to be the principal substantiation for deterministic redundancy claims (in preference to analysis intended to support the best-estimate PSA). However, I do take some further reassurance from this claim of 'N+2' provision. Ultimately, I am satisfied that the levels of redundancy provided in the SRV design are adequate and consistent with the expectations of SAPs EDR.4 and FA.6 (Ref. 5).

725. The SRV design also includes partial diversity for the various functions identified to be delivered:

- The spring-loaded A1 overpressure protection is only called upon if the C3 automatic pneumatic actuation fails.
- To depressurise the RPV for low pressures safety injection, seven of the SRVs are designated to provide the A1 ADS function. Another seven provide the A2 RDCF function, initiated through the diverse A2 HWBS C&I, powered from the A2 B/B and with dedicated accumulators. Both the ADS and RDCF SRVs can achieve the necessary conditions for low pressure safety injection.
- Only two of the 16 SRVs are required to depressurise the RPV after scram for RHR shutdown cooling and to take the plant to a stable, safe state. This can be achieved by either the ADS valves or the RDCF SRVs.

726. Despite this, all 16 SRVs are basically the same design. Hitachi-GE has stated in PCSR Chapter 5 (Ref. 31) that "for frequent [reactor] design basis faults each identified safety function is required to have a diverse means of delivery". However, there is no diverse means of providing the overpressure protection function. This function is vital to ensure a fault does not escalate either by the RPV (and associated pipework) failing or by the head of the high pressure ECCS being exceeded. Only limited credit can be taken in the design basis safety case for C3 pneumatic actuation of the same SRVs. It was therefore my opinion during GDA Step 4 that the UK ABWR was not meeting

[39] *Analysis presented in Appendix B of Ref. 113 shows that only 2 out of the 16 SRVs are needed maintain the bounding non-ATWS transient peak reactor coolant pressure beneath safety limits (a feedwater controller failure). Design basis ATWS faults are a more significant challenge because the power remains high and more SRVs are required to control the pressure rise.*

either my expectations or Hitachi-GE's own deterministic design basis rules in this regard.

727. Given this apparent shortfall, I asked Hitachi-GE to undertake a multi-disciplinary review (fault studies, PSA and mechanical engineering) of the UK ABWR design to demonstrate why it reduces risks to be ALARP. Hitachi-GE's consolidated response is provided in Ref. 113. It does the following:

- Systematically discusses all the safety functions provided by the SRVs and the associated design provision.
- Identifies the claims placed on the SRVs by the bounding frequent faults, infrequent faults, and beyond design basis faults.
- Lists the SFCs and SPCs applied to the SRVs.
- Identifies the design requirements and properties established in Hitachi-GE's internal guidance to protect against CCFs, and then reviews the SRV design against those requirements, considering all delivered safety functions.
- States that it considers that adequate protection against CCF has been provided for reactor core cooling (FSF-2) and long-term heat removal (FSF-3) but concedes there is a need to review diversity options for the overpressure protection function for frequent faults.
- Reviews European BWRs as examples of relevant good practice, identifying three cases where diverse overpressure protection has been back-fitted to operating plants. The bases for the design changes are compared against the UK ABWR design.
- Three options to provide additionally diversity in overpressure protection in the UK ABWR are considered (extra discharge routes off the MS lines controlled by motor operated valves, the inclusion of a rupture disc, or extra lines controlled by vacuum breakers). The possibility of replacing some of the spring loaded SRVs with valves of a different type (for example pilot operated valves) is also discussed.
- From a mechanical engineering perspective, the potential failure mechanisms of the extant SRV design are identified and possible improvements reviewed. The Japanese operational experience with the SRV design proposed for the UK ABWR is also reviewed.
- A PSA review of importance of SRV reliability to the core damage frequency and the potential benefits of additional diversity is presented.

728. Ref. 113 concludes that Hitachi-GE judges the extant design to be ALARP. The main basis for this is an assertion that the spring-loaded SRVs provide a high level of reliability, which is demonstrated by many years of Japanese operating experience. It argues that modifications made to European BWRs to add diversity do not represent directly applicable relevant good practice because their basic design utilised less-reliable pilot-operated SRVs or they were making changes to increase capacity as part of a power uprate. The alternative / additional design options considered were all judged to have disadvantages associated with them, while not significantly reducing the risks predicted by the PSA modelling.

729. The PSA and mechanical engineering arguments put forward have been reviewed by the relevant ONR specialists in their parallel GDA Step 4 assessment, and broadly accepted (Refs. 59 and 108). From my fault studies perspective:

- Hitachi-GE has not ignored the notional deviation from its own deterministic rules and my expectations for diversity to be provided for frequent faults.
- I judge Ref. 113 to be a comprehensive and systematic review of the issue, with a wide scope that fully meets my expectations.
- Its conclusions are a judgement on Hitachi-GE's part, but they are supported by evidence and analysis.

- I accept that spring-loaded SRVs are a simple and reliable means of providing the overpressure protection function, and operational experience supports their use over pilot valves.
- Including additional and novel design features is rarely an easy or desirable option as it can introduce new risks (both expected and unexpected).

730. Given these factors, together with assessment conclusions of specialist colleagues, I am content with Hitachi-GE's judgement that the extant design is ALARP and I see no grounds for insisting on further design changes in GDA.

731. However, while I can accept there is operational evidence to support the conclusion that the UK ABWR's spring loaded SRVs are more reliable than the potential alternatives, I do not believe the possibility of a CCF can be totally eliminated, especially one associated with maintenance and calibration errors throughout the SRV's operational life. Hitachi-GE has recognised this at the end of Ref. 113, stating that improvements through administrative measures could reduce the risk of CCFs due to human errors. It recommends that a future licensee explores this further during site-specific phases of the UK ABWR. This requirement to look at means to minimise human error is also established in ONR's mechanical engineering assessment through assessment finding AF-ABWR-ME-02 (Ref. 108). As a result, I am content that my residual concerns are adequately captured outside of this report.

4.11.2 FLSS design

732. The inclusion in the UK ABWR design of the FLSS as a permanently engineered means of providing water to the R/B is a notable post-Fukushima addition to the basic ABWR concept developed in the US and Japan. The FLSS was originally envisaged as a severe accident and beyond design basis measure, however, in the final safety case some of its functionality is claimed for design basis events. Therefore, DBA expectations on design requirements apply to aspects of it.

733. Hitachi-GE claims the FLSS as a diverse A2 SSC for providing safety injection to the reactor and makeup water to the SFP in the event of a CCF to A1 SSCs. In accordance with Table 2, Hitachi-GE's design rules specify that the FLSS needs to be 'N+1' with regard to these operations. A review of the design shows that while there is redundancy in water supply and the two trains within the B/B each have 2 x 50% pumps, there are only single lines leaving the B/B for the RPV and SFP within the R/B (see Figure 7). These single lines contain check valves and are therefore potentially vulnerable to both passive (pipe blockage or rupture) and active failures (valve failure).

734. As a result, I asked Hitachi-GE to review its design for the FLSS to see if it would be reasonably practicable to eliminate these weaknesses. I also advised Hitachi-GE not to limit the scope of this review to DBA aspects, but also to consider if other design options (for example different or multiple tie-ins to the RPV circuit) could represent reasonably practicable improvements for those beyond design basis events where the FLSS is a claimed low pressure safety injection measure.

735. In response, Hitachi-GE provided Ref. 139. It does the following:

- Describes the FLSS and the SFCs placed on it.
- Summarises the injection line design, including the piping and the check valves used.
- The design back-fitted post-Fukushima to the Japanese reference plants is briefly discussed, along with the evolution the UK ABWR FLSS design has undergone.
- Lists the design basis events which make claims on the FLSS, along with any alternative means included within the design to provide the same function (eg LPFL, FLSR, MUWC and FP).

- Summarises the contribution the FLSS piping and check valve reliability make to the core damage frequencies calculated by the PSA.
- Reviews relevant good practice and operational experience, acknowledging that there is precedent in UK safety cases for other reactor designs in treating failures of check valves as active failures to be considered within the design basis, and not as low probability passive failures that can be excluded from single failure tolerability studies.
- Summarises all the design measures included in the extant design which Hitachi-GE states supports its claim that risks have been reduced to be ALARP.
- Discusses further options that could reduce risk, notably:
  - alternative connections points for the FLSS to the RPV;
  - providing an alternative connection for the FLSR (it currently connects to the RPV via the single FLSS line); and
  - parallel check valves to ensure a single failure does not prevent injection.
- In an appendix, it details the results of a FMEA performed on the FLSS.

736. It concludes that it considers the extant design is ALARP because:

- The FLSS pipework is designed to a high standard and is therefore reliable.
- The check valves are part of the PCV boundary and are therefore designed to a high A1 standard, so their failure in combination with an event which puts a demand of the FLSS is very unlikely.
- The check valve design provides a test lever that an operator can use to both see whether the valve is open and manually force it open if necessary.
- The check valves will be tested every month during operation to reduce the risks from ‘stuck-closed’ events.
- There are alternative ways of providing injection to the RPV and makeup water to the SFP. It points out that although the B3 FLSR shares the same injection route to the RPV (and therefore is potentially vulnerable to any check valve failure that affects the FLSS), the C3 MUWC and FP use a different injection line. It also observes that there is a FLSR line to the SFP that is completely separate from the FLSS line.

737. I found Ref. 139 to be a good quality report, with a wide scope and some reasonable arguments. However, it is largely restricted in its considerations to design basis scenarios, and does not consider if design changes could be of benefit to beyond design basis events and severe accidents. Through a RQ, I asked Hitachi-GE to supplement Ref. 139 with additional information, including on the consideration of the beyond design basis events. The response (Ref140) was comprehensive and adequately addressed the shortfalls in Ref. 139.

738. When taken together, I am satisfied that through Refs 139 and 140 Hitachi-GE has adequately considered the FLSS design and demonstrated that it is ALARP. The most important arguments that convince me are:

- By simply providing the FLSS, Hitachi-GE is already improving the UK ABWR design compared with the original ABWR concept.
- Check valves and steel pipes are generally reliable components if correctly inspected and maintained through life. The inherently less reliable active components (the pumps and their power supplies) are ‘N+1’ in line with DBA expectations.
- The check valve design allows for regular testing in normal operations and visual inspections of their open status when a demand is placed on them (with the ability to force them open if necessary).
- If a reactor fault did occur which required low pressure safety injection but the LPFL, FLSS and FLSR all failed for some reason, the MUWC and FP provide

an alternative injection path that does not use the FDW lines. Although these SSCs are C3, they would only be called upon in circumstances that are a long way outside the design basis. I have no objections to these classifications for defence-in-depth measures.

739. In Ref. 140, Hitachi-GE committed to ensuring that the defence-in-depth role of the MUWC and the FP are appropriately captured in the fault schedule (Ref. 38) and the list of safety classified SSCs (Ref. 141). I have checked the final versions of these two documents issued to ONR during GDA Step 4, and I am satisfied these commitments have been delivered.

4.11.3 The resilience of the UK ABWR to biological fouling and the provision of a RUHS.

740. The major three-divisional A1 SSCs that deliver the major safety functions on the UK ABWR rely on a three-divisional active cooling chain to reject both decay heat and any heat generated through SSC operation to the ultimate heat sink. The closed loop RCW takes heat from the A1 SSCs and rejects it through heat exchangers in the heat exchanger building to the RSW. The RSW takes its water from a water intake pit, passes it through the RCW heat exchangers and then discharges it to a water discharge pit.

741. On the basis of the RCW and RSW also being three-divisional A1 systems to match the systems they support (with multiple redundancies within each division with regard to pumps, strainers, piping, etc), Hitachi-GE has assumed in Ref. 38 that mechanical failures that result in a complete loss of either the RSW or RCW should be treated as infrequent faults. The fault schedule identifies the A2 FLSS and PCV venting as the single means of providing the lost cooling function in a fault condition. This level of protection (in terms of safety classification and redundancy) is consistent with Hitachi-GE's guidance set out in Ref. 54 for an initiating event associated with a CCF of an A1 'N+2' SSC, and is something I have already accepted in principle in Section 4.2.5 of this report.

742. Hitachi-GE has entirely appropriately declared the design of the intake and discharge pits to be a site-specific activity and beyond the scope of GDA. At some point in the future, a licensee will need to review its specific design and justify its resilience against site-specific hazards. However, regardless of the site-specific design and location, it is almost certain any UK ABWR will be located on the coast and the ultimate heat sink will be the sea. There is extensive experience on UK coastal sites of power generation operations being challenged by biological fouling hazards such as jellyfish or seaweed. It is therefore my opinion that a loss of ultimate heat sink (and therefore the RSW and RCW) should be treated as frequent fault within GDA, with appropriate provision included in the generic UK ABWR design.

743. Hitachi-GE has accepted this judgement during GDA Step 4, and included water-based biological fouling as a frequent fault on the fault schedule (Ref. 38). As frequent fault, there is an expectation that there will be A1 and A2 protection, so it follows that extra measures are required in addition to the A2 FLSS and venting capability. Hitachi-GE has addressed this by proposing an A1 'N+2' reserve ultimate heat sink (RUHS).

744. The proposed RUHS is a new system for the UK ABWR, and its detailed design will be a site-specific matter (different sites may have different RUHS designs). However, for the purposes of GDA, Hitachi-HE has added a conceptual design for the RUHS to the UK ABWR reference design (Ref. 142) and written a topic report detailing its basic functional requirements and discussing options for the proposed Wylfa site (Ref. 143).

745. I am satisfied that the concept of the RUHS is included within the final UK ABWR design reference established by Ref. 144. I am also content with the general scope of

Ref. 143 and the basic requirements it identifies for the RUHS. In terms of options, Ref. 143 considers whether the RUHS should be connected to the RSW as an alternative to the sea, or should be connected directly to the RCW as an alternative for the RSW. No preference is prescribed for the generic design but requirements for both cases are set out. I judge this to be a reasonable approach for GDA.

746. In an Appendix to Ref. 143, it is stated that the preferred solution for the Wylfa site is forced draught evaporative cooling tower technology connected to the RCW system, with each ECCS division supported by its own 100% train. While recognising that the final design option will not be determined until after GDA, I am satisfied that this proposed option for Wylfa is credible and likely to be consistent with ONR's expectations.

4.12 Overseas regulatory interface

747. ONR has formal information exchange agreements with a number of international nuclear safety regulators, and collaborates through the work of the IAEA and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). This enables ONR to utilise overseas regulatory assessments of reactor technologies, where they are relevant to the UK. It also enables the sharing of regulatory assessment findings, which can expedite assessment and helps promote consistency.

748. ONR also represents the UK at the Multinational Design Evaluation Programme (MDEP). MDEP seeks to:

- enhance multilateral co-operation within existing regulatory frameworks
- encourage multinational convergence of codes, standards and safety goals
- implement the products it develops in order to facilitate the licensing of new reactors, including those being developed by Generation IV International Forum

749. Through the MDEP forum, ONR was informed of several minor modelling issues applicable to the extant DBA that supports the ABWR design certification in the US. These issues were put to Hitachi-GE in the form RQs, asking it to discuss any implications for the UK ABWR analysis.

750. In its responses to the supplied RQs, Hitachi-GE has stated that the reported issues do not impact the UK ABWR analysis (Refs 145 and 146).

751. I am satisfied with the responses provided by Hitachi-GE. The analysis that supports the US ABWR is long established. Submissions to US NRC were originally provided between 1987 and 1989, and the regulator ruled on the design in 1997. It is therefore not surprising that some small issues have been observed in the original analysis in the time that has elapsed. In contrast, Hitachi-GE's analysis for the UK ABWR has only recently been undertaken, cognisant of historic modelling issues.

4.13 Assessment findings

752. During my assessment 14 residual matters were identified for a future licensee to take forward in their site-specific safety submissions. Details of these are contained in Annex 1.

753. These matters do not undermine the generic safety submission and are primarily concerned with the provision of site specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages. These items are captured as assessment findings.

754. I have recorded residual matters as assessment findings if one or more of the following apply:

- site specific information is required to resolve this matter;
- resolving this matter depends on licensee design choices;
- the matter raised is related to operator specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters;
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

755. Assessment Findings are residual matters that must be addressed by the Licensee and the progress of this will be monitored by the regulator.

5 CONCLUSIONS

756. This report details my GDA Step 4 fault studies assessment of the UK ABWR.

757. Despite the UK ABWR being based on an established design supported with analysis, Hitachi-GE has produced a brand new suite of DBA and BDBA, in support of a UK-centric safety case developed for GDA Step 4. This has involved a tremendous amount of work by Hitachi-GE, and has resulted in a much broader and deeper safety case for fault studies than was available at the start of GDA.

758. I have reviewed this extended safety case against the applicable expectations of the SAPs and relevant international guidance. I am satisfied that:

- Hitachi-GE has adequately identified design basis and beyond design basis faults for all reactor operating modes, and has given appropriate consideration to fuel route and non-reactor facilities with significant radiological hazards.
- Hitachi-GE has produced an adequate fault schedule with contents consistent with my expectations.
- Hitachi-GE has appropriately assessed reactor faults with adequate tools and methods, with levels of conservatism consistent with DBA and BDBA approaches.
- Hitachi-GE has shown through its analysis that the successful operation of the safety measures identified in the fault schedule allows all relevant acceptance criteria to be met. Significantly, no consequential fuel damage is predicted for design basis faults, and most events do not result in a release outside of the PCV. For those events which are associated with a bypass of the containment, or are managed through a deliberate release, the predicted doses have been shown to be acceptable against numerical targets established in the SAPs.
- From a limited starting point, acceptable claims and arguments have been made for the fuel route and non-reactor SSCs, and appropriate analysis has been performed to substantiate these claims.
- Fault studies has been used to support general ALARP claims on the adequacy of the extant UK ABWR design. This has been supplemented in a number of areas by detailed optioneering studies where further design changes have been considered.

759. Limits and conditions for safe operation have been identified from the analysis, notably constraints on planned maintenance of SSCs. In general, ‘N+2’ capability has been demonstrated for major A1 safety systems, which should provide future operators with valuable flexibility. However, the SBO safety case does impose a need for the RCIC to be available throughout power operations.

760. To conclude, I am satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for fault studies. I consider that from a fault studies view point, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to future permissions and permits beings secured.

761. Several assessment findings (Annex 1) were identified; these are for future licensee to consider and take forward in their site-specific safety submissions. These matters do not undermine the generic safety submission and require licensee input/decision.

6 REFERENCES

1	Generic Design Assessment of Hitachi-GE's UK Advanced Boiling Water Reactor (UK ABWR) - Step 4 Assessment Plan for Fault Studies, ONR-GDA-AP-15-004 Revision 0, November 2015, TRIM 2015/340948
2	Step 2 Assessment of the Fault Studies of Hitachi GE's UK Advanced Boiling Water Reactor (UK ABWR), ONR-GDA-AR-14-005 Revision 0, August 2014, TRIM 2014/167870
3	GDA Step 3 Assessment of the Fault Studies of Hitachi GE's UK Advanced Boiling Water Reactor (UK ABWR), ONR-GDA-AR-15-005 Revision 0, January 2016, TRIM 2015/214507
4	ONR Guidance on Mechanics of Assessment, TRIM 2013/204124
5	Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0, ONR, November 2014, www.onr.org.uk/saps/saps2014.pdf
6	Transient Analysis for DBAs in Nuclear Reactors, NS-TAST-GD-034, Revision 3, July 2016, TRIM 2016/ 2016/232907
7	The Limits and Conditions for Nuclear Plant Safety, NS-TAST-GD-035, Revision 4, August 2014, TRIM 2016/315875
8	Safety Systems, NS-TAST-GD-003, Revision 7, December 2014, TRIM 2016/323002
9	Radiological Analysis - Fault Conditions, NS-TAST-GD-045, Revision 3, July 2016, TRIM 2016/298876
10	Validation of Computer Codes and Calculational Methods, NS-TAST-GD-042, Revision 3, July 2016, TRIM 2016/233047
11	Essential Systems, NS-TAST-GD-019, Revision 3, July 2016, TRIM 2016/295507
12	Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094, Revision 0, November 2015, TRIM 2015/364369
13	The Purpose, Scope, and Content of Safety Cases, NS-TAST-GD-051, Revision 4, July 2016, TRIM 2016/230683
14	International Atomic Energy Agency (IAEA) Standards and Guidance: ■ IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements SSR-2/1, Revision 1, February 2016 www.iaea.org
15	Western European Nuclear Regulators Association: ■ Reactor Safety Levels for Existing Reactors, September 2014 ■ WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010 ■ Safety of New NPP Designs, March 2013 www.wenra.org
16	ONR. Step 4 Assessment of Severe Accident Analysis for the UK ABWR, ONR-NR-AR-17-015 Revision 0, December 2017, TRIM 2017/98159
17	Specific Safety Guide No. SSG-2: Deterministic Safety Analysis for Nuclear Power Plants, IAEA, 2010, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1428_web.pdf
18	US NRC. Standard Review Plan for the Review of Safety Analysis Reports for

	Nuclear Power Plants: LWR Edition (NUREG-0800), https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/
19	US NRC. NRC Regulations: Title 10, Code of Federal Regulations Part 50 – Domestic Licensing of Production and Utilization Facilities, https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/
20	GRS. Provision of Technical Support to Assess the Adequacy of Transient Analysis Codes Used for UK ABWR Design Basis Analysis - GRS-ONR284 Final Summary Report D1.2, November 2016, TRIM 2016/461934
21	GRS. Input Description, Final Report, GRS-ONR285-D1.2 Revision 0, March 2017, TRIM 2017/194954 and 2017/194957
22	GRS. Partial and Total Loss of Reactor Coolant Flow, GRS-ONR285-Final Report D2.2, September 2016, TRIM 2017/55477
23	GRS. Medium Term LOOP with CCF of EDGs, GRS-ONR285-Final Report D3.2, March 2017, TRIM 2017/163460
24	GRS. Generator Load Rejection Without Bypass, GRS-ONR285-Final Report D4.2, March 2017, TRIM 2017/163485
25	GRS. LOCA Faults Analysis, GRS-ONR285-Final Report D5.2, March 2017, TRIM 2017/163516
26	GRS. Feedwater Controller Failure – Maximum Demand, GRS-ONR285-Final Report D8.2, March 2017, TRIM 2017/163530
27	GRS. ATWS Fault Analysis, GRS-ONR285-Final Report D6.3, March 2017, TRIM 2017/194949
28	Hitachi-GE. UK ABWR Generic PCSR Chapter 1: Introduction, XE-GD-0214, Revision C, August 2017, TRIM 2017/335101
29	Hitachi-GE. UK ABWR Generic PCSR Chapter 24: Design Basis Analysis, UE-GD-0208, Revision C, August 2017, TRIM 2017/335109
30	Hitachi-GE. UK ABWR Generic PCSR Chapter 26: Beyond Design Basis and Severe Accident Analysis, AE-GD-0148, Revision C, August 2017, TRIM 2017/335083
31	Hitachi-GE. Generic PCSR Chapter 5: General Design Aspects, XE-GD-0645, Revision C, August 2017, TRIM 2017/335111
32	Hitachi-GE. Generic PCSR Chapter 11: Reactor Core, UE-GD-0182, Revision C, August 2017, TRIM 2017/335090
33	Hitachi-GE. Generic PCSR Chapter 12: Reactor Coolant Systems, Reactivity Control Systems and Associated Systems, XE-GD-0646, Revision C, August 2017, TRIM 2017/335097
34	Hitachi-GE. Generic PCSR Chapter 13: Engineered Safety Features, XE-GD-0647, Revision C, August 2017, TRIM 2017/335040
35	Hitachi-GE. Generic PCSR Chapter 16: Auxiliary Systems, XE-GD-0649, Revision C, August 2017, TRIM 2017/335093
36	Hitachi-GE. Generic PCSR Chapter 19: Fuel Storage and Handling, M1D-UK-0004, Revision C, August 2017, TRIM 2017/335053
37	Hitachi-GE. Generic PCSR Chapter 28: ALARP Evaluation, SE-GD-0140, Revision C, August 2017, TRIM 2017/335068
38	Hitachi-GE. Topic Report on Fault Assessment, UE-GD-0071, Revision 6, July 2017, TRIM 2017/287331

39	Hitachi-GE. Topic Report on Design Basis Analysis UE-GD-0219, Revision 14, August 2017, TRIM 2017/321334
40	Hitachi-GE. Topic Report on SBO Analysis, AE-GD-0265, Revision 7, June 2017, TRIM 2017/234326
41	Hitachi GE. Containment Venting Strategy in UK ABWR, AE-GD-0524, Rev. 2, July 2017, TRIM 2017/263519
42	Hitachi GE. Overarching Report on Support Systems Safety Case, UE-GD-0688, Revision 1, May 2017, TRIM 2017/209291
43	Hitachi GE. Topic Report on Safety Case of Fuel Route, AE-GD-0861, Revision 1, June 2017, TRIM 2017/256320
44	Hitachi-GE. Topic Report on Fault Assessment for SFP and Fuel Route AE-GD-0229, Revision 3, July 2017, TRIM 2017/265344
45	Hitachi-GE. Topic Report on Design Basis Analysis for SFP and Fuel Route AE-GD-0441, Revision 3, June 2017, TRIM 2017/219771
46	Hitachi-GE. Topic Report on Beyond Design Basis Analysis, AE-GD-0473, Revision 5, August 2017, TRIM 2017/299917
47	Spurious C&I Failures as Design Basis Initiating Events, RO-ABWR-0007, June 2014, TRIM 2014/285928
48	Common Cause Failure of Electrical Distribution Systems, RO-ABWR-0008, June 2014, TRIM 2014/285977
49	Analysis of Loss of Offsite Power Events, RO-ABWR-0009, June 2014, TRIM 2014/285932
50	Design Basis Analysis of Essential Services and Support Systems, RO-ABWR-0010, June 2014, TRIM 2014/285933
51	Safety Case for Spent Fuel Pool and Fuel Route, RO-ABWR-0011, June 2014, TRIM 2014/285934
52	Safety Case for Faults not Directly Related to the Reactor, RO-ABWR-0037, January 2015, TRIM 2015/203872
53	Hitachi-GE. Nuclear Safety and Environmental Design Principles (NSEDPs), XD-GD-0046, Revision 1, July 2017, TRIM 2017/269935
54	Hitachi-GE. GDA Safety Case Development Manual, XD-GD-0036, Revision 3, June 2017, TRIM 2017/249277
55	Hitachi-GE. Topic Report on PSA Summary, AE-GD-0804, Revision 2, TRIM 2017/276539
56	Hitachi-GE. Generic Technical Specifications, SE-GD-0378, Revision 3, August 2017, TRIM 2017/337634
57	Hitachi-GE. Fault Studies to Discuss Deterministic Analysis, PSA and Fault Schedule Development, XE-GD-0105, Revision C, March 2014, TRIM 2014/134332
58	GRS. Review of the BWR Event List regarding Design Basis Accidents, Final Report, ONR197-333071-FR, January 2015, TRIM 2015/62730
59	ONR. Step 4 Assessment of PSA for the UK ABWR, ONR-NR-AR-17-014 Revision 0, December 2017, TRIM 2017/98147
60	ONR. Step 4 Assessment of Management of Radioactive Wastes for the UK ABWR, ONR-NR-AR-17-025 Revision 0, December 2017, TRIM 2017/98298

61	Hitachi-GE. Topic Report on Mechanical SSCs Architecture, SE-GD-0425, Revision 1, July 2017, TRIM 2017/273964
62	Hitachi-GE. Topic Report on Exceptions to Segregation, BKE-GD-0021, Revision 3, May 2017, TRIM 2017/173369
63	ONR. Step 4 Assessment of Internal Hazards for the UK ABWR, ONR-NR-AR-17-033 Revision 0, December 2017, TRIM 2017/98141
64	ONR. Step 4 Assessment of External Hazards for the UK ABWR, ONR-NR-AR-17-027 Revision 0, December 2017, TRIM 2017/98329
65	Hitachi-GE. Decay Heat for UK ABWR Analyses (Response to RQ-ABWR-0265), UE-GD-0301, Revision 1, December 2014, TRIM 2014/450232
66	Hitachi-GE. Uncertainty of Decay Heat for ATWS and Spent Fuel Pool Analyses, AE-GD-0498, Revision 0, July 2015, TRIM 2015/286970
67	US NRC. NRC Regulations: Title 10, Code of Federal Regulations Part 50 – Domestic Licensing of Production and Utilization Facilities, Appendix K to Part 50 https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appk.html
68	Hitachi-GE. Basis of Safety Cases on Reactor Coolant Pressure Boundary Overpressure Protection System, SE-GD-0167, Revision 2, July 2017, TRIM 2017/256870
69	Hitachi-GE. Basis of Safety Cases on Control Rod Drive System, SE-GD-0038 Revision 3, June 2017, TRIM 2017/256300
70	Hitachi-GE. Consideration of a Stuck Rod or Two Stuck Rods from the same HCU in ODYN Transient Analysis, UE-GD-0728 Revision 0, August 2017, TRIM 2017/308937
71	ONR. Step 4 Assessment of Fuel and Core Design for the UK ABWR, ONR-NR-AR-17-019 Revision 0, December 2017, TRIM 2016/492101
72	ONR. Step 4 Assessment of Structural Integrity for the UK ABWR, ONR-NR-AR-17-037 Revision 0, December 2017, TRIM 2017/98277
73	Hitachi-GE. Basis of Safety Cases on Reactor Recirculation System, SE-GD-0037, Revision 3, June 2017, TRIM 2017/255260
74	Hitachi-GE. Response to Queries on Topic Report on DBA – Attachment A – Plant Transient (Response to RQ-ABWR-1058, 3E-GD-D160, Revision 0, October 2016, TRIM 2016/412918
75	Hitachi-GE. Gap Conductance Model and Limiting Steam Line Length for Design Basis Accidents (Response to RQ-ABWR-1443), UE-GD-0725, Revision 0, August 2017, TRIM 2017/321386
76	GRS. Develop Reactor Physics Model Input Deck for ABWR, Final Report, GRS-ONR192-D1.2, October 2015, TRIM 2016/32072
77	Hitachi-GE. Analysis of Rod Withdrawal Error at Power and All Rod Insertion, UE-GD-0501, Revision 1, May 2017, TRIM 2017/206512
78	Hitachi-GE. Study on All Rod Insertion Fault, UE-GD-0660, Revision 1, May 2017, TRIM 2017/214426
79	ONR. Step 4 Assessment of Control & Instrumentation for the UK ABWR, ONR-NR-AR-17-017 Revision 0, December 2017, TRIM 2017/98182
80	Hitachi-GE. Queries Concerning Control Rod Faults at Start-up (Response to RQ-ABWR-1297), UE-GD-0684, Revision 0, March 2017, TRIM 2017/135683

81	Email Correspondence between ONR and Hitachi-GE, RQ-ABWR-1469 Rod Withdrawal at Zero Power, June 2017, TRIM 2017/246547
82	Hitachi-GE. Additional Queries Concerning Control Rod Withdrawal Errors (Response to RQ-ABWR-1418), UE-GD-0708, Revision 0, May 2017, TRIM 2017/205530
83	Hitachi-GE. Generic PCSR Chapter 7: Internal Hazards, SE-GD-0127, Revision C, August 2017, TRIM 2017/335032
84	Hitachi-GE. Generic PCSR Chapter 8: Structural Integrity, RE-GD-2043, Revision C, August 2017, TRIM 2017/335034
85	Hitachi-GE. Initiating Event Analysis for Internal Event at Power Level 1 PSA, AE-GD-0184, Revision 6, March 2017, TRIM 2017/86536
86	Hitachi-GE. Basis of Safety Cases on Emergency Core Cooling System, SE-GD-0164, Revision 2, June 2017, TRIM 2017/256969
87	Hitachi-GE. Supporting LOCA References (Response to RQ-ABWR-0266), AE-GD-0234, Revision 0, November 2014, TRIM 2014/413338
88	Hitachi-GE. Containment Performance Analysis Report in UK ABWR, AE-GD-0561, Revision 3, June 2017, TRIM 2017/256271
89	Hitachi-GE. Basis of Safety Cases on Containment Heat Removal Systems, SE-GD-0165, Revision 2, June 2017, TRIM 2017/257302
90	Hitachi-GE. Basis of Safety Cases on Residual Heat Removal System, SE-GD-0042, Revision 3, June 2017, TRIM 2017/256765
91	Comprehensive list in GDA for requirements and assumptions to be transferred to operating regime, XD-GD-0049, Revision 1, September 2017, TRIM 2017/368146
92	Hitachi-GE. Assumptions Relevant for Upper Drywell Head Temperature Calculations for DBF and SAA (Response to RQ-ABWR-1113), AE-GD-0852, Revision 0, November 2016, TRIM 2016/442696
93	Hitachi-GE. Anticipated Transient Without Scram System Design Description, 3D-GD-D006, Revision 2, October 2016, TRIM 2016/421312
94	Hitachi-GE. Basis of Safety Cases on Standby Liquid Control System, SE-GD-0195, Revision 2, June 2017, TRIM 2017/253800
95	Hitachi-GE. Performance of SLC Boron Injection, UE-GD-0497, Revision 0, February 2016, TRIM 2016/91606
96	Hitachi-GE. GDA Initial Core Analysis Report, UE-GD-0159, Revision 2, November 2016, TRIM 2016/463581
97	Hitachi-GE. GDA Equilibrium Core Analysis Report, UE-GD-0158, Revision 2, November 2016, TRIM 2016/463564
98	UK ABWR GDA Fault Studies & Severe Accident L4 Technical Workshop 14-18 March 2016, ONR-GDA-CR-15-472, March 2016, TRIM 2016/135989
99	Hitachi-GE. Information on the Standby Liquid Control System (Response to RQ-ABWR-0820), UE-GD-0530, Revision 0, April 2016, TRIM 2016/171788
100	Hitachi-GE. Further Queries Concerning ATWS Faults (Response to RQ-ABWR-1167), UE-GD-0658, Revision 2, April 2017, TRIM 2017/173491
101	Hitachi-GE. ONR285 Independent Confirmatory Analysis – Request for Observations or Comments on Factual Accuracy (Input Description and ATWS) (Response to RQ-ABWR-1466), UE-GD-0722, Revision 0, July 2017, TRIM 2017/283622

102	Hitachi-GE. ALARP Assessment Report for Fuel Route, AE-GD-0472 Revision 1, June 2017, TRIM 2017/251628
103	Hitachi-GE. Topic Report on ALARP Assessment for Steam Generation Resulting from a Loss of Decay Heat Removal from the SFP and Open RPV, AE-GD-0989, Revision 0, May 2017, TRIM 2017/206561
104	Hitachi-GE. Demonstration of Practical Elimination of Early or Large Fission Product Release for UK ABWR, AE-GD-0992, Revision 0, June 2017, TRIM 2017/254924
105	Hitachi-GE. Loss of Spent Fuel Pool Water from Pipe Breaks (Response to RQ-ABWR-0729), UE-GD-0499, Revision 0, February 2016, TRIM 2016/89251
106	Hitachi-GE. FPC Diffuser Pipe Design (Response to RQ-ABWR-0971), SE-GD-0431, Revision 0, September 2016, TRIM 2016/373528
107	Hitachi-GE. Summary of Fuel Route Safety Case Claims for Rapid Evacuations (Response to RQ-ABWR-1426), UE-GD-0711, Revision 0, June 2017, TRIM 2017/225010
108	ONR. Step 4 Assessment of Mechanical Engineering for the UK ABWR, ONR-NR-AR-17-022 Revision 0, December 2017, TRIM 2017/98264
109	Hitachi-GE. Presentation of Evidence of Dose Assessment of Fuel Assembly Adjacent to RPV Wall and or Base Leading to Subsequent Exposure of Workers in Upper and Lower Drywell (Response to RQ-ABWR-1394), UE-GD-0702, Revision 0, May 2017, TRIM 2017/209282
110	ONR. Step 4 Assessment of Reactor Chemistry for the UK ABWR, ONR-NR-AR-17-020 Revision 0, December 2017, TRIM 2017/98232
111	Hitachi-GE. Topic Report on ALARP Assessment for Off-Gas System, GE-GD-0035, Revision 4, July 2017, TRIM 2017/287430
112	Robust Demonstration that the Design of the UK ABWR Off-Gas System Reduces Risks SFAIRP, RO-ABWR-0073, August 2016, TRIM 2016/376974
113	Hitachi-GE. Topic Report on Safety Relief Valve Diversity, SE-GD-0601, Revision 0, April 2017, TRIM 2017/173427
114	Hitachi-GE. Multiple Piping Break Evaluation of Reactor and Containment for Structural Integrity Classification, AE-GD-1010 Revision 0, June 2017, TRIM 2017/254775
115	ONR. Assessment Note: ABWR TRACG Core Modelling, May 2016, TRIM 2016/78361
116	Hitachi-GE. Description of ODYN / STEMP Code, 3E-GD-D054, Revision 0, August 2014, TRIM 2014/318574
117	Hitachi-GE. Description of LAMB Code, AE-GD-0182, Revision 0, August 2014, TRIM 2014/318796
118	Hitachi-GE. Description of SAFER Code, AE-GD-0183, Revision 0, August 2014, TRIM 2014/318581
119	Hitachi-GE. References of the Report about LAMB and SAFER Codes Descriptions (Response to RQ-ABWR-0856), AE-GD-0715, Revision 0, May 2016, TRIM 2016/218907
120	Hitachi GE. Event Sequence Analysis for Internal Event at Power Level 1 PSA, AE-GD-0187, Rev. 8, April 2017, TRIM 2017/135699
121	Hitachi-GE. References of SHEX Code Validation and/or Verification (Response to RQ-ABWR-0916), ASE-GD-0045, Revision 0, June 2016, TRIM 2016/245383

122	ONR. ONR-NR-CR-16-689, UK ABWR GDA Fault Studies and Severe Accidents Level 4 Workshop, 24-28 October 2016, November 2016, TRIM 2016/438983
123	Hitachi-GE. Description of TRACG Code, UE-GD-0218, Revision 0, August 2014, TRIM 2014/318554, 2014/318616, 2014/318638
124	Hitachi-GE. Provision of Shutdown Fault Analysis Documentation (Response to RQ-ABWR-0973), UE-GD-0592, Revision 0, August 2016, TRIM 2016/338264
125	ONR. Shutdown Analysis Tool Assessment Note, September 2016, TRIM 2016/380389
126	Hitachi GE. Severe Accident Safety Case for Shutdown Reactor and SFP, AE-GD-0633, Rev. 1, June 2016, TRIM 2016/263197
127	ONR. ONR-GDA-CR-14-183, UK ABWR Fault Studies Step 3 Level 4 Technical Workshop held in Hitachi City, Japan 6-10 October 2014, October 2014, TRIM 2014/3861390
128	ONR. ONR-NR-CR-17-56, UK ABWR Fault Studies/Severe Accident Workshop 10-13 April 2017, May 2017, TRIM 2017/173008
129	ONR. License Condition Handbook, February 2017, http://www.onr.org.uk
130	ONR-NR-AR-16-074, Assessment of the Responses to RI-ABWR-0001, December 2016, TRIM 2016/381996
131	Hitachi-GE. Source Term Strategy Report, HE-GD-0107, Revision 2, March 2017, TRIM 2017/128072
132	ONR. Radiological Consequence Assessment Excluding Offsite Level 3 PSA, August 2017, TRIM 2017/308854
133	AMEC, Lot 5 Support to HSE – AP1000 DBA Radiological Consequences Assessments, January 2011, TRIM 2011/57129
134	Hitachi-GE. Radiological Consequences QA (Response to RQ-ABWR-0713), HE-GD-0191, Revision 0, May 2016, TRIM 2016/198591
135	US NRC Draft Regulatory Guide, Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Reactor Sites, DG-1199 October 2009, https://www.nrc.gov/docs/ML0909/ML090960464.pdf
136	Hitachi-GE. Methodology Report on Target 5 & 6 – Approach and General Principles for the Assessment, HE-GD-0151, Revision 0, January 2017, TRIM 2016/26803
137	Hitachi-GE. Topic Report on UK ABWR Worker Risk Assessment (Target 5 and Target 6), HE-GD-0295, Revision 1, July 2017, TRIM 2017/274035
138	ONR. File Note to Support Closure of RO-ABWR-37, July 2017, TRIM 2017/260390
139	Hitachi-GE. FLSS Design Review and ALARP Report, SE-GD-0595, Revision 0, April 2017, TRIM 2017/173527
140	Hitachi-GE. Response to Queries on FLSS ALARP Report (Response to RQ-ABWR-1432), SE-GD-0636, Revision 0, June 2017, TRIM 2017/235553
141	Hitachi-GE. List of Category and Class for UK ABWR, AE-GD-0224, Revision 4, August 2017, TRIM 2017/336173
142	Hitachi-GE and Horizon Nuclear Power. Inclusion of Reserve Ultimate Heat Sink within GDA – Change to GDA Design Reference, HGNE-REG-0119R, April 2016, TRIM 2016/168108

143	Hitachi-GE. Topic Report on RUHS, AE-GD-0812, Revision 0, October 2016, TRIM 2016/411249
144	Hitachi-GE. Design Reference for UK ABWR, XE-GD-0178, Revision 8, September 2017, TRIM 2017/367071
145	Hitachi-GE. Response to RQ-ABWR-0267, Error reported in GE-Hitachi LOCA analysis, November 2014, TRIM 2014/439464
146	Hitachi-GE. ABWR Design Certification Renewal Application (Response to RQ-ABWR-1482), August 2017, TRIM 2017/300095
147	Hitachi-GE. Response to RQ-ABWR-1046, Claims on the Fuel Pool Liner Drain Leakage Detection System, SE-GD-0516, October 2016, TRIM 2016/411282

7 TABLES

Table 1: UK ABWR Fault and Event Categories

Fault / Event Category		Fault Frequency (/y)	Potential Consequences	
			Off-site	On-site
Design Basis Faults	Frequent DB Faults	FF ≥ 10^{-3}	> 1 mSv (BSL)	> 20 mSv (BSL)
	Infrequent DB Faults	10^{-3} ≤ FF < 10^{-4}	> 10 mSv (BSL)	> 200 mSv (BSL)
		10^{-4} ≤ FF ≤ 10^{-5}	> 100 mSv (BSL)	> 500 mSv (BSL)
Beyond Design Basis Faults		10^{-5} ≤ FF < 10^{-7}	> 100 mSv	> 500 mSv (BSL)
Foreseeable Events		FF > 10^{-3}	0.01 mSv (BSO) to 1 mSv (BSL)	0.1 mSv (BSO) to 20 mSv (BSL)
Expected Events		FF > 10^{-2}	< 0.01 mSv (BSO)	< 0.1 mSv (BSO)

Hitachi-GE has defined Severe accidents are those fault sequences that could lead either to consequences exceeding the highest off-site radiological doses given in the BSL of NSEDP Target 4, or to an unintended relocation of a substantial quantity of radioactive material within the facility which places a significant demand on remaining physical barriers.

Table 2: Typical UK ABWR Redundancy Levels

Standby Systems		Continuously Operating Systems	
Safety Class	Redundancy	Safety Class	Redundancy
A1	N+2	A1	N+1
A2/B2	N+1	A2/B2	N+1/N
B3/C3	N	B3/C3	N

Table 3 – List of UK ABWR design basis (at power) reactor faults

Design Basis Fault	Fault Frequency	Type of Fault	Location of any sample assessment in this report
Non-LOCA reactor transients			
Non-isolation events			
Generator load rejection with bypass	FF	Transient	
Feedwater controller failure – Maximum demand	FF	Transient	Section 4.3.4.3
Reactor pressure regulator failure in the closed direction	FF	Transient	
Inadvertent control valve closure	FF	Transient	
Partial loss of reactor coolant flow (Trip of three Reactor Internal Pumps)	FF	Transient	Section 4.3.4.1
Loss of reactor coolant flow (Trip of all reactor internal pumps)	FF	Transient	Section 4.3.4.2
Recirculation flow control failure (Runout of all reactor internal pumps)	FF	Transient	
Loss of feedwater heating	FF	Transient	
Inadvertent High Pressure Core Flooder (HPCF) pump start	FF	Transient	
Isolation events			
Generator load rejection with failure of all Bypass valves	FF	Transient	Section 4.3.4.4
Inadvertent Main Steam Isolation Valve (MSIV) closure	FF	Transient	
Reactor pressure regulator failure in the open direction	FF	Transient	
Loss of main condenser vacuum	FF	Transient	
RPV water level decreasing events			
Loss of all feedwater flow	FF	Transient	
Loss of off-site power (LOOP)			
Short term LOOP (2 hours duration)	FF	Transient	Section 4.3.8
Medium term LOOP (24 hours duration)	FF	Transient	Section 4.3.8
Long term LOOP (168 hours duration)	IF	Transient	Section 4.3.8
Inadvertent opening of SRV			
Inadvertent opening of a SRV	FF	SRV open	
Control Rod Faults			
Control rod withdrawal error at reactor start-up	FF	Reactivity insertion	Section 4.3.5.1
Control rod withdrawal error at power	FF/IF	Reactivity insertion	Section 4.3.5.2
Control rod drop	IF	Reactivity insertion	Section 4.3.5.3

Design Basis Fault	Fault Frequency	Type of Fault	Location of any sample assessment in this report
LOCA events (including main steam line breaks)			
LOCA –RPV bottom drain line break–	IF	LOCA	Section 4.3.7.1
Small line break LOCA	FF	LOCA	
LOCA –HPCF line break–	IF	LOCA	Section 4.3.7.1
LOCA –Low Pressure Flooder (LPFL) line break–	IF	LOCA	Section 4.3.7.1
LOCA –Feedwater line break–	IF	LOCA	Section 4.3.7.1
LOCA –Main steam line break–	IF	LOCA	Section 4.3.7.1
LOCA –Residual Heat Removal (RHR) Outlet line break–	IF	LOCA	Section 4.3.7.1
LOCA outside primary containment –Main steam line break–	IF	LOCA	Section 4.3.7.2
LOCA outside primary containment –Reactor Water Clean-up line break–	IF	LOCA	
LOCA outside primary containment –Feedwater line (Reactor Core Isolation Cooling system (RCIC) connected) break–	IF	LOCA	Section 4.3.7.2
Small line break LOCA outside primary containment	FF	LOCA	
CCF initiated events (including ATWS)			
Generator load rejection with failure of all Bypass valves with Failure to Scram	IF	Transient	Section 4.3.10.4
Feedwater Controller Failure at Maximum demand with Failure to Scram	IF	Transient	Section 4.3.10.4
Recirculation Flow Controller Failure at Maximum Demand with Failure to Scram	IF	Transient	Section 4.3.10.4
Main Steam Isolation Valve Closure with Failure to Scram	IF	Transient	Section 4.3.10.4
Pressure Regulator Failure Open – Maximum Steam Demand with Failure to Scram	IF	Transient	Section 4.3.10.4
Loss of Condenser Vacuum with Failure to Scram	IF	Transient	Section 4.3.10.4
Short term Loss of Off-site Power with Failure to Scram	IF	Transient	
Pressure Regulator Failure Open – Maximum Steam Demand with Failure to Scram	IF	Transient	
ATWS instability (Not identified separately in the Fault Schedule)	IF	Transient	Section 4.3.11
Short term LOOP with CCF of Emergency Diesel Generators (EDGs)	IF	Transient	Section 4.3.10.4
Medium term LOOP with CCF of EDGs	IF	Transient	
All Control Rods, electrical drive units, insertion	FF	Transient	Section 4.3.5.4
Inadvertent opening of all Automatic Depressurisation System (ADS) (Other Safety System Logic and Control systems (SSLCs) are	IF	LOCA	

Design Basis Fault	Fault Frequency	Type of Fault	Location of any sample assessment in this report
available)			
Inadvertent start-up all injection system	IF	Transient	
Inadvertent opening of all ADS due to spurious failure of Class 1 SSLC	IF	LOCA	
Inadvertent MSIV closure due to spurious failure of Class 1 SSLC	IF	Transient	
Inadvertent start-up A1 (RHR,HPCF) injection system in shutdown modes	IF	Transient	
Inadvertent start-up A2 (FLSS) injection system in shutdown modes	FF	Transient	
Metal-Clad switchgear (M/C) power supply failure on electrical CCF	IF	Transient	
D/C power supply failure on electrical CCF	IF	Transient	
Loss of all Reactor Building Cooling Water (RCW)	IF	Transient	
Loss of all Reactor Building Service Water (RSW)	IF	Transient	
Loss of all Class 1 Heating Ventilation and Air Conditioning (HVAC)	IF	Transient	

Table 4 – Summary of Hitachi-GE's LOCA PCV Performance Analysis

Design Parameter	Design Value	Calculated Value
Drywell pressure (kPa gauge)	310	295
Drywell temperature (°C)	171	280 *
Wetwell pressure (kPa gauge)	310	202
Wetwell temperature (°C) • Gas Space • Suppression Pool	 104 104	 101 100

* Stated to be an airspace temperature with only lasts circa 1 second. The drywell structures will remain below the temperature limit.

The information is taken from PCSR Chapter 24 (Ref. 29) and presents the bounding value calculated for each parameter from the short and long term analysis of the two in-containment LOCAs (suppression pool temperature is only calculated by the long-term analysis).

Table 5 – Overview of Hitachi-GE's analysis tools for DBA and BDBA

Analysis Item	Analysis Tools
DBA	
Transients	ODYN ISCOR TASC
CR faults	PANACEA TRACG
LOCA	SAFER LAMB TASC
Containment performance	SHEX M3CPT
SBO	SAFER SHEX
Safe shutdown	SHEX
Diverse cooling	SAFER SHEX
Shutdown faults	Spreadsheet SHEX
SFP	Spreadsheet
ATWS	ODYN ISCOR TASC STEMP TRACG
Fuel route sub-criticality	SCALE 6
Fuel route enthalpy	TRACG
BDBA	
Majority of faults	SAFER MAAP
Medium LOCA with failure of scram	TRACG SHEX
Beyond design basis shutdown faults	Spreadsheet SHEX

Note, Radiological consequences codes are excluded from this list.

Table 6 – List of UK ABWR beyond design basis faults

No.	Fault
At power reactor faults	
1	Long-term LOOP with failure of scram
2	Medium Break LOCA with failure of scram
3	Non-LOOP frequent transient with failure of scram and ARI
4	Medium-term LOOP with failure of scram and ARI
5	Long-term LOOP with CCF of EDGs
6	Medium Break LOCA with CCF of EDGs
7	Small Break LOCA with CCF of EDGs and failure of RCIC
8	Medium-term LOOP with CCF of EDGs and failure of RCIC
9	Non-LOOP frequent transient with CCF of RHR and failure of containment venting
10	Short-term LOOP with CCF of RHR and failure of containment venting
11	Rupture of one outboard MSIV with failure of one inboard MSIV
12	Rupture of one outboard check valve with failure of one inboard check valve at FDW line
Shutdown reactor faults	
13	Loss of operating RHR with Loss of all ECCS and Failure of FLSS (Operating state C-1, C-2, C-3-1 and C-5)
14	Loss of operating RHR with Loss of all ECCS and Failure of FLSS and FLSR (Operating state C-3-2 and C-4)
15	Short term LOOP with CCF of EDGs and BBGs (Operating state C-1 and C-2)
16	Medium term Loss of Off-site Power (LOOP) with CCF of EDGs and BBGs (Operating state C-3 and C-4)
17	Long term LOOP with CCF of EDGs (Operating state C-1 to C-5)
18	LOCA at FDW line inside PCV with Loss of all ECCS (Operating state C-3 and C-4)
19	LOCA (mechanical) below TAF (Operating state C-1, C-2 and C-5)
20	LOCA (mechanical) below TAF with Loss of all ECCS (Operating state C-3 and C-4)
21	Inadvertent start-up of A2 injection systems with Loss of all ECCS and Failure of FLSS and FLSR (Operating state C-3-1)
SFP and fuel route faults	
22	Loss of all FPC pumps with failure of FLSS
23	Long term SBO
24	Small leak of SFP with failure of FPC and FLSS
25	Over-raise of irradiated fuel by FHM main hoist with failure of Class 1 limit switch and Class 2 limit switches
26	Drop of cask with loaded canister with water into the SFP

8 FIGURES

Figure 1 – UK ABWR primary and secondary containment

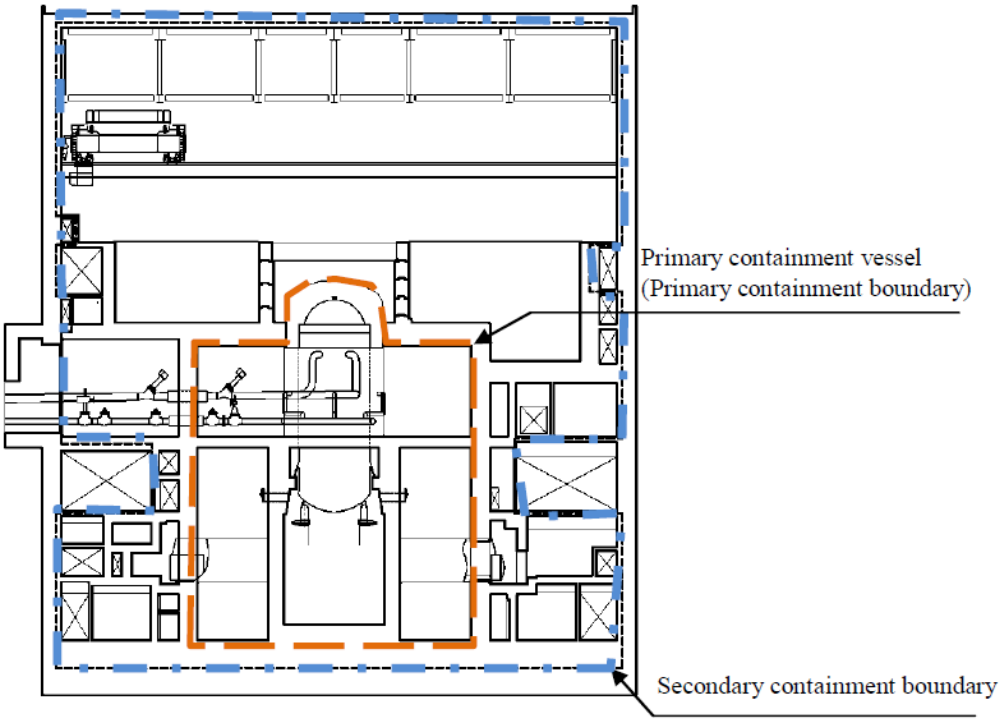


Figure 2 – Outline of the MS System in the R/B

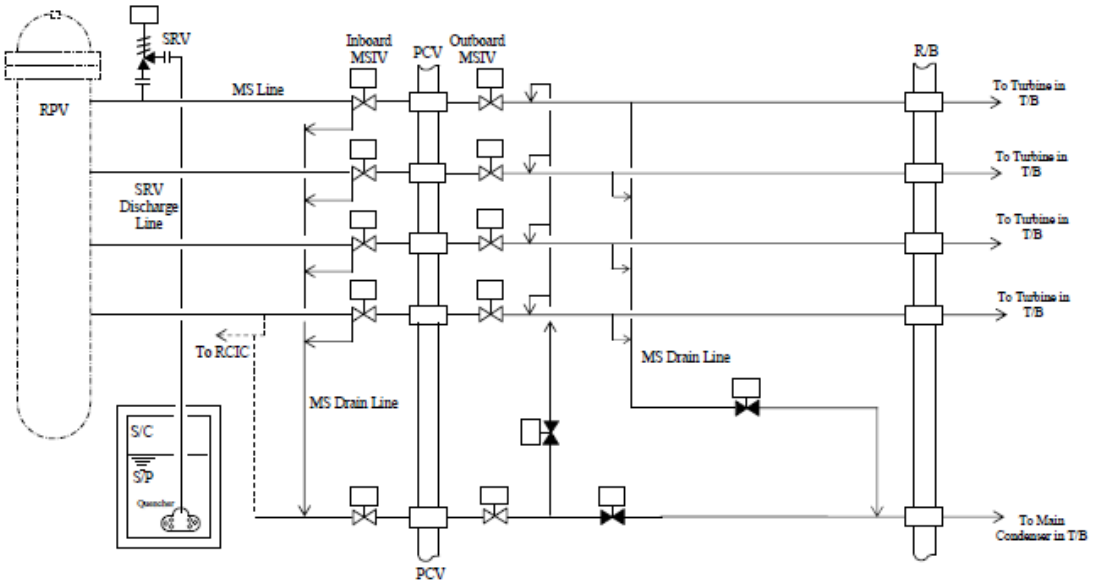


Figure 3 – Outline of the FDW system

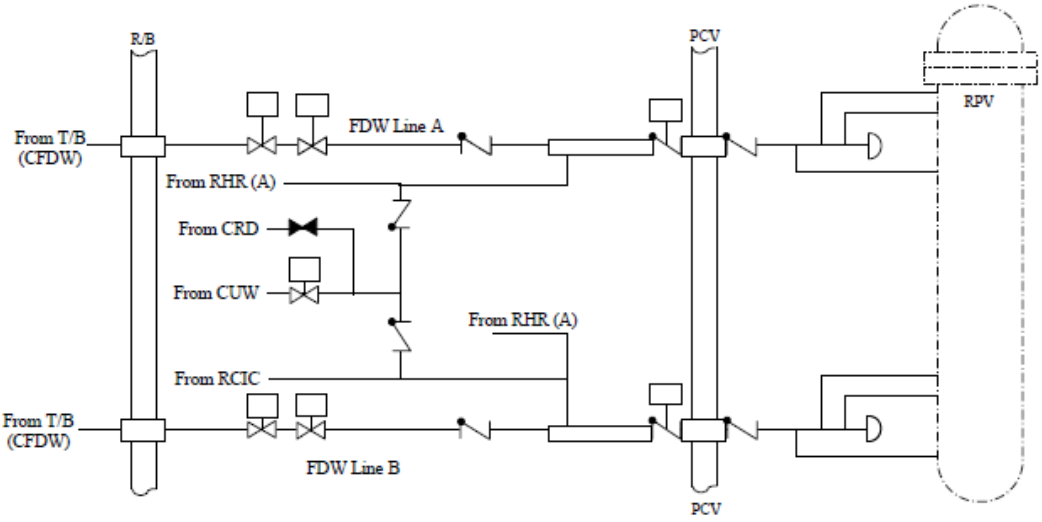


Figure 4 – UK ABWR PCV

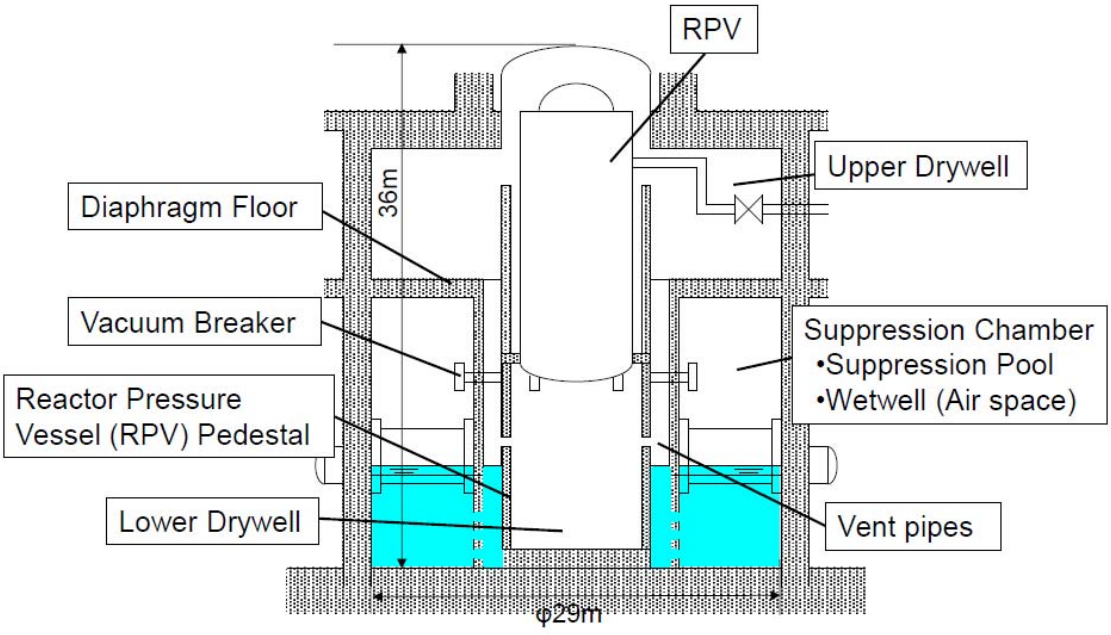


Figure 5 – ECCS and FLSS reactor injection lines

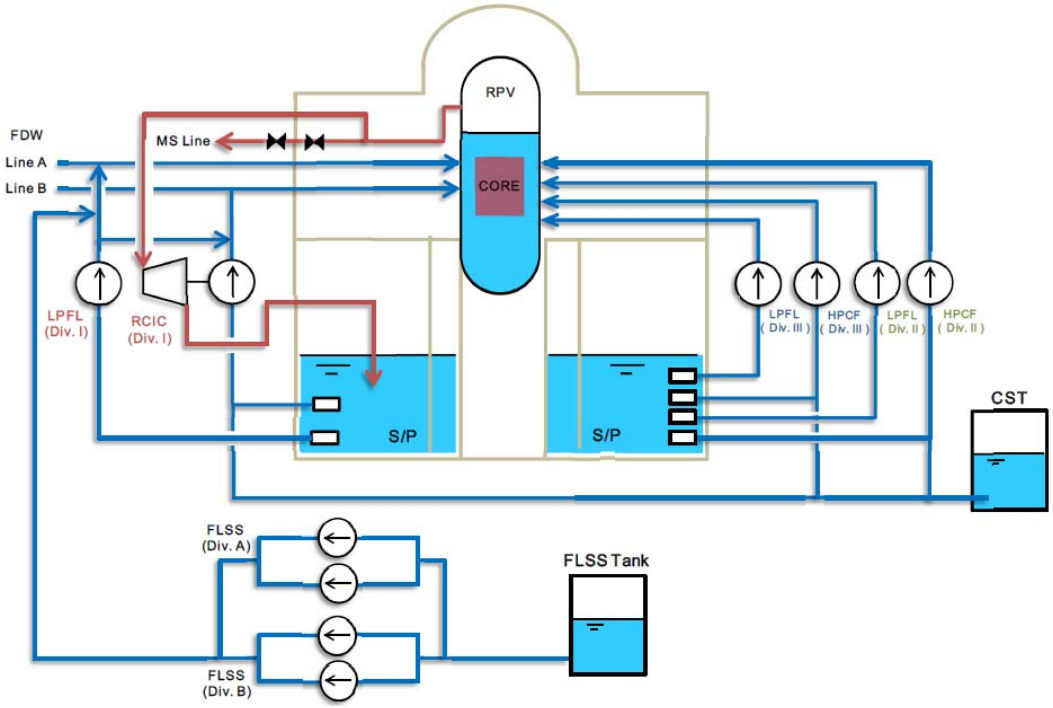


Figure 6 – SRV locations

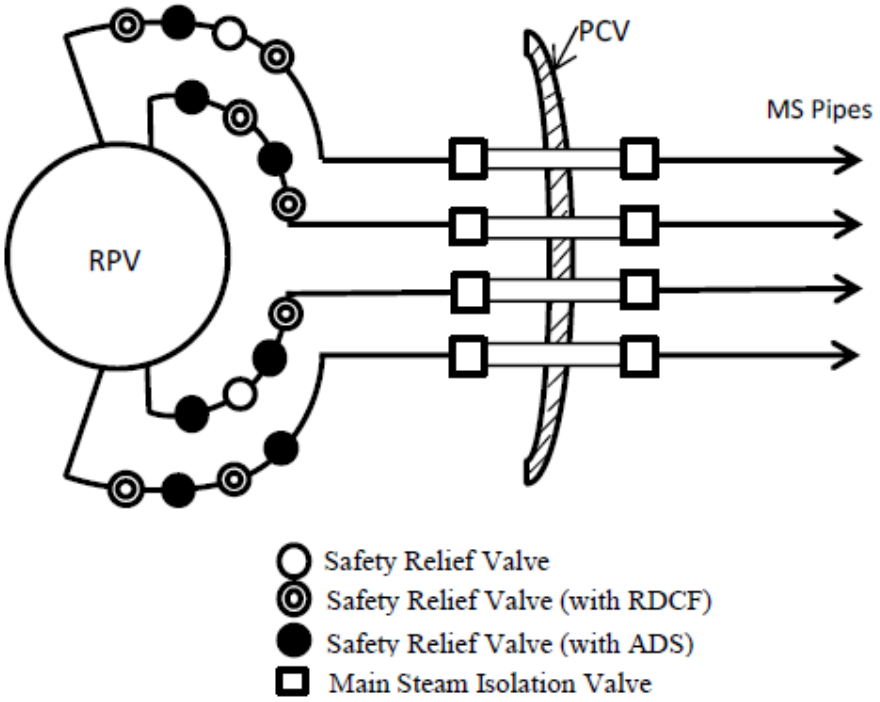


Figure 7 – Outline of FLSS

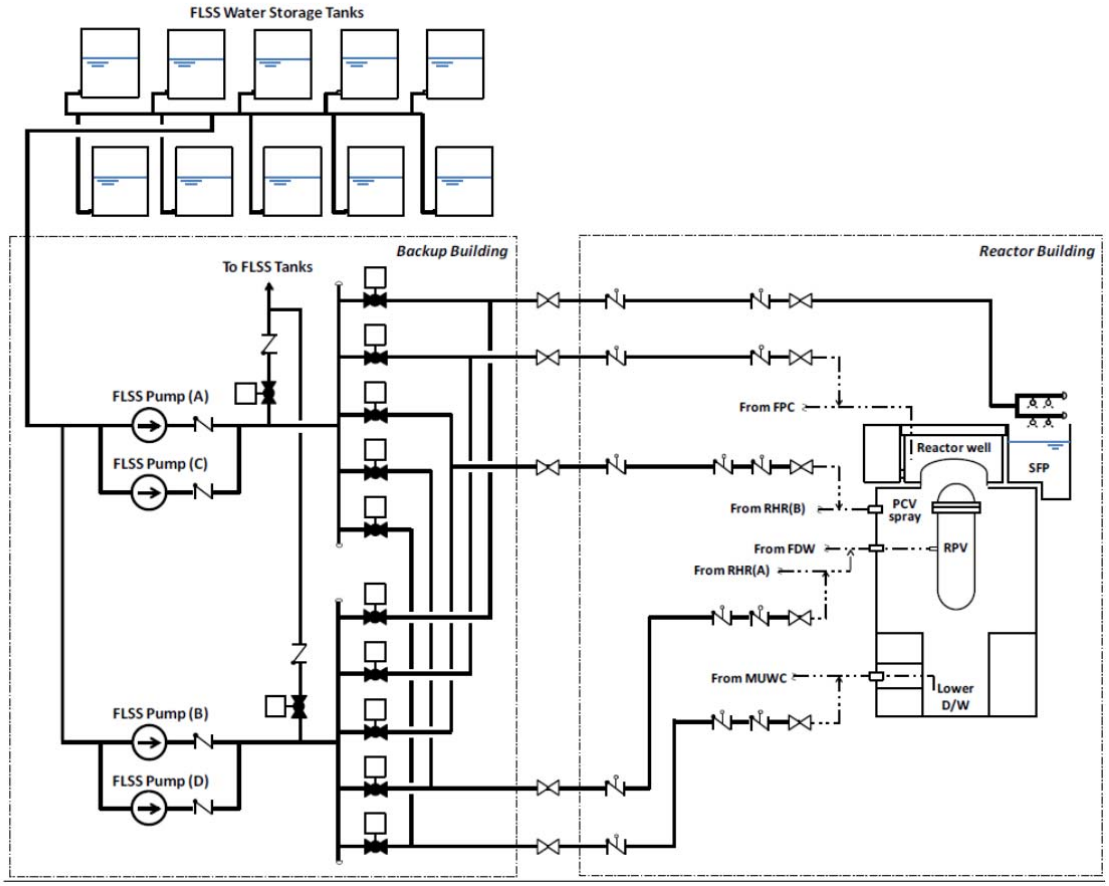
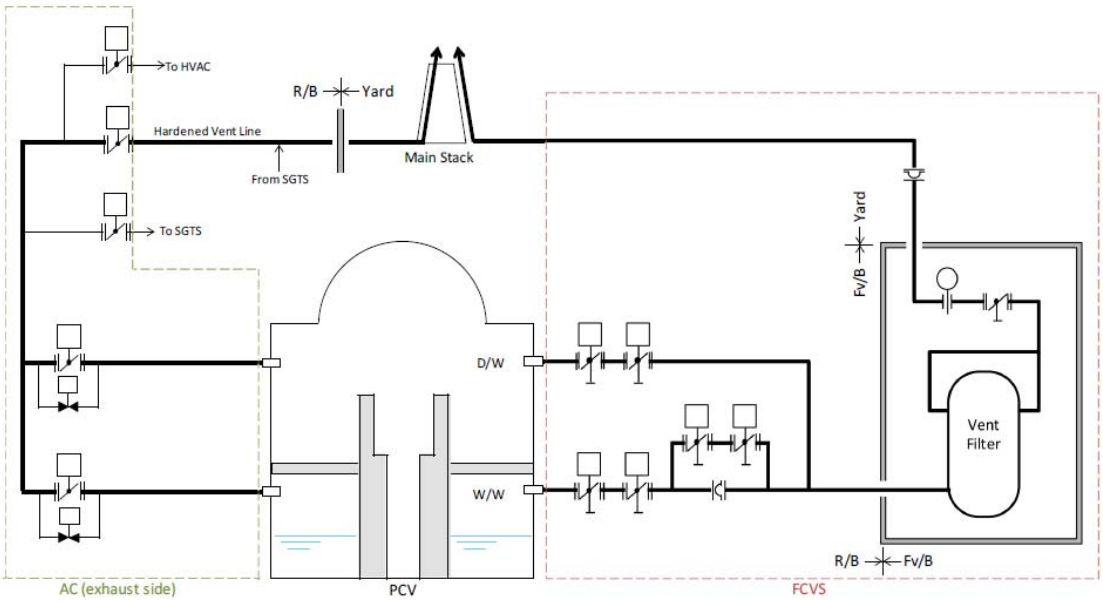


Figure 8 – Outline of the unflitered hardened venting route and the FCVS



Annex 1

Assessment Findings

Assessment Finding Number	Assessment Finding	Report Section Reference
AF-ABWR-FS-01	To allow constraints on the availability of structures, systems and components (SSCs) established by the safety case to be respected in operation (especially in the various shutdown sub-states), the licensee shall review its terminology and definitions of different operating modes to ensure that there is appropriate consistency between the fault schedule, probabilistic safety analysis (PSA) and the technical specifications.	4.2.2, 4.4.8
AF-ABWR-FS-02	To address the limitations in the prioritised GDA scope adopted by Hitachi-GE, the licensee shall provide a proportionate consideration of the impact of internal and external hazards on non-reactor facilities and activities (with potential to result in a significant dose being received by a person) in future design basis safety case submissions.	4.2.4
AF-ABWR-FS-03	The licensee shall confirm the GDA event categories applied to design basis events with substantiated initiating event frequencies when detailed design and probabilistic safety analysis (PSA) information becomes available, and update the safety case and fault schedule appropriately.	4.2.4
AF-ABWR-FS-04	The level of design provision established in GDA for faults associated with A1 essential supports systems is based on an argument that the likelihood of a common cause failure (CCF) is very low. The licensee shall demonstrate that it has done everything reasonably practicable in terms of design, operation and maintenance to minimise the vulnerability of the A1 essential support systems to CCFs (in addition to the assurances provided in GDA on the amount of the redundancy and segregation etc delivered by the systems' architecture).	4.2.4
AF-ABWR-FS-05	ONR's GDA fault studies assessment has established that some of Hitachi-GE's reactor transient analyses are potentially sensitive to the assumed length of the main steam (MS) lines. The licensee shall ensure that any decisions on the length of the MS lines made for the final site specific design take appropriate cognisance of the impact on reactor fault studies, as part of wider evaluations to ensure design choices reduce risks to be ALARP.	4.3.4.4
AF-ABWR-FS-06	To address limitations in the level of detail and justifications provided in GDA submissions, the licensee shall review and update the UK ABWR safety case to demonstrate that control rod (CR) withdrawal faults during startup, caused by malfunctions in the Class 3 rod control and information system (RCIS) and involving a greater number of CRs than is permitted by the standard withdrawal sequence controls, have adequate protection.	4.3.5.1
AF-ABWR-FS-07	As a result of changes made during GDA to meet UK relevant good practice, Hitachi-GE's 'traditional' analysis methodology was not able to demonstrate simple compliance with long-established primary containment vessel (PCV)	4.3.7.3, 4.3.8, 4.7.1, 4.8.2.4

	design limits, without calling on additional calculations and discussion. The licensee shall review the design basis acceptance criteria defined for dry well (D/W) and wet well (W/W) temperatures in the GDA safety case and ensure there is no ambiguity on what needs to be demonstrated in any future safety case analysis to provide the necessary assurances that PCV integrity will be maintained in fault conditions.	
AF-ABWR-FS-08	In the absence of detailed design information during GDA, it was necessary for Hitachi-GE to make assumptions about achievable flow rates in its demonstrations of the effectiveness of primary containment vessel (PCV) venting in design basis fault conditions. The licensee shall demonstrate that the final designs of the unfiltered hardened vent system and filtered containment vent system are effective in reducing PCV pressure and temperature in extended station blackout (SBO) events (and other frequent reactor faults where venting is claimed as a diverse measure).	4.3.8
AF-ABWR-FS-09	Hitachi-GE's arguments and analyses for anticipated transients without scram (ATWS) faults are distributed across multiple documents, severely limiting their ability to support safety case claims and inform future safe operations of the UK ABWR. The licensee shall review the available evidence for ATWS faults and consolidate it in future versions of the UK ABWR safety case, such that it is able to demonstrate it fully understands the design requirements for the ATWS systems, it can identify appropriate testing requirements for the standby liquid control system (SLCS), and can implement operator procedures which reduce risks to ALARP.	4.3.10.6
AF-ABWR-FS-10	The UK ABWR secondary containment is provided with a blowout panel to protect the civil structure from high pressure steam releases. However, over the course of GDA the number of claims on this panel has expanded from the original design intent. The licensee shall review and optimise the opening setpoint of the secondary containment blowout panel, cognisant of the safety requirements for high pressure piping ruptures, spent fuel pool (SFP) and reactor design basis loss of active cooling events resulting in steam generation, and the management of radioactivity and hydrogen in severe accidents.	4.4.4
AF-ABWR-FS-11	Hitachi-GE has shown in GDA the importance of closing primary containment vessel (PCV) hatches and airlocks following a loss of coolant accident (LOCA) in certain shutdown operating states. However, a full demonstration that the necessary actions can be completed with an adequate time margin cannot be made until the UK ABWR design and outage strategies are further developed. The licensee shall review its detailed design, outage plans and procedures to ensure that everything reasonably practicable has been done to ensure that hatches and airlocks in the PCV can be closed in a shutdown fault condition in accordance with the reactor safety case requirements, without the safety of workers being compromised to an unacceptable level.	4.4.6, 4.7.2
AF-ABWR-FS-12	As a result of ONR's GDA Step 4 assessment establishing that the Class 3 rod control and information system (RCIS) is active during refuelling operations, the licensee shall review its design and safety case to ensure that the risks from an uncontrolled criticality caused by an erroneous control rod(s) withdrawal event are reduced so far is reasonably practicable. It is assumed this will require a greater appreciation of the detailed design of fuel route control systems and likely refuelling strategies than is available in GDA.	4.4.7

AF-ABWR-FS-13	Hitachi-GE has made acceptable use of spreadsheets and hand calculations to support its safety case for shutdown faults and the spent fuel pool (SFP). However, these are not supported by the same level of validation evidence as the computer codes extensively used for at-power fault analysis, and the accompanying verification records are in Japanese. As a result, the licensee shall review its design basis tools (DBA) tools and methods for shutdown faults and faults in the SFP to ensure it has confidence in the available verification and validation evidence, while also demonstrably understanding and owning the predicted results.	4.11.4
AF-ABWR-FS-14	Given that the control of many of the computer models which support the UK ABWR safety case is ensured by the knowledge and processes of a third party (GE-Hitachi), the licensee shall put in place version controls and change management processes to ensure that there are clear links between the latest generations of the fault studies analyses (and the computer models which generated them), and the changing UK ABWR design reference it is controlling through its normal arrangements.	4.11.5