Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Fault Studies for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-014
Revision 0
January 2022

Published 01/22

EXECUTIVE SUMMARY

This report presents the findings of my assessment of the Fault Studies aspects of the UK HPR1000 reactor design undertaken as part of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA). My assessment was carried out using the Pre-Construction Safety Report (PCSR) and supporting documentation submitted by the Requesting Party (RP).

The objective of my assessment was to make a judgement, from a Fault Studies perspective, on whether the generic UK HPR1000 design could be built and operated in Great Britain, in a way that is acceptably safe and secure (subject to site specific assessment and licensing), as an input into ONR's overall decision on whether to grant a Design Acceptance Confirmation (DAC).

The scope of my assessment was to review the safety aspects of the generic UK HPR1000 design by examining the claims, arguments and supporting evidence in the safety case. My GDA Step 4 assessment built upon the work undertaken in GDA Steps 2 and 3, and enabled a judgement to be made on the adequacy of the Fault Studies information contained within the PCSR and supporting documentation.

My assessment focussed on the following aspects of the generic UK HPR1000 safety case:

- The general aspects of the RP's Fault Studies safety case which provide the framework for identifying design basis faults and performing the deterministic safety assessment.
- The adequacy of a sample of the RP's analysis of design basis conditions and design extension conditions.
- The adequacy of a sample of the deterministic analysis conducted as part of the safety case for the fuel route.
- The adequacy of the deterministic analysis conducted as part of the safety case for faults not associated with fuel, termed non-reactor faults by the RP. The RP has claimed that there are no non-reactor faults which meet the definition of a design basis fault and my assessment has been limited to gaining confidence in this claim.
- The RP's UK-specific method for the calculation of off-site radiological consequences and a comparison of the representative design basis fault consequences against ONR's Target 4.
- How the various analyses are used as part of a complete and coherent safety case in the fault studies area.
- How assumptions, requirements and limits and conditions of safe operation are identified from the fault studies safety case.
- The use of the design basis analysis to support the demonstration that the residual risks associated with the UK HPR1000 are As Low As Reasonably Practicable.

The conclusions from my assessment are:

- The RP has adequately identified design basis faults and design extension conditions for all reactor operating modes for a range of potential initiating events, including those arising from support systems or as a result of spurious control or instrumentation actuations. The RP has also given appropriate consideration to fuel route and non-reactor facilities with significant radiological hazards.

- The RP has produced an adequate fault schedule which summarises its safety case and has contents consistent with my expectations.
- The RP has appropriately assessed faults with adequate tools and methods, with appropriate levels of conservatism.
- The RP 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. While a departure from nucleate boiling is predicted for two limiting reactor faults, the predicted doses have been shown to be acceptable against numerical targets established in the SAPs.
- The RP has demonstrated that the design is capable of protecting against a loss of spent fuel pool cooling and that the consequences of potential leaks from the spent fuel pool will be limited or that they can be isolated and water level maintained.
- The RP has demonstrated that the availability requirements of the design basis analysis can be satisfied by the scheduling of maintenance activities.
- The analysis of non-reactor faults is sufficient for GDA and there are no faults arising within the waste route which qualify for treatment as design basis faults, however further development of the safety case will be required as the detailed design progresses.
- Where faults lead to a loss of one or more containment barriers the predicted radiological doses have been shown through conservative analysis to be acceptable against numerical targets established in ONR SAPs.
- Fault studies has been used to support general ALARP claims on the adequacy of the generic UK HPR1000 design. This has been supplemented in a number of areas by detailed optioneering studies where further design changes have been considered and implemented by the RP.

These conclusions are based upon the following factors:

- A detailed and in-depth technical assessment, on a sampling basis, of the full scope of safety submissions at all levels of the hierarchy of the generic UK HPR1000 safety case documentation.
- Independent information, reviews and analysis of key aspects of the generic safety case undertaken by Technical Support Contractors (TSCs).
- Detailed technical interactions on many occasions with the RP, alongside the assessment of the responses to the substantial number of Regulatory Queries (RQs) and Regulatory Observations (ROs) raised during the GDA.
- A comparison of the predicted off-site consequences of design basis events against the radiological targets set by Target 4 of the SAPs.

A number of matters remain, which I judge are appropriate for a licensee to consider and take forward in its site-specific safety submissions. These matters do not undermine the generic UK HPR1000 design and safety submissions but are primarily concerned with the provision of site-specific safety case evidence which will become available as the project progresses through the detailed design, construction and commissioning stages. These matters have been captured in 17 Assessment Findings.

Overall, based on my assessment undertaken in accordance with ONR's procedures, the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK HPR1000 design. I recommend that from a Fault Studies perspective a DAC may be granted.

LIST OF ABBREVIATIONS

ACT	Average Coolant Temperature
ALARP	As Low As Reasonably Practicable
ASDS	Atmospheric Steam Dump System (VDA [ASDS])
ARN	(Argentina's) Autoridad Regulatoria Nuclear
ATWS	Anticipated Transient Without Scram
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
C&I	Control and Instrumentation
CAE	Claims-Arguments-Evidence
CCF	Common Cause Failure
CCWS	Component Cooling Water System (RRI [CCWS])
CGN	China General Nuclear Power Corporation Ltd
CHF	Critical Heat Flux
CHRS	Containment Heat Removal System (EHR [CHRS])
CIG	Containment Isolation function Group
CSBVS	Containment Sweeping and Blowdown Ventilation System (EBA [CSBVS])
CSTS	Coolant Storage and Treatment System (TEP [CSTS])
CVS	Condenser Vacuum System (CVI [CVS])
CWS	Circulating Water System (CRF [CWS])
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System (KDS [DAS])
DBA	Design Basis Analysis
DBC	Design Basis Condition
DEC	Design Extension Condition
DG	Diesel Generator
DMGL	Delivery Management Group Lead
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DRP	Design Ref. Point
EBS	Emergency Boration System (RBS [EBS])
ECS	Extra Cooling System (ECS [ECS])
EDG	Emergency Diesel Generator
EFWS	Emergency Feedwater System (ASG [EFWS])
EMIT	Examination. Maintenance, Inspection and Testing
EPDS	Emergency Power Distribution System (LHA/B/C [EPDS])
ESWS	Essential Service Water System (SEC [ESWS])

FA	Fuel Assembly
FHSS	Fuel Handling and Storage System (PMC [FHSS])
FLB	Feedline Break
FLIV	Full Load Isolation Valve
FP	Full Power
FPCTS	Fuel Pool Cooling and Treatment System (PTR [FPCTS])
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd.
GWTS	Gaseous Waste Treatment System (TEG [GWTS])
The RP	General Nuclear System Ltd.
HBSC	Human Based Safety Claims
HF	Human Factors
HIC	High Integrity Component
HOW2	(ONR) Business Management System
HPR1000WG	HPR1000 Design Specific Working Group (within MDEP)
HTC	Heat Transfer Coefficient
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IE	Initiating Event
IEF	Initiating Event Frequency
IRWST	In-Containment Reactor Water Storage Tank
ISF	Interim Storage Facility
IVR	In-vessel Retention
KDS [DAS]	Diverse Actuation System
LCD	Low pressure full Cooldown
LLCV	Low Load Control Valve
LLIV	Low Load Isolation Valve
LOFW	Loss of Feedwater
LOOP	Loss of Off-Site Power
LUHS	Loss of Ultimate Heat Sink
MCD	Medium pressure Cooldown
MCR	Main Control Room
MDEP	Multinational Design Evaluation Programme (within OECD-NEA)
MDSL	Master Document Submission List
MFFCS	Main Feedwater Flow Control System (ARE [MFFCS])
MFPS	Motor-driven Feedwater Pumps System (APA [MFPS])
MHSI	Medium Head Safety Injection
MSIV	Main Steam Isolation Valve

MSS	Main Steam System (VVP [MSS])
MSSV	Main Steam Safety Valve
MTC	Moderator Temperature Coefficient
MW	Megawatts
NEA	Nuclear Energy Agency (within OECD)
NIS	Nuclear Instrumentation System (RPN [NIS])
NNR	(South Africa's) National Nuclear Regulator
NNSA	(China's) National Nuclear Safety Administration
NPP	Nuclear Power Plant
NSL	Nuclear Site Licence
NSS	Nuclear Sampling system (REN [NSS])
NT	Numerical Target
OECD	Organisation for Economic Cooperation and Development
ONR	Office for Nuclear Regulation
OpEx	Operational Experience
PCSR	Pre-construction Safety Report
PCT	Peak Cladding Temperature
PIE	Postulated Initiating Event
POS	Plant Operating State
PRMS	Plant Radiation Monitoring system (FRT [PRMS])
PRV	Pressuriser Relief Valves
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report (includes security and environment)
PWR	Pressurised Water Reactor
RBWMS	Reactor Boron and Water Makeup System (REA [RBWMS])
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System (RCP [RCS])
RGP	Relevant Good Practice
RHWG	Rector Harmonization Working Group (of WENRA)
RI	Regulatory Issue
RMI	Reflective Metal Insulation
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RPS	Reactor Protection System [PS]
RPV	Reactor Pressure Vessel
RQ	Regulatory Query

SAA	Severe Accident Analysis
SAP(s)	ONR's Safety Assessment Principle(s)
SBO	Station Blackout
SBOPDS	Station Black Out Power Distribution System (LJA/LJU [SBOPDS])
SCWS	Safety Chilled Water System (DEL [SCWS])
SDM	System Design Manual
SFIS	Spent Fuel Interim Storage
SFP	Spent Fuel Pool
SG	Steam Generator
SGBS	Steam Generator Blowdown System (APG [SGBS])
SLB	Steam Line Break
SIS	Safety Injection System (RIS [SIS])
SoDA	(Environment Agency's) Statement of Design Acceptability
SPHRS	Secondary Passive Heat Removal System (ASP [SPHRS])
SSFS	Shutdown Feedwater system (AAD [SSFS])
SQEP	Suitably Qualified and Experienced Personnel
SSC	Structures, Systems and Components
SyAP(s)	Security Assessment Principle(s)
TAG	Technical Assessment Guide(s)
TBS	Turbine Bypass System (GCT [TBS])
TESG	Technical Expert Subgroup
TSC	Technical Support Contractor
WENRA	Western European Nuclear Regulators' Association
VDS	(Nuclear Island) Vent and Drain System (RPE (VDS])
V&V	Verification and Validation

TABLE OF CONTENTS

Tables

Annexes

Appendix

1 INTRODUCTION

1.1 Background

1. This report presents my assessment conducted as part of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA) for the generic UK HPR1000 design within the topic of Fault Studies.

2. The UK HPR1000 is a pressurised water reactor (PWR) design proposed for deployment in the UK. General Nuclear System Ltd (the RP) is a UK-registered company that was established to implement the GDA on the UK HPR1000 design on behalf of three joint requesting parties (RP), i.e. China General Nuclear Power Corporation (CGN), EDF SA and General Nuclear International Ltd (GNI).

3. GDA is a process undertaken jointly by the ONR and the Environment Agency. Information on the GDA process is provided in a series of documents published on the joint regulators' website (www.onr.org.uk/new-reactors/index.htm). The outcome from the GDA process sought by the RP is a Design Acceptance Confirmation (DAC) from ONR and a Statement of Design Acceptability (SoDA) from the Environment Agency.

4. The GDA for the generic UK HPR1000 design followed a step-wise approach in a claims-argument-evidence hierarchy which commenced in 2017. Major technical interactions started in Step 2 which focussed on an examination of the main claims made by the RP for the UK HPR1000. In Step 3, the arguments which underpin those claims were examined. The Step 2 reports for individual technical areas, and the summary reports for Steps 1, 2 and 3 are published on the joint regulators' website. The objective of Step 4 was to complete an in-depth assessment of the evidence presented by the RP to support and form the basis of the safety and security cases.

5. The full range of items that form part of ONR's assessment is provided in ONR's GDA Guidance to Requesting Parties (Ref. 1). These include:

   - Consideration of issues identified during the earlier Step 2 and 3 assessments.
   - Judging the design against the Safety Assessment Principles (SAPs) (Ref. 2) and whether the proposed design ensures risks are As Low As Reasonably Practicable (ALARP).
   - Reviewing details of the RP's design controls and quality control arrangements to secure compliance with the design intent.
   - Establishing whether the system performance, safety classification, and reliability requirements are substantiated by a more detailed engineering design.
   - Assessing arrangements for ensuring and assuring that safety claims and assumptions will be realised in the final as-built design.
   - Resolution of identified nuclear safety and security issues, or identifying paths for resolution.

6. The purpose of this report is therefore to summarise my assessment in the Fault Studies topic which provides an input to the ONR decision on whether to grant a DAC, or otherwise. This assessment was focused on the submissions made by the RP throughout GDA, including those provided in response to the Regulatory Queries (RQs), and Regulatory Observations (ROs) I raised. ROs issued to the RP are published on the GDA's joint regulators' website, together with the corresponding resolution plans.

1.2 Scope of this Report

7. This report presents the findings of my assessment of the Fault Studies of the generic UK HPR1000 design undertaken as part of GDA. I carried out my assessment using the Pre-construction Safety Report (PCSR) (Ref. 3) and supporting documentation submitted by the RP. My assessment was focussed on considering whether the generic safety case provides an adequate justification for the generic UK HPR1000 design, in line with the objectives for GDA.

1.3 Methodology

8. The methodology for my assessment follows ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (Ref. 4).

9. My assessment was undertaken in accordance with the requirements of ONR's How2 Business Management System (BMS). ONR's SAPs (Ref. 2), together with supporting Technical Assessment Guides (TAG) (Ref. 4), were used as the basis for my assessment. Further details are provided in Section 2. The outputs from my assessment are consistent with ONR's guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

10. The strategy for my assessment of the Fault Studies aspects of the generic UK HPR1000 design and safety case is set out in this section. This identifies the scope of the assessment and the standards and criteria that have been applied.

2.1 Assessment Scope

11. A detailed description of my approach to this assessment can be found in assessment plan ONR-GDA-UKHPR1000-AP-19-015 Rev 0 (Ref. 5).

12. I considered all of the main submissions within the remit of my assessment scope, to various degrees of breadth and depth. I chose to concentrate my assessment on those aspects that I judged to have the greatest safety significance, or where the hazards appeared least well controlled. My assessment was also influenced by the claims made by the RP, my previous experience of similar systems for reactors and other nuclear facilities, and any identified gaps in the original submissions made by the RP. A particular focus of my assessment has been the RQs and ROs I raised as a result of my on-going assessment (Refs. 6 and 7), and the resolution thereof.

13. Within this report I present my assessment of the RP's fault studies safety case, which encompasses the deterministic analysis of faults for the reactor plant (during power operation, shutdown and other intermediate states), the fuel route (including the receipt of new fuel, refuelling and the storage and export of spent fuel) and the radioactive waste facilities. The majority of the fault studies safety case comprises of the Design Basis Analysis (DBA) which is a demonstration of the fault tolerance of the facility and the effectiveness of its safety measures.

2.2 Sampling Strategy

14. In line with ONR's guidance (Ref. 4), I chose a sample of the RP's submissions to undertake my assessment. The main themes considered were:

- The general aspects of the RP's fault studies safety case which provide the framework for identifying faults, defining the limits of DBA and performing the deterministic safety assessment.
- The adequacy of a sample of the RP's analysis of qualifying faults.
- The adequacy of a sample of the deterministic analysis conducted as part of the safety case for the fuel route.
- The adequacy of the deterministic analysis conducted as part of the safety case for faults not associated with fuel, termed non-reactor faults by the RP. The RP has claimed that there are no non-reactor faults which meet the definition of a design basis fault and my assessment has been limited to gaining confidence in this claim.
- The UK specific method for the calculation of off-site radiological consequences and a comparison of the representative design basis fault consequences against ONR's Target 4.
- How the various analyses are used to support a complete and coherent safety case.
- How assumptions, requirements and limits and conditions of safe operation are identified from the fault studies safety case.
- The use of the relevant deterministic analysis to support the demonstration that the residual risks associated with the UK HPR1000 are ALARP.

15. 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, design code compliance, redundancy,

single failure tolerance etc) is a matter for engineering topic areas and is beyond the scope of this report.

2.3 Out of Scope Items

16. The following items were outside the scope of my assessment.

- Consistent with the scope of the RP's submissions for GDA, load follow operation will not be subject to explicit regulatory assessment within the scope of the Fault Studies Step 4 assessment.
- Detailed assessment of the faults that could occur within the Spent Fuel Interim Storage (SFIS) is out with the scope of the RP's submissions for GDA and will similarly be outside of the scope of the Fault Studies Step 4 assessment.
- Faults arising from naturally occurring hazards have been considered by ONR's external hazards assessment along with the claimed protection against them and are out with the scope of this assessment.
- The characterisation of hazards internal to the building, and the adequacy of engineered barriers against these have been considered by ONR's internal hazards assessment and out with the scope of this assessment.
- As part of my assessment I have considered the potential for faults within the fuel route to lead to a radiological release, however criticality faults that could occur within the fuel route are out with the scope of this assessment.
- An objective of this assessment has been to judge the adequacy with which the RP has identified significant limits and conditions from its UK HPR1000 fault studies safety case. However, a detailed assessment of setpoints, technical specifications, operating procedures and emergency arrangements has not been performed.
- Faults associated with construction and commissioning need to be addressed by an appropriate safety case during the relevant construction and commissioning stages, hence are not within the scope of GDA.

2.4 Standards and Criteria

17. The relevant standards and criteria adopted within this assessment are principally the SAPs (Ref. 2), TAGs (Ref. 4), relevant national and international standards, and relevant good practice informed from existing practices adopted on nuclear licensed sites in Great Britain. The key SAPs and any relevant TAGs, national and international standards and guidance are detailed within this section. Relevant good practice (RGP), where applicable, is cited within the body of the assessment.

2.4.1 Safety Assessment Principles

18. The SAPs (Ref. 2) constitute the regulatory principles against which ONR judge the adequacy of safety cases. The SAPs applicable to Fault Studies are included within Annex 1 of this report. The key SAPs applied within my assessment were SAPs FA.1 to FA.9, ECS.1 to ECS.3, AV.1 to AV.8, and Target 4.

- SAPs FA.1 to FA.3 set general expectations for the assessment of fault analysis (including Design Basis Analysis (DBA), Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA)).
- The main fault analysis SAPs FA.4 to FA.9 present established practice in the UK for DBA.
- ECS.1 to ECS.3 provide ONR expectations for the categorisation of safety functions and the classification of the equipment that deliver those functions, and how this should be informed by the DBA.
- AV.1 to AV.8 are principles governing the methods and data used in safety case analyses.

- Target 4 defines the faults for which ONR would expect DBA to be undertaken and also the acceptability of mitigated consequences of design basis fault sequences.

2.4.2 Technical Assessment Guides

19. The following Technical Assessment Guides were used as part of this assessment (Ref. 4):

- NS-TAST-GD-005, ONR Guidance on the Demonstration of ALARP.
- NS-TAST-GD-006, Design Basis Analysis.
- NS-TAST-GD-035, Limits and Conditions for Nuclear Safety (Operating Rules)
- NS-TAST-GD-051, The Purpose, Scope and Content of Nuclear Safety Cases.
- NS-TAST-GD-094, Categorisation of Safety Functions and Classification of Structures, Systems and Components.

2.4.3 National and International Standards and Guidance

20. The following international standards and guidance were used as part of this assessment (Refs. 8 and 9):

- IAEA SSR-2/1, Safety of Nuclear Power Plants: Design.
- IAEA SSG-2, Deterministic Safety Analysis for Nuclear Power Plants.
- IAEA SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants.
- WENRA, Reactor Safety Levels for Existing Reactors.
- WENRA, Statement on Safety Objectives for New Nuclear Power Plants.
- WENRA, Safety of New NPP Designs.

2.5 Use of Technical Support Contractors

21. It is usual in GDA for ONR to use Technical Support Contractors (TSCs) to provide access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision making.

22. Table 1 below sets out the areas in which I used TSCs to support my assessment. I required this support to provide additional technical expertise and capability.

Table 1: Work Packages Undertaken by the TSC

Number	Description
1	Tractebel undertook an independent review of the verification and validation evidence submitted for the computer codes used by the RP for analysis of reactor transients. (ONR385)
2	GRS performed independent confirmatory analysis of a selection of fault sequences to gain confidence in the RP's analysis methods. (ONR 396)

23. The review by my TSC of the verification and validation evidence submitted by the RP for the computer codes has been a significant input into my assessment. I have summarised the outcomes of the TSC review and my assessment of the codes in Appendix 1.

24. The independent confirmatory analysis undertaken by my TSC has been referenced on a case-by-case basis as part of the assessment of key design basis reactor transients within Section 4.3. This analysis has been undertaken using the ATHLET code.

25. Whilst the TSCs undertook detailed technical reviews, this was done under my direction and close supervision. The regulatory judgment on the adequacy, or otherwise, of the generic UK HPR1000 safety case in this report has been made exclusively by ONR.

2.6 Integration with Other Assessment Topics

26. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot be carried out in isolation as there are often issues that span multiple disciplines. I have therefore worked closely with a number of other ONR inspectors to inform my assessment. The key interactions were:

- The RP has developed a list of initiating events which is used as a common input for both the DBA and PSA. The detailed postulated initiating event (PIE) identification process has been considered in detail by ONR's PSA inspector. The RP has also used the PSA as part of the identification of design extension conditions. I therefore worked closely with the PSA inspector.
- The technical basis and validity of the acceptance criteria related to fuel failure considered in this assessment report have been assessed by ONR's Fuel and Core inspector. The basis for acceptance criteria of the reactor coolant barrier has been assessed by ONR's Structural Integrity inspector. The basis for acceptance criteria on the containment structure has been assessed by ONR's Civil Engineering inspector. I have worked with the relevant ONR inspectors when considering the results of the RP's analysis against these acceptance criteria.
- The deterministic analysis within the scope of the faults studies assessment requires core physics design data. The RP has produced data for use in the analysis of design basis faults and design extension conditions and the adequacy of this data has been assessed by ONR's Fuel and Core inspector.
- The Fuel and Core topic has also considered the adequacy of the specialist computer codes which are used to model the reactor physics. In addition, the Fuel and Core inspector has also assessed the validity of sub-channel codes and codes predicting fuel behaviour under accident conditions.
- The safety analysis performed by the RP uses conservative assumptions on system performance and the timing of key events. I have worked closely with the engineering topic areas throughout my assessment to gain confidence that the assumptions related to system performance used in the safety analysis are appropriate and reflected in engineering specification documents.
- Internal and external hazards are potential initiators of faults and have been considered by the RP within the safety case. I have worked with ONR's Internal and External hazards inspectors to understand the progression of these faults and the protection against them. However, the completeness of the list of hazards considered by the RP and the adequacy of barriers that protect against hazards (or limit their consequences) has been separately assessed by inspectors who specialise in internal and external hazards.
- The treatment of wastes arising and operation of the radioactive waste management systems has been considered within the Radioactive Waste Management topic area. My assessment has considered the RP's fault identification process for these systems and the claim that there are no design basis faults arising from these systems.
- The risk of hydrogen combustion from accident conditions has been assessed in detail by the Severe Accident Analysis inspector. As the challenges from

combustible gases are more onerous in severe accident conditions, I have worked with the Severe Accident Analysis inspector to gain confidence that the relevant systems will also be effective in mitigating hydrogen risk arising from design basis accidents.

- The containment heat removal system provides a diverse means of cooling of the reactor during some fault conditions if the normal cooling chain is lost. It is also used to mitigate the consequences of a severe accident where the fuel melts. I have worked closely with the Severe Accident Analysis inspector to ensure that the RP has demonstrated that this system is effective in performing its safety functions and that the methodologies employed in the analysis of the effectiveness are appropriate.
- In this report, I have looked in detail at the RP'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.

2.7 Overseas Regulatory Interface

27. ONR has formal information exchange agreements with a number of international nuclear safety regulators, and collaborates through the work of the International Atomic Energy Agency (IAEA) and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). This enables us to utilise overseas regulatory assessments of reactor technologies, where they are relevant to the UK. It also enables the sharing of regulatory assessments, which can expedite assessment and helps promote consistency.

2.7.1 Bilateral Collaboration

28. As part of my assessment I have engaged with the Chinese nuclear safety regulator, National Nuclear Safety Administration (NNSA), to discuss the computer codes used in the reactor transient analyses which form a major part of the fault studies parts of the safety case. Through these engagements I established that NNSA have not yet completed the regulatory review of the computer codes used by the RP for the UK HPR1000 safety case. NNSA however gave assurance that the analysis conducted for the reference plant using alternative codes show acceptable results against the relevant acceptance criteria. I have considered this within my regulatory judgement on the adequacy of the codes for GDA.

2.7.2 Multilateral Collaboration

29. ONR also represents the UK at the Multinational Design Evaluation Programme (MDEP), facilitated by OECD-NEA. MDEP seeks to:

- enhance multilateral co-operation within existing regulatory frameworks;
- encourage multinational convergence of codes, standards and safety goals; and
- implement the products it develops in order to facilitate the licensing of new reactors.

30. The HPR1000 Working Group is made up of representatives from ONR, NNSA, Autoridad Regulatoria Nuclear (ARN, Argentina's nuclear safety regulator) and the National Nuclear Regulator (NNR, South Africa's nuclear safety regulator). Through membership of the HPR1000 Working Group I have shared assessment progress and sought to understand shared regulatory expectations to maximise the ability to influence improvements in safety.

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the Generic UK HPR1000 Design

31. The generic UK HPR1000 design is described in detail in the PCSR (Ref. 3). It is a three-loop PWR designed by CGN using the Chinese Hualong technology. The generic UK HPR1000 design has evolved from reactors which have been constructed and operated in China since the late 1980s, including the M310 design used at Daya Bay and Ling'ao (Units 1 and 2), the CPR1000, the CPR1000$^+$ and the more recent ACPR1000. The first two units of CGN's HPR1000, Fangchenggang Nuclear Power Plant (NPP) Units 3 and 4, are under construction in China and Unit 3 is the reference plant for the generic UK HPR1000 design. The design is claimed to have a lifetime of at least 60 years and has a nominal electric output of 1,180 MW.

32. The reactor core contains zirconium clad uranium dioxide (UO_2) fuel assemblies and reactivity is controlled by a combination of control rods, soluble boron in the coolant and burnable poisons within the fuel. The core is contained within a steel Reactor Pressure Vessel (RPV) which is connected to the key primary circuit components, including the Reactor Coolant Pumps (RCPs), Steam Generators (SGs), pressuriser and associated piping, in the three-loop configuration. The design also includes a number of auxiliary systems that allow normal operation of the plant, as well as active and passive safety systems to provide protection in the case of faults, all contained within a number of dedicated buildings.

33. The reactor building houses the reactor and primary circuit and is based on a double-walled containment with a large free volume. Three separate safeguard buildings surround the reactor building and house key safety systems and the main control room. The fuel building is also adjacent to the reactor and contains the fuel handling and short-term storage facilities. Finally, the nuclear auxiliary building contains a number of systems that support operation of the reactor. In combination with the diesel, personnel access and equipment access buildings, these constitute the nuclear island for the generic UK HPR1000 design.

34. One of the purposes of DBA is to demonstrate the effectiveness of the safety measures within the generic UK HPR1000 design. These safety measures are included to ensure that the critical safety functions of cooling, criticality and containment are controlled in the reactor or Spent Fuel Pool (SFP) in the event of a design basis fault. Within the generic UK HPR1000 safety case (and this report), safety measures are described with a system code followed by an acronym in the form XXX [YYY]. The principal safety measures are:

- Reactor Protection System (RPS [PS])
  - The RPS [PS] is a centralised Control and Instrumentation (C&I) platform which actuates the safety systems based upon measured plant parameters.
- Reactor Trip
  - In the event of a fault the reactor trip is initiated which inserts the Rod Cluster Control Assemblies (RCCAs), providing a rapid insertion of negative reactivity to terminate the nuclear reactions.

- Safety Injection System (RIS [SIS])
  - The RIS [SIS] injects borated water into the reactor coolant system to control the reactivity of the reactor and provide cooling of the reactor core.
  - There are three trains of RIS [SIS], each consisting of an accumulator, medium head safety injection (MHSI) and low head safety injection (LHSI)
  - The RIS [SIS] also provides a Residual Heat Removal (RHR) function for long term cooling.
- Atmospheric Steam Dump System (VDA [ASDS])
  - The VDA [ASDS] discharges steam from the secondary circuit into the atmosphere to cool the reactor.
- Emergency Feedwater System (ASG [EFWS])
  - When normal feedwater is lost, the ASG [EFWS] supplies water to all three SGs to remove the residual heat to cool the reactor until the RHR conditions are reached.
- Containment Isolation function Group (CIG)
  - The CIG consists of multiple centralised C&I systems and isolation valves on systems of all penetrations of the containment (except the main steam isolation valves (MSIVs). It's safety function is to prevent radioactive leakage from the containment during accidents.
- Pressuriser Relief Valves (PRVs)
  - The PRVs are designed to prevent RCP [RCS] overpressure and loss of integrity of the RCP [RCS]. Three pilot operated PRVs are connected to the pressuriser. All PRVs have different setpoints.
- Component Cooling Water System (RRI [CCWS]) Essential Service Water System (SEC [ESWS])
  - These systems provide the primary cooling chain for components important for safety, such as the RCPs and the RHR heat exchanger.
- Fuel Pool Cooling and Treatment System (PTR [FPCTS])
  - The PTR [FPCTS] removes decay heat for the fuel assemblies stored within the Spent Fuel Pool (SFP). The PTR [FPCTS] also maintains boron concentration in the SFP and provides water purification, filling and discharge for the reactor pools, spent fuel building pools, In-Containment Reactor Water Storage Tank (IRWST) and In Vessel Retention (IVR) tank.

35. The generic UK HPR1000 design includes a number of specific features to protect against more extreme fault conditions and ensure that the plant can be returned to a safe condition without core damage. These systems are:

- Containment Heat Removal System (EHR [CHRS])

- The function of the EHR [CHRS] is to limit the pressure increase of the containment and ensure cooling of the IRWST if RHR fails.

- Extra Cooling System (ECS [ECS])
  - This is an extra cooling source for the Containment Heat Removal System (EHR [CHRS]) and Fuel Pool Treatment and Cooling System (PTR [FPTCS]) in the event of a Total Loss of Cooling Chain (loss of Component Cooling Water System (RRI [CCWS]) or the Essential Service Water System (SEC [ESWS]))
- Safety Chilled Water System (DEL [SCWS])
  - The DEL [SCWS] provides a diverse cooling chain to cool the LHSI pumps in the event of a failure of RRI[CCWS] and/or SEC [ESWS].
- Station Black Out Diesel Generators
  - In the case of a Station Black Out (SBO, a loss of off-site power with common cause failure of Emergency Diesel Generators) two SBO DGs are available to supply electricity to the required safety systems.
- Diverse Actuation System (KDS [DAS])
  - The KDS [DAS] is designed to provide protection against failure of the RPS [PS].
- Emergency Boration System (RBS [EBS])
  - The RBS [EBS] system provides protection against a failure of reactor trip and provides hold down after shutdown.
- Manual feed and bleed operation
  - Manual feed and bleed is achieved by opening three trains of the Pressuriser Safety Valves and actuation of RIS [SIS].
- Low pressure full cooldown (LCD)
  - LCD is designed to depressurise the primary pressure rapidly for the efficient injection of LHSI in the case of a small break loss of coolant accident (SB-LOCA) with total loss of MHSI, This function is realised by operators via the stepwise pressure setpoint reduction leading to full opening of all VDA [ASDS].
- Secondary Passive Heat Removal System ASP [SPHRS]
  - The ASP [SPHRS] is designed as a passive means to remove decay heat from the reactor when the active heat removal system fails. The ASP [SPHRS] tank can also be used as a water source for the ASG [EFWS] tank or as a water source to make up the SFP in the event of a loss of normal cooling or loss of inventory accident.

36. The generic UK HPR1000 design also includes a variety of equipment for the handling of new and spent fuel. The fuel handling and storage system PMC [FHSS] includes the

auxiliary crane for handling new fuel, the SFP crane for handling spent fuel within the SFP and the refuelling machine for transferring assemblies within the reactor cavity.

3.2 The Generic UK HPR1000 Safety Case

37. The nuclear safety objective of the UK HPR1000 safety case is defined in Chapter 4 of the PCSR (Ref. 3) as follows:

- The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defence to fulfil the fundamental safety functions, reducing the nuclear safety risks to a level that is as low as reasonably practicable.

38. In this section I provide an overview of the fault studies aspects of the generic UK HPR1000 safety case as provided by the RP during GDA. Details of the technical content of the documentation and my assessment of its adequacy are reported in the subsequent sections of my report.

3.2.1 PCSR

39. The PCSR has 33 chapters. The following two chapters are most relevant to ONR's fault studies assessment:

- Chapter 12: Design Basis Condition Analysis (Ref. 3).
- Chapter 13: Design Extension Conditions and Severe Accident Analysis (Ref. 3).

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

- Chapter 4 General Safety and Design Principles
- Chapter 5 Reactor Core
- Chapter 6 Reactor Coolant Systems
- Chapter 7 Safety Systems
- Chapter 8 Instrumentation and Control
- Chapter 9 Electric Power
- Chapter 10 Auxiliary Systems
- Chapter 11 Steam and Power Conversion System
- Chapter 14 Probabilistic Safety Assessment
- Chapter 15 Human Factors
- Chapter 18 External Hazards
- Chapter 19 Internal Hazards
- Chapter 31 Operational Management
- Chapter 33 ALARP evaluation

41. The PCSR is a top tier document and is supported by a range of references. Tier 2 documents are the principal references to the PCSR, and these are in turn supported by Tier 3 documentation. The principal references for Chapters 12 and 13 of the PCSR are the transient analyses for each bounding fault sequence and the methodologies and input data for the analyses. The safety functions and requirements for each system are presented in a suite of System Design Manuals (SDMs) which are supporting references to Chapters 6 to 11 of the PCSR.

3.2.2 Safety Case Submissions Addressing Regulatory Observations

42. During the course of my assessment I identified a number of significant gaps in the RP's safety case that needed to be addressed through regulatory observations (ROs):

- RO-UKHPR1000-0021 Demonstration of the Adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of Structures, Systems and Components Important to Safety
- RO-UKHPR1000-0023 Demonstration of Diverse Protection for Frequent Faults
- RO-UKHPR1000-0027 Debris effects on Safety Injection System and Containment heat Removal System performance
- RO-UKHPR1000-0032 Inadvertent Flooding of the Reactor Pit
- RO-UKHPR1000-0056 Fuel Route Safety Case

43. Final safety case submissions from the RP to address these ROs were supplied during GDA Step 4. This work has been fully integrated into the wider safety case and is reflected within the PCSR. With the original gaps filled, the safety case aspects dealt with by these ROs are not of more or less significance than any other part of the UKHPR1000 safety case.

3.2.3 General Safety Case Aspects

44. Chapters 4, 12 and 13 of the PCSR set out the general principles and approaches to the deterministic analysis of fault sequences. Selected aspects of this methodology are described in this section.

45. The fault studies safety case is summarised within a Fault Schedule (Ref. 10) which contains all design basis and design extension conditions along with relevant safety functions and the safety measures which deliver them.

3.2.3.1 Event Categories

46. The PCSR Chapter 12 (Ref. 3) outlines the RP's process for the identification of PIEs and how they are grouped and bounded by similar consequences or plant response. The RP has defined criteria for inclusion of PIEs within the design basis which are applicable to any faults or hazards which may arise within the reactor, fuel route or waste treatment routes. Such design basis faults are termed Design Basis Conditions (DBCs) and the RP has assigned the bounding faults into one of four DBC categories based on the frequency of occurrence or based on good practice from other nuclear power plant (Ref. 11). The four categories are:

- DBC-1: Normal Operation. Operation within specified operational limits and conditions
- DBC-2: Anticipated operational occurrences. An operational process deviating from normal operation which is likely to occur at least once during the operational lifetime of a single unit facility but which, because of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.
- DBC-3: Design Basis Condition category 3. Conditions that may occur once during the lifetime of a fleet of operating plants and may result in the failure of a small fraction of the fuel rods but do not generate a Design Basis Category 4 condition or result in the consequential loss of function of the Reactor Coolant System or Containment System.
- DBC-4: Design Basis Condition category 4. Conditions which are not expected to occur but are postulated because their consequences could include the potential release of significant amounts of radioactive material; they are the

most extreme conditions which must be considered in the design and they represent limiting cases.

47. For each DBC the RP has identified safety measures to protect the core and prevent a radiological release. The analyses of the resulting transients is split into two phases, a short term phase to the controlled state and a longer term phase to a safe state. This analysis aims to show that, based on successful operation of the safety measures, a defined set of acceptance criteria are met. The RP has also taken consideration of UK practice and further considered faults as either frequent or infrequent faults. For frequent faults the RP has established the need for diversity in the delivery of safety functions.

Table 2: UK HPR1000 Design Conditions

<table>
<tr><th>UK HPR1000 Design Condition</th><th>Frequency (per year)</th><th>Description</th></tr>
<tr><td>DBC-1</td><td>≥1</td><td rowspan="2">Normal Operation</td></tr>
<tr><td rowspan="2">DBC-2</td><td rowspan="2">Frequency ≥10^{-2}</td></tr>
<tr><td rowspan="3">Frequency ≥10^{-2}</td><td rowspan="2">Frequent Faults</td></tr>
<tr><td rowspan="2">DBC-3</td></tr>
<tr><td>10^{-2}> Frequency ≥10^{-3}</td><td rowspan="2">Infrequent Faults</td></tr>
<tr><td>10^{-3}> Frequency ≥10^{-4}</td></tr>
<tr><td>DBC-4</td><td>10^{-4}> Frequency ≥10^{-5}</td></tr>
</table>

48. The list of DBCs for the generic UK HPR1000 safety case is reproduced as Table 3 of this report. Each of the initiating events is postulated to occur in one or more plant operating state (POS). The majority of PIEs are postulated to occur during POS A, and one or multiple shutdown modes. For these faults, the RP claims that the consequences of faults that occur from full power are limiting, which bounds the same fault in low power or shutdown modes. Other faults which are unique to shutdown conditions are also included in the list of DBCs.

49. It should be noted that in the generic UK HPR1000 safety case, one initiating event could be treated as two or more different faults at different states. For example, a break in pipework could occur in different plant states and may be treated as different design basis faults with different predicted frequencies of occurrence.

50. Within Chapter 12, the RP has stated that design basis fault sequences have been considered to a frequency of 10^{-7} per year. Taken together with a limit of claims of safety system reliability (probability of failure on demand) of 10^{-4} the RP require a diverse means of delivering safety functions for frequent faults. Such sequences are identified within Chapter 12 and analysis has been submitted (Ref. 12) for bounding sequences.

3.2.3.2 Design Extension Conditions

51. DEC-A events are low frequency events where the conditions may be more severe than those identified in the DBC analysis and are considered by the generic UK HPR1000 safety case in Chapter 13 of the PCSR (Ref. 3). The RP defines DEC-A events as those without significant fuel degradation. Specifically, these sequences

involve multiple failures or sequences following more severe initiating events than those considered in the design basis. Protection measures are included within the design to prevent core damage. The list of DEC-A events is reproduced in Table 4 of this report.

3.2.3.3 Safety Functions

52. The RP has defined four fundamental safety functions that need to be delivered in all plant states in the generic UK HPR1000 safety case. These are:

- R: Control of Reactivity
- H: Removal of heat from the reactor and fuel store
- C: Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.
- E: Extra safety functions which support the delivery of the other functions.

53. These are decomposed into high-level safety functions which are further developed into low-level safety functions and applied in safety system design. The high-level safety functions are:

- Control of reactivity
  - R1: Maintain core reactivity control;
  - R2: Shutdown and maintain core sub-criticality;
  - R3: Prevention of uncontrolled positive reactivity insertion into the core;
  - R4: Maintain sufficient sub-criticality of fissile material stored outside the reactor coolant system but within the site.
- Removal of heat
  - H1: Maintain sufficient Reactor Coolant System water inventory for core cooling;
  - H2: Remove heat from the core to the reactor coolant;
  - H3: Transfer heat from the reactor coolant to the ultimate heat sink;
  - H4: Maintain heat removal from fuel stored outside the RCS but within the site.
- Confinement
  - C1: Maintain integrity of the fuel cladding to ensure confinement of radioactive material;
  - C2: Maintain integrity of the Reactor Coolant Pressure Boundary to ensure confinement of radioactive material;
  - C3: Maintain integrity of reactor containment to ensure confinement of radioactive material;
  - C4: Maintain integrity of the fuel stored outside of reactor containment;
  - C5: Store the radioactive material;
  - C6: Shield against radiation, control planned radioactive releases, and limit accidental radioactive releases.
- Extra safety functions
  - E1: Support Type R, H or C safety function;
  - E2: Prevent, protect and mitigate hazards impact.

54. These safety functions form the basis of the Fault Schedule (Ref. 10) which presents, for each DBC and DEC-A event, the safety measures which deliver these safety functions.

3.2.3.4 Categorisation of Safety Functions and Classification of SSCs

55. The approach to safety categorisation and classification for the generic UK HPR1000 safety case is summarised within Chapter 4 of the PCSR (Ref. 3) and is based upon the IAEA Safety Standard SSG-30 (Ref. 6). The detail of this method is contained within Ref. 13.

56. In this approach, safety functions are categorised based upon their role in delivering defence in depth, whether the function contributes to achieving a safe state or a controlled state, and the potential consequences of not delivering the safety function. Three function categories are defined and the classification of equipment delivering the function directly matches the categorisation. Therefore, equipment that deliver a category 1 safety function are assigned safety class 1, that which delivers a category 2 function are assigned safety class 2 and that which delivers a category 3 function are safety class 3.

57. The generic UK HPR1000 safety case uses the notation F-SC1, F-SC2 and F-SC3 to indicate safety class 1, 2 and 3, respectively.

58. Alternatively, some SSCs are classified directly based on the consequences of failure (loss of integrity). The potential consequences are graded as High, Medium or Low (as defined in Ref. 13). These SSCs are referred to as ‘Design Provisions’. The generic UK HPR1000 safety case uses B-SC1, B-SC2 and B-SC3 to indicate Design Provisions Class 1, 2 and 3 which informs the structural integrity classification of components, as presented in Chapter 17 of the PCSR (Ref. 3).

59. Of most relevance to the scope of my assessment:

- SSCs which deliver a function to reach a controlled state under DBC-2, DBC-3 or DBC-4 conditions are F-SC1;
- SSCs which deliver a function to reach a safe state under DBC-2, DBC-3 or DBC-4 conditions are F-SC2;
- SSCs which provide a diverse means of delivering a Category 1 function in a frequent fault are F-SC2;
- SSCs which provide a diverse means of delivering a Category 2 function in a frequent fault are F-SC3;
- SSCs which deliver DEC-A functions are F-SC3.

60. Support systems that are required by 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.

61. The RP has submitted a suite of System Design Manuals (SDMs) which summarise the required safety functions, SSC classifications and performance requirements, along with other system information.

3.2.3.5 Approach to Single Failures, Maintenance and Redundancy

62. The UK HPR1000 has been designed against a number of design requirements to ensure the availability and reliability of the safety systems, depending on the classification of these systems. These requirements can be summarised as follows:

- F-SC1 systems must meet the single failure criterion and as such must include redundancy.
- F-SC2 systems may not need redundancy but if it does not meet the single failure criteria then another system must fulfil the same function (functional diversity). An FSC-2 system is not required to meet the single failure criterion if it performs a function that provides a backup to a Category 1 function.
- F-SC3 systems do not need to meet the single failure criterion.

63. In its DBA the RP does not consider that any systems or trains of systems would be unavailable due to maintenance, as the maintenance activities and tests are scheduled only when the systems are not required to deliver their safety functions.

3.2.3.6 Computer Codes for Reactor Transient Analysis

64. The transient analysis for reactor faults has been undertaken using the RP's in-house computer codes. These codes have not been used for the licensing activities for the reference plant and have not previously been used outside of China. The principal analysis codes used by the RP for reactor transient analysis are:

- LOCUST is a system thermal-hydraulic code, which is used to simulate two-fluid, non-equilibrium, and heterogeneous hydrodynamic conditions (predominantly occurring in LOCA faults). A pessimised version of LOCUST has been developed which follows the Appendix K method of US Nuclear Regulatory Commission (NRC) and is called LOCUST-K. The RP has used both LOCUST and LOCUST-K within the assessment of DBCs and DEC-A events.
- GINKGO is a thermal hydraulic code used in the analysis of most intact circuit faults. It is described by the RP as a realistic conservative code.
- CATALPA is a containment modelling code, used to evaluate the transient conditions in the containment during design basis accidents.

65. The RP has submitted qualification reports for each of the computer codes used for the reactor transient analysis. These qualification reports (Refs. 14 to 16) provide an overview of the code and the qualification evidence. They are supplemented by Validation and Verification reports (Refs. 17 to 19) which provide the detail of the evidence for the suitability of the codes.

66. Analysis of SFP faults has been undertaken using simpler methods such as heat balance equations. For radioactive waste faults the analysis is predominantly based on the estimation of radiological release.

4 ONR ASSESSMENT

4.1 Structure of Assessment Undertaken

67. The fault studies assessment is reported in various sections, reflecting the assessment strategy set out in the Step 4 Assessment Plan (Ref. 5) and Section 2 of this report:

- In Section 4.2 I have considered the general aspects of the RP's fault studies safety case. These general aspects provide the criteria and methods by which the RP has analysed potential fault sequences and the demonstration that the plant has sufficient protection against these faults.
- In Section 4.3 I have presented my assessment of the design basis reactor faults, sub-divided to consider groups of similar faults. Where the analysis of faults occurring from power bounds other plant states I have included this discussion in this section.
- In Section 4.4 I have presented my assessment of design extension conditions.
- In Section 4.5 I have presented my assessment of fuel route faults.
- In Section 4.6 I have presented my assessment of other non-reactor faults
- In Section 4.7 I have discussed the adequacy of the RP's method for the calculation of off-site radiological consequences and compared the resulting doses with the expectations set by ONR's SAPs FA.7 and Target 4.
- In Section 4.8 I have discussed the way in which the fault studies safety case has contributed to the demonstration that risks are reduced ALARP.
- In Section 4.9 I have recorded my views on the final (consolidated) safety case and any significant differences from the documents that have been assessed in previous sections.
- In Section 4.10 I have given a summary of a comparison with standards, guidance and Relevant Good Practice

4.2 General Aspects

68. ONR's SAP FA.1 (Ref. 2) sets the general expectation that fault analysis should be carried out, comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrates that risks are ALARP. FA.4 states that DBA should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures. By submitting the information within Chapters 12 and 13 of the PCSR I am content that these general expectations have been met and my assessment recorded in this section leads to my conclusion on the adequacy of this analysis.

4.2.1 Event Categories and Acceptance Criteria

69. ONR's SAP FA.5 (Ref.2) sets the criteria for which faults should be considered within the design basis, based on the well-established principles of using the predicted frequency of occurrence. The initiating event frequency of a design basis fault should be calculated on a best estimate basis and NS-TAST-GD-006 (Ref. 4) also sets the expectation that for less frequent initiating events it may be acceptable to relax some of the criteria or have less confidence in the integrity of one physical barrier.

70. The criteria chosen by the RP, of including events down to 10^{-5} per annum (pa), is identical to those outlined in SAP FA.5. The list of design basis faults for the generic UK HPR1000 safety case are contained within Ref. 11 and reproduced as Table 3 within this document. Within Ref. 11, the RP differentiates between frequent and infrequent faults with frequent faults being those with a frequency of occurrence greater than 10^{-3} per annum. In practice this means that all DBC-2 and some DBC-3 faults are considered as frequent faults. The distinction between frequent and infrequent fault is a common approach to UK safety cases to set deterministic rules for

the number of safety systems required for various faults and I am content that this is appropriate and is an important part of demonstrating the fault tolerance of the generic UK HPR1000 design.

71. I am content to judge that the RP's approach to categorising internal design basis faults as set out in the PCSR Chapter 12 is consistent with the expectations of FA.5 and NS-TAST-GD-006 for faults arising within the facility.

72. The RP has also considered sequences of events which have a frequency of occurrence lower than those within the design basis. The RP has termed these events as Design Extension Conditions and are considered within Chapter 13 of the PCSR. The identification of DEC-A events includes sequences with a frequency cut-off around 10^{-7} pa. The SAPs (FA.6) sets the expectation that this would be a typical cut-off for applying design basis techniques and the RP's approach is also consistent with international guidance (as described in IAEA SSR-2/1 and SSG-2, Ref. 8). I am therefore content with the RP's fault categorisation of low frequency sequences, with the objective of demonstrating that there are no cliff edges (escalation of consequences) just beyond the design basis.

73. For each category of fault the RP has assigned a set of acceptance criteria (Ref. 11). Compliance with these acceptance criteria ensures that the safety objectives relevant to the DBC accident are met. The RP has set two main types of acceptance criteria: radiological limits and decoupling criteria.

- The 'Radiological Protection Targets' (RPTs) used by the RP are identical to numerical targets set out in ONR's SAPs (FA.7 and Target 4). These limits provide criteria for both on-site and off-site radiological consequences and apply across the reactor, fuel route and non-reactor faults.
- In addition, for reactor faults the RP has used technical decoupling criteria which are applied to the thermal hydraulic and neutronic calculations. These decoupling criteria relate to the integrity of the barriers to the releases of radioactivity, i.e. the fuel, the primary circuit or the containment. For different accident transients, different criteria are applicable.

74. My assessment of the adequacy of the radiological analysis methods is contained within Section 4.7 of this report along with a comparison of the results against ONR's Numerical Targets. However, I am content that the radiological targets set by the RP are appropriate for GDA.

75. The decoupling criteria can be summarised as follows.

- For DBC-2 faults the RP aims to show that fuel integrity is ensured by a demonstration that there is no Departure from Nucleate Boiling (DNB) and that the fuel temperature remains below the fuel melting temperature.
- For non-LOCA DBC-3 and DBC-4 events no more than 10% of rods can experience DNB, and the fuel pellet melting at the hot spot must not exceed 10% by volume.
- For all DBC-3 and DBC-4 accidents which do not experience a rapid oxidation of the fuel, the peak cladding temperature must remain below 1482 °C.
- Specific criteria are applied for LOCA faults and rod ejection faults and these are discussed in the relevant sections of this report.
- Overpressure criteria for the primary and secondary circuit boundaries are set in accordance with the RCC-M methodology (this is a French standard for the design and construction of pressurised equipment within nuclear power plant). Separate analysis has been performed by the RP to demonstrate the effectiveness of the overpressure protection in Chapter 6 of the PCSR (Ref. 3).

76. The adequacy of decoupling criteria for the fuel is discussed within the Fuel and Core assessment report (Ref. 20). Other decoupling criteria are discussed in the relevant sections of this report.

77. ONR does not define the decoupling criteria to be used for reactor faults but has the expectation that the consequences of design basis faults will be minimised (SAP FA.7, Ref. 2). Setting an acceptable limit of 10% DNB is not aligned with ONR's expectation that risks should be reduced ALARP. Moreover, it is UK RGP for PWRs to provide a demonstration, so far as is reasonably practicable, that there will be no fuel failures for any design basis faults, and that there will be no DNB for frequent faults.

78. In Chapter 12 of the PCSR, the RP recognises this. Since the RP conservatively consider that DNB results in fuel failure, the RP has attempted to demonstrate that DNB will not occur in all DBC-3 and DBC-4 faults, as well as DBC-2 faults. For faults in which no DNB cannot be demonstrated, the RP has submitted a specific report to consider this expectation (Ref. 21) and I have supported the assessment of this document which is reported in the Fuel and Core Assessment report (Ref. 20) and in the relevant sections below. It should be noted that, while the criterion is expressed as no DNB, the RP's analysis expresses the results as a ratio between the heat flux needed to cause DNB and the predicted heat flux, DNBR (Departure from Nucleate Boiling Ratio).

79. To demonstrate the effectiveness of diverse means of delivering safety functions for frequent reactor faults, the RP has chosen to apply the DEC-A safety criteria. However, the RP has not defined any additional criteria for the analysis of DEC-A events, instead the DBC-4 criteria are applied. I am satisfied that this is appropriate and sets a challenging target for the demonstration that there will be no escalation of consequences for these faults, consistent with the expectations of IAEA SSG-2 (Ref. 8), and SAPs FA.6 and FA.7 (Ref. 2).

80. The safety criteria for DBC accidents associated with spent fuel storage are:

- Maintenance of sub-criticality (k_{eff} <0.98); and
- The fuel assemblies remain covered.

81. For most DBCs affecting the SFP the maintenance of cooling ensures that the SFP water does not boil. However, in some specific scenarios boiling is permitted but the above criteria are respected. These criteria are also applied to DEC-A events in the SFP. My view on the acceptability of this is reported in Sections 4.5 and 4.7 below.

82. Overall, I am content that the criteria specified in Chapters 12 and 13 of the PCSR are appropriate for the analysis of DBCs and DEC-A events. I am content that the RP has sought to demonstrate that the consequences are ALARP and consistent with UK practice, rather than limiting conclusions on adequacy to the criteria alone.

4.2.2 Identification of Design Basis Initiating Events

83. ONR's SAP (FA.2) sets the expectation that fault analysis should identify all initiating faults and that the process for identifying faults should be systematic, auditable and comprehensive. Paragraph 618 of the SAPs (Ref. 2) goes on to clarify that the scope of the fault identification should include all significant inventories of radioactive material, all planned operating modes and configurations and all sources of fault initiation.

84. The RP has recognised these expectations and has undertaken a significant amount of work to ensure that the list of design basis faults for all areas of the plant is well underpinned. Whilst reactor faults during power operations have the greatest potential

for significant consequences, during shutdown operations the plant is reconfigured in terms of the safety systems that are available and the integrity of the containment barriers. Therefore faults arising during shutdown modes will progress differently to those at power. To identify these differences, the RP has defined six discrete Plant Operating States (POS) in Ref. 22. These six operating modes are sub-divided into detailed operating states for PIE identification and safety analysis states for DBC analysis and this is presented in T-12.4-1 of Chapter 12 of the PCSR (reproduced as Table 6 of this report). The definition of operating modes is also applied consistently in RP's generic limits and conditions (Ref. 23). For the SFP, the RP has considered how these POS may impact faults that may arise in the fuel route, for example when the reactor and SFP are hydraulically connected for fuelling or defueling.

85. 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 informing the permitted plant configurations and the availability of safety systems as will be necessary to demonstrate compliance with SAP FA.9 (i.e. availability controls to be captured within technical specifications). It should be noted that the generic UK HPR1000 safety case typically refers to POS in PIE identification and uses State (A/B/C etc) within the analysis of bounding faults. As such this report uses both POS and State when discussing individual faults.

86. The RP has developed a methodology for the identification of PIEs which are then grouped according to operating conditions, fault progression and plant response into the bounding DBCs. This methodology is based on Failure Modes and Effects Analysis (FMEAs) and Master Logic Diagrams to identify those faults and hazards that could lead to a fault. The PIE list covers all significant sources of radioactivity and is used as a common input for both the DBA and PSA. The PIE identification has been considered in detail by ONR's PSA topic area (Ref. 24).

87. From the identified PIEs the RP has grouped them into similar faults (by fault progression and plant response) and determined which fault groups can bound other, less onerous faults. The list of DBCs (Table 3 of this report) includes the plant states to which the faults are relevant. Where the fault progression is similar in different POS these have been grouped by the RP and considered as a single DBC. A number of faults have been identified which are unique to shutdown POS. In this way the RP has determined the bounding set of DBCs (Ref. 11). I am content that the RP's approach to grouping of similar faults is appropriate and consistent with SAPs FA.6 and NS-TAST-GD-006 (Ref. 4)

88. The RP acknowledged early in GDA that additional work was required to ensure that the PIE list included all potential initiators of faults and so undertook additional work to investigate potential faults arising from loss of support systems and spurious actuation of C&I systems.

89. Arising from this work, the RP has identified a number of potential fault conditions not covered by existing analysis (these are reproduced in Table 5). However, these are not categorised as DBCs or DEC-A events but instead are described as Specific Studies (Ref. 11). For these specific studies, the safety analysis rules are the same as DEC-A but the decoupling criteria and safety criteria are chosen based on the frequency of the PIEs.

90. I have considered these specific studies and the adequacy of the analysis methods in the relevant sections of this report but in my opinion they should be included as either DBCs or DEC-A (depending on their predicted frequency of occurrence once the detailed design of support systems and C&I systems has been completed) and assessed accordingly. I have therefore raised the following Assessment Finding to

ensure that these faults are appropriately incorporated into the safety case by a licensee:

AF-UKHPR1000-0025 – The licensee shall, as part of detailed design, incorporate the specific studies undertaken during GDA (listed in Table 5 of this AR) into the design basis conditions or design extension conditions, supported by appropriate analysis.

91. In my opinion the work undertaken by the RP represents a welcome and ambitious intent to provide a logical and comprehensive suite of documentation to record the fault identification processes for all operating conditions. However, the safety case is complex with the various stages from PIE identification through various grouping and bounding processes to the DBC list being contained within a number of documents. These documents do not include a consistent numbering system and so, whilst I have been able to follow faults from PIE identification to the list of DBCs, it is not straightforward. Nevertheless, I am content that this does not undermine my confidence in the list of DBCs and I consider that this is a Minor Shortfall (as defined in Ref. 1).

92. To further investigate the completeness of the list of DBCs the RP has undertaken a comparison against other publicly available lists (Ref. 25). The RP has identified a number of DBCs from these other sources which are not included within the UK HPR1000 DBC list. For each of these DBCs the RP has presented a justification of why these are not included for the generic UK HPR1000 safety case; these justifications are either based on differences in the design or are excluded on grounds of low consequence.

93. The comparison of the list of DBCs with other available lists is a good addition to the safety case and is aligned with the expectations set out on fault identification in NS-TAST-GD-006 that multiple techniques should be applied to ensure the completeness of the list of initiating events. I am content that the RP's reasons for differences between the lists are reasonable. I have not examined the arguments for each instance in detail but, given the confidence gained through my detailed assessment of a sample of design basis faults (reported in other sections of Part 4) I have no reason to challenge the conclusions within Ref. 25.

94. I am therefore satisfied that the RP has presented an appropriate list of DBCs for analysis in the generic UK HPR1000 safety case (SAP FA.5), and that this is underpinned by a comprehensive fault identification process and categorisation process (FA.2).

95. As my assessment has progressed, I have identified some potential faults which were not included in the list of DBCs. I therefore sought specific arguments for these faults and my assessment is presented in the following sub-sections 4.2.2.1 and 4.2.2.2.

4.2.2.1 Reactor Coolant Pump Overspeed

96. Within the PIE list (Ref. 26) the RP has considered the potential for the RCP to run at either a lower or higher speed than is required and these are identified as PIEs. RCP underspeed leads to a low core flow and I have assessed the safety case for these faults in Section 4.3 below. An overspeed of the RCP has the potential to lead to overcooling of the core or damage to fuel assemblies, but this fault has not been taken forward as a DBC.

97. There are two potential causes of an RCP overspeed. The first is due to a frequency change within the electrical supply grid. The second cause is a turbine overspeed. A turbine overspeed can occur following a sharp load stepdown to house load. This is due to continued steam energy input and a reduction in rotational resistance from the

generator. The result is that the turbine will rapidly increase in speed. This increase in speed impacts the frequency of the RCPs and can result in overspeed.

98. The RP has considered RCP overspeed as a result of changes in grid frequency and argue (Ref 27) that such faults are naturally limited by the range of grid frequencies and that with an increased flow the reactor will reach a new steady state operation. I am content to accept this argument.

99. RCP overspeed as a result of turbine overspeed is not identified as a PIE within Ref. 26. Usually, turbines are designed with a protection system consisting of a speed control governor that will close steam valves to control the speed. If this fails, the turbine protection emergency trip system will rapidly close the steam valves. The UK HPR1000 protection system is designed to close steam supply valves if the speed exceeds 110% and, in the safety case it is not given a safety classification.

100. There is international experience of these devices failing with consequential turbine overspeed which have destroyed the turbine, caused local fires and release high energy missiles. Turbine failure as a result of overspeed and consequential failures are predominately within the scope of the ONR Internal Hazards assessment (Ref. 28). However, even if the turbine overspeed does not result in turbine damage, there is still the potential for the increased electrical frequency to lead to RCP overspeed.

101. Despite not being identified as a DBC, the generic UK HPR1000 safety case does include an assessment of RCP overspeed on the mechanical integrity of fuel assemblies. To address this specific area, Framatome has carried out analysis on behalf of the RP of a bounding RCP overspeed of 120%. This analysis shows that the increased flow will not cause damage to the fuel assemblies (Ref. 29) and the detailed assessment of this is included within the Fuel and Core Assessment Report (Ref. 20).

102. The safety case for RCP overspeed as a result of turbine overspeed is therefore based on a demonstration that the fuel assemblies are tolerant to an overspeed of up to 120% and that the turbine overspeed protection system will limit any overspeed to 110%. In my opinion this is a reasonable case to make, however it relies on the integrity of the overspeed system which is not safety classified

103. I therefore consider that there is a shortfall in visibility within the generic UK HPR1000 safety case for the turbine protection system's safety classification. However, the turbine design is not presented as complete for GDA and a licensee will need to develop the turbine design as part of site-specific implementation. Therefore, I am content not to progress this shortfall further during GDA. Instead, I have raised the following assessment finding:

AF-UKHPR1000-0028 – The licensee shall, as part of detailed design, identify and categorise the safety functions claimed to prevent turbine overspeed and classify the relevant structures, systems and components that deliver those functions.

4.2.2.2 Inadvertent IVR Initiation

104. The RPV is located in the reactor pit. In a severe accident, valves are manually operated to allow water in the IVR tank to flood the reactor pit to remove heat from the RPV. Inadvertent operation of the IVR strategy during normal operations has the potential for a thermal shock challenge to the RPV and have consequences for the thermal hydraulics within the reactor system. The RP was therefore required to produce a safety case to consider the response of the plant to such accidents. The safety case is based on the following arguments:

- The RP has undertaken fault identification work and has identified one PIE that has the potential to be considered within the design basis (Ref. 26). This PIE involves a leakage of water past two isolation valves. The RP argues that the frequency of this occurrence would be very unlikely as it would require failure of both valves and a failure of an operator to take remedial action. Active failures (such as inadvertent operation of the EHR [CHRS] pumps) are ruled out as the RP highlights that the pumps are isolated from the containment during normal operation and that filling the pit during the pump tests is very unlikely.
- Irrespective of the low frequency, the RP has performed consequence analysis to determine the thermal and mechanical consequences of inadvertent reactor pit flooding. Ref. 30 demonstrates that the impact on the primary thermal hydraulics and subsequent power transient is negligible. In Ref. 31 the RP has demonstrated that there is margin to the appropriate failure criteria of the RPV and fuel. ONR's Structural Integrity inspector considers that the confidence that can be gained from the methodologies and analysis results is commensurate with the risk and this is considered in more detail in the Structural Integrity Step 4 report (Ref. 32).
- The RP has undertaken optioneering to identify potential improvements (Ref. 33). Following consideration of these options the RP concludes that the extant design represents the ALARP solution. I welcome this willingness to look for further improvements and I am content that the RP met the expectations of NS-TAST-GD-005 (Ref. 4) and has demonstrated that the benefit gained from any modification is grossly disproportionate to the disbenefits.

105. On the basis of the low frequencies of the PIE and the benign consequences the RP does not consider inadvertent reactor pit flooding as a design basis fault. On the basis of the work that has been submitted I am content to judge that the safety case meets the expectations of FA.3 that analysis should be carried out to provide understanding of the behaviour of a facility under fault conditions. I am also content that the inadvertent IVR initiation fault is not a design basis fault, as defined by SAP FA.5 and Target 4.

4.2.3 Identification of Diverse Protection for Frequent Faults

106. As noted above, the RP has sought to demonstrate diverse protection for frequent faults. The fault schedule (Ref. 10) clearly highlights the primary and diverse lines of protection for each of the safety functions required to bring the plant to a safe state and a controlled state following a frequent fault. The RP has considered a common cause failure of the safety signal, C&I system or safety system such that it cannot deliver its required function and identified an alternative (diverse) means. I am content that the layout of the fault schedule is clear and that it demonstrates that the RP has taken a methodical approach to the identification of diverse lines of protection.

107. To demonstrate that the systems can be considered as independent and diverse from each other the RP has submitted several documents. The extent to which the RP has demonstrated the independence and diversity of these systems is considered within the relevant engineering topic area and is out of scope of this report. Nevertheless, I consider that the work that has been undertaken by the RP in this area demonstrates an understanding of the expectations, and a number of modifications to the generic UK HPR1000 design have been made and incorporated into DR.3.0 to address some identified shortfalls. These are considered later in discussion of the relevant design basis faults.

108. The RP has recognised that it is not feasible or necessary to analyse all fault sequences involving the diverse protection to demonstrate their effectiveness. Instead, the RP has grouped the sequences (Ref. 34) where they make similar demands on safety systems and identified 27 bounding sequences. Some of these sequences had

previously been analysed as DBC-4 faults, some had been assessed as DEC-A events (see Section 4.2.4 below) and some required new analysis. The transient analysis is summarised within Ref. 12 which provides references to the relevant supporting analysis.

109. I have reviewed Ref. 34 and in my opinion the RP has undertaken a comprehensive and logical review of the safety functions to identify bounding sequences where the primary line is assumed to be failed. The RP has considered each fault sequence and each safety function required and for each considered a failure of the safety system, C&I system or signal. It is therefore straightforward to identify the relevant sections of the report to find the consideration for a particular fault. However, the arguments made for each fault are brief and there is often little discussion of why some sequences are bounded by others. In some instances, the RP refers to analysis which has been conducted to inform these judgements, but no references are provided. These arguments have been considered where relevant in Sections 4.3 below in consideration of the groups of design basis faults.

4.2.4 Identification of Design Extension Conditions

110. The identification and deterministic consideration of sequences that fall outside of the traditional design basis is now established international practice. IAEA SSG-2 (Ref. 8) suggests that these should include initiating events of a low frequency and sequences involving multiple failures. The generic UK HPR1000 safety case aims to demonstrate that the UK HPR1000 can tolerate these events without fuel damage or a significant radiological release.

111. To identify the DEC-A events the RP has considered international expectations, insights from the PSA and expert judgement and operating experience. The full process is described within Ref. 35 and summarised within Chapter 13 of the PCSR (Ref.3). The RP has identified from the PSA over 40 events and sequences with frequencies greater than 10^{-8} per year. The RP has considered the progression of these sequences and identified a number of bounding scenarios; this list is further supplemented by additional sequences identified from examination of international guidance documents (such as IAEA TecDoc 1791, Ref. 8.).

112. There are 18 bounding DEC-A events within Chapter 13 of the PCSR. These sequences typically involve faults with CCF of one of the main safety systems (for example a total loss of feedwater) or are a more severe version of the DBC (for example a multiple steam generator tube leak). The protection against these fault sequences is generally provided for by the DEC-A systems which are not considered within the design basis analysis.

113. I welcome the addition of specific systems to provide protection against these DEC-A events as a demonstration that there are no cliff edge effects in terms of consequences for sequences just beyond the design basis. I am content that the RP's approach to identifying and assessing these sequences is consistent with SAP FA.6 which expects that fault sequences down to 10^{-7} pa should be assessed using DBA methods. I am also content that the RP's approach is consistent with international guidance (IAEA SSR-2/1/ and SSG-2, Ref. 8 and WENRA Safety Objectives for New NPP, Ref. 9).

4.2.5 Safety Functions and Classification of SSCs

114. SAPs ESC.1 to ESC.3 (Ref. 2) set ONR's expectations that safety functions will be identified and categorised based on their significance to safety, that SSCs that deliver the functions will be classified and that the SSCs are managed to appropriate codes and standards. These expectations are further developed in ONR's TAG NS-TAST-GD-094 (Ref. 4). I have therefore sought to gain confidence that the RP's

method for the categorisation of safety functions and classification of SSCs is appropriate and consistent with the approach to DBA, as expected by SAP ECS.1.

115. The RP's approach to categorisation and classification (Ref. 13) is based upon guidance given in IAEA Safety Guide SSG-30 (Ref. 8), amended to recognise and address UK expectations. The RP has classified both SSCs and human actions, consistent with the categorisation of safety functions. In my opinion, use of SSG-30 provides a sound foundation to the process and, at a high level can be seen to be consistent with the expectations of ECS.1 and ECS.2. I consider that the most important UK specific developments include the development of radiological criteria, the enhanced focus on on-site risks and the expansion of the guidance to apply to non-reactor faults.

116. The RP's process described in Ref. 13 is based upon an identification of safety functions, with the safety category being assigned depending on the level of defence-in-depth that the function is supporting and the severity of the consequences if the function is not performed. As I have introduced in Section 3, the following are of most relevance to my assessment:

- Functions that are required to reach a controlled state under DBC-2, 3 and 4 conditions are FC1 for the highest consequences.
- Functions that are required to reach and maintain a safe state under DBC-2, 3 and 4 conditions are FC2 for the highest consequences.
- Functions which provide a diverse backup to a Category 1 function in a frequent fault are FC2.
- Functions which provide a diverse backup to a Category 2 function in a frequent fault are FC3.
- Functions required to reach and maintain the final state in DEC-A events are FC3.

117. The definition of the key safety functions and their breakdown into system and component level functions is therefore important to the successful application of the categorisation and classification methodology described in Ref. 13. The breakdown of safety functions is described within Ref. 36 and these safety functions are then used as the basis of the fault schedule (Ref. 10). From a review of Ref. 13 I am content that this breakdown is sensible and logical and is to a level appropriate to which it can be assigned to an SSC.

118. Having defined the Function Category, the SSC Class is equivalent to the category i.e. an FC1 function is delivered by a F-SC1 system. This scheme places emphasis on the definition and breakdown of safety functions such that each safety function is delivered by a single SSC, rather than identifying multiple SSCs of different classes to deliver a higher level safety function.

119. ONR's guidance on categorisation and classification (NS-TAST-GD-094, Ref. 4) describes the factors that should be considered in the categorisation of safety functions, expanding on the general requirements of SAPs ECS.1 (Ref. 2). I am satisfied that Ref. 13 adequately describes how these factors have been considered by the RP's scheme. NS-TAST-GD-094 (Ref. 4) does recommend that the safety function categorisation and SSC classification should be distinct to avoid confusion. Notwithstanding this advice, given that there is a direct relationship between the functional categorisation and the safety classification I do not consider that this is a significant shortfall.

120. The RP also describes an approach to the direct classification of design provisions. Ref. 13 states that functional categorisation of the functions provided by design provisions is not necessary because the safety significance of the SSC can be directly

derived from the consequences of its failure. This approach is consistent with IAEA SSG-30 (Ref. 6). Table T-6-2 of Ref. 13 describes the two types of design provisions:

- those whose failure could lead directly to radiological release during normal operation; and
- those whose failure could lead to radiological release during a fault due to loss of containment of radioactive material.

121. From examination of the examples of design provisions given in Ref. 13 these are generally associated with pressure retaining SSCs such as pipework and vessels. Ref. 13 links to a specific document on the methods and requirements of Structural Integrity Classification and the application of these methods has been considered by ONR's structural integrity assessment (Ref. 32).

122. The fault schedule (Ref. 10) lists the fault sequences, safety measures and the required safety category of the function that is being delivered. It does not explicitly state the safety classification of the SSCs delivering that function but it can be inferred that the SSCs are at least of the required classification (but it may be higher). In my opinion the fault schedule is a good demonstration of the application of the methodology of categorisation and classification. The fault schedule (Ref. 10) also clearly indicates the frequent faults and the main and diverse means of delivering the required safety functions. I am content that the fault schedule is a good demonstration of the expectations of SAP FA.8.

123. Overall I am content that the scheme adopted by the RP for the generic UK HPR1000 safety case is consistent with ONR expectations (NS-TAST-GD-094, Ref. 4) and international guidance (IAEA SSG-30, Ref.086). I have reported my assessment of the categorisation of safety functions and the classification of associated SSCs against each fault that I have sampled within the relevant sections.

4.2.6 Approach to Single Failures, Maintenance and Redundancy

124. It is well established good practice to consider within the DBA the most limiting random single failure within a safety system (FA.6 and NS-TAST-GD-006). This random single failure is assumed to render part of the systems as unavailable. Together with requirements on maintenance, consideration of the single failure criterion determines the required number of independent, redundant trains provided within a safety system.

125. The RP has established some basic design rules (redundancy requirements) as follows (Ref. 13):

- The single failure criterion is applied to F-SC1 systems.
- F-SC2 systems may not need redundancy to meet the single failure criterion but in such cases another system must fulfil the safety function.
- An F-SC3 system does not need to meet the single failure criterion.

126. In my opinion, these basic rules considered in the generic UK HPR1000 design are aligned with the expectation of SAPs FA.6 and EDR.4 (single failure criterion).

127. The RP has not explicitly considered the potential for systems to be unavailable due to preventive maintenance within the safety analysis. Instead, the RP has assumed that the preventive maintenance activity can only be carried out when the safety functions are not required to deliver safety functions should a DBC-2/3/4 event occur. Since many safety functions are required to be available both at power and shutdown states in case of an accident, it was not clear in the original submissions whether this assumption was valid nor how the RP intended to identify the permitted combinations

of equipment unavailability for each operating state. This was part of RO-UKHPR1000-021 (Ref. 7).

128. In response to this RO the RP has established an Examination, Maintenance, Inspection and Testing (EMIT) Strategy, Ref. 38. This document clarifies how the EMIT requirements are derived and justified through an EMIT design process and how deterministic safety analysis is used to inform those requirements. Following the EMIT design process and method, the RP has undertaken a series of activities to demonstrate that the generic UK HPR1000 design and safety case is compatible with its EMIT strategy.

129. The most relevant part for my assessment is the EMIT windows analysis, which has been undertaken using deterministic analysis results to identify when the SSCs important to safety could be taken out of service for EMIT. Other documents then compare the available EMIT windows with the required EMIT activities.

130. In Ref. 39, the EMIT windows analysis approach is presented as a 6-step iterative process diagram with tabulated details of the considerations used to inform the steps/inputs and decision-making points that lead to the final determination of EMIT windows. The RP's EMIT windows analysis approach starts with the fault schedule to identify the safety function to be analysed and its corresponding safety feature claimed to deliver this safety function. The RP identifies all the design basis faults against which the safety feature is claimed to protect and the operating modes in which the identified faults are postulated to occur. The RP then identifies the EMIT windows of the safety feature, i.e. the operating modes in which the safety feature is not claimed.

131. From my assessment of Refs 38 and 39 I am content that the RP has adequately demonstrated that preventative maintenance activities can be managed in such a way to be consistent with the assumptions made in the DBA. I consider that the RP's EMIT windows analysis method is a good means of demonstrating how the expectation of NS-TAST-GD-006 (Ref.4) and SAP FA.9 (that DBA should provide the basis for conditions governing permitted plant configurations and the availability of safety systems) are met.

132. The required availability of systems claimed within the design basis are clearly identified within the limits and conditions document (Ref. 23). However, this document does not include those systems which may be claimed as diverse protection for frequent faults nor those required for protection against DEC-A events. Ref. 23 states that these requirements will be completed by a licensee. I expect that this will include the assumptions within the transient analysis on equipment availability for the demonstration of diverse protection for frequent faults and DEC-A events. Assessment Finding AF-UKHPR1000-0111 has been raised within the cross-cutting Assessment Report (Ref. 40) to ensure that the operating rules consider all important aspects not fully developed during GDA. I am content that resolution of this AF will ensure that the key assumptions made within Chapters 12 and 13 of the PCSR are met.

4.2.7 Analysis Codes and Methods

133. Analysis of DBCs and DEC-A events has been carried out by the RP to model the plant response to faults and demonstrate the effectiveness of the protection systems. This analysis should be performed on a conservative basis (SAPs FA.6, FA.7) using conservative assumptions, including those for plant conditions and system performance. This section summarises the assessment that I have undertaken on the RP's methods used for fault analysis. More detail of my assessment of the computer codes used for transient analysis is contained within Appendix 1 to this report.

134. To ensure that the transient analysis of the reactor DBCs will produce conservative results the RP has applied a number of assumptions (these are summarised in the PCSR Chapter 12, Ref. 3). The most significant of these assumptions can be summarised as follows:

- Conservative performance of the F-SC1 and F-SC2 systems are considered in DBC analyses.
- It must be shown in the DBC analysis that:
  - the controlled state can be reached relying only on F-SC1 systems; and
  - the transition from the controlled state to the safe state can be done relying only on F-SC1 and/or F-SC2 systems.
- F-SC3 and NC systems are not credited if their operation would have a beneficial effect. If the actuation of an F-SC3 or NC system worsens the consequences of the transient it is assumed this system is performing normally.
- The most pessimistic single failure must be assumed in a system needed to perform a safety function.
- A Loss of Off-Site Power (LOOP, due to turbine trip) shall be considered for DBC analysis where it is conservative to do so.
- Manual actions in the Main Control Room (MCR) are assumed no earlier than 30 minutes after the first significant information is transmitted to the operator. A local manual action is assumed to take place no earlier than one hour after the first significant information is transmitted to the operator.

135. In my opinion these are appropriate assumptions for the analysis of the DBCs and consistent with the expectations of FA.6 and FA.7.

136. For DEC-A analysis (and the analysis of diverse means of protection for frequent faults) the RP does not consider a random single failure or coincident Loss of Off-Site Power (LOOP), unless this is the initiating event.

137. ONR does not have explicit requirements for the analysis of diverse lines of protection or DEC-A but as FA.6 sets the expectation that sequences with a frequency down to 10^{-7} pa should be assessed using DBA methods, most of the general expectation of SAPs FA.7 and NS-TAST-GD-006 are relevant. However, ONR's NS-TAST-GD-006 notes that conservatisms for lower frequency initiating events and sequences may be relaxed and states that it is not necessary to assume a random single failure when demonstrating the effectiveness of a diverse safety measure. Noting this and given that the RP has applied the same conservative assumptions for key parameters and acceptance criteria for the demonstration of the diverse means of protection and DEC-A as the infrequent design basis faults, I am content that the RP's analysis rules are appropriate.

138. The deterministic analysis within the scope of the fault studies assessment requires information on the fuel and conditions within the core. The RP has produced data for use in the analysis of design basis faults and design extension conditions and the adequacy of this data has been assessed within ONR's Fuel and Core topic area. The RP has identified a limiting set of data chosen from a range of possible core configurations and times in life. As a result, the core data does not represent any real single core but instead is a combination of worst-case parameters. ONR's Fuel and Core Inspector has also considered the adequacy of the decay heat curves used by the RP. I worked closely with the Fuel and Core topic area during GDA and taken these conclusions into account in my assessment below.

139. The RP's analysis of reactor faults has been undertaken using a suite of proprietary CGN codes. The principal codes used in the fault studies area are the thermal hydraulics codes LOCUST and GINKGO and the containment code CATALPA. The sub-channel code LINDEN and the core physics codes PINE, COCO and BIRCH are considered within the Fuel and Core Assessment Report (Ref. 20).

140. The RP has submitted Qualification Reports and Verification and Validation (V&V) reports for each code. The Qualification Reports (Refs. 14 to 16) are essentially a high-level summary of the V&V reports and were submitted to give ONR visibility of the main aspects of the codes in advance of the V&V reports (Refs 17 to 19, which were submitted at the start of Step 4). To gain confidence in the adequacy of the evidence provided to support the use of these codes I commissioned a TSC to undertake a review of the key submissions, focussing on LOCUST and GINKGO.

141. My TSC's reviews are reported in Refs 41 to 43 and I discuss my assessment of the validation evidence for LOCUST, GINKGO and CATALPA in Appendix 1 of this report. Overall I am satisfied that the RP has demonstrated that LOCUST, GINKGO and CATALPA are appropriate for use for the analysis of DBCs and DEC-A events within the generic UK HPR1000 safety case. I am also confident that the codes have been used in such a way to ensure conservative results within the safety analysis, as expected by FA.7. However, I have raised two Assessment Findings for a licensee to strengthen the justification of these codes where my assessment has identified shortfalls:

> AF-UKHPR1000-0242 – The licensee shall provide sufficient evidence to demonstrate that the uncertainties of the LOCUST code are understood and have been accounted for within the transient analysis.

> AF-UKHPR1000-0243 – The licensee shall provide sufficient evidence to demonstrate that the uncertainties of the GINKGO code are understood and have been accounted for within the transient analysis.

142. For SFP faults, I have considered the adequacy of the methods in Section 4.5.

4.2.8 Strengths

143. In my opinion the RP has understood ONR's expectations for a robust and auditable fault identification process which includes all operating modes and has extended this to cover faults which may arise in support systems and as a result of spurious C&I actuations.

144. I am content that the RP has established clear criteria for determining the categories of design basis faults and appropriate acceptance criteria and analysis methods for them.

145. I consider that the identification and assessment of DEC-A events is aligned with modern safety case expectations to demonstrate that the generic UK HPR1000 design is tolerant to a range of fault conditions.

4.2.9 Outcomes

146. As a result of my assessments of the general aspects of the generic UK HPR1000 safety case I am content that an adequate case has been presented. However, four Assessment Findings have been raised, to be addressed by a licensee to incorporate the specific studies in to the list of DBCs and DEC-As, to review the classification of the protection against turbine overspeed and to strengthen the validation base of the LOCUST and GINKGO computer codes.

4.2.10 Conclusion

147. Based on the outcome of my assessment of the General Aspects of the fault studies safety case, I have concluded that the RP has established an appropriate basis for the identification and assessment of faults arising within the reactor and fuel route. I am content that the RP has identified an appropriate list of DBCs and DEC-A events consistent with the expectations of SAPs FA.5.

148. I have also concluded that the RP has established appropriate methods and criteria for the analysis of DBCs and DEC-A events, consistent with the expectations of SAPs FA.6 and FA.7.

149. In my opinion the fault schedule is an important demonstration of the protection available against each of the DBCs and DEC-A events and meets the expectations of SAP FA.8. I am also content that the DBA should be appropriate as an input to the safety classification and engineering requirements for SSCs, identifying limits and conditions and operator actions, as expected by SAP FA.9 (Ref. 9).

4.3 Design Basis Reactor Faults

4.3.1 Increase in Primary Side Temperature Faults

150. In a PWR a loss of secondary side cooling will lead to an increase in primary temperature. If cooling is not re-established this can lead to fuel damage. The RP has identified the following DBCs which lead to an increase in primary side temperature:

- Turbine trip
- Spurious reactor trip
- Short term LOOP of 2 hours duration
- Loss of normal feedwater flow
- Loss of one cooling train of RIS [SIS] in RHR mode
- Medium term LOOP of 24 hours duration
- Inadvertent closure of one or all main steam isolation valves
- Small feedwater system break including breaks in connecting lines to SG
- Long term LOOP of 168 hours duration
- Large feedwater system break including breaks in connecting lines to SG

151. The above faults range from DBC-2 to DBC-4 faults. I have chosen to assess a sample of the above accidents to gain confidence that the RP has demonstrated that the generic UK HPR1000 design is tolerant to increase in primary side temperature faults. My reasoning for sampling is presented below.

152. The loss of RIS [SIS] in RHR mode is a fault which can only initiate from a shutdown condition; my assessment of shutdown faults is presented in Section 4.3.7. I have therefore excluded this from my sampling of increase in primary side temperature faults.

153. Of the above, only large feedwater system piping break (referred to as large Feed Line Break (FLB) herein) and long-term LOOP are identified as infrequent faults. I have chosen to sample the large feedwater system break including breaks in connecting lines to SG as it is the limiting fault for sizing of the ASG [EFWS].

154. From the remaining faults, I have chosen to sample inadvertent closure of one or all main steam isolation valves as it presents the case which is most liming in terms of DNB.

155. In addition to the above, given the prominence of LOOP events in the above list and the international expectations for plants to be self-sufficient, I have also chosen to assess the UK HRP1000 response to LOOP accidents. In the following subsections I present my assessment of inadvertent closure of MSIV, FLB and LOOP events faults in turn.

4.3.1.1 Inadvertent Closure of One or All Main Steam Isolation Valves

156. The RP has performed transient analysis of inadvertent closure of one or all MSIVs from the initiating event to the controlled state. The transient analysis is presented in Ref. 44.

157. The inadvertent closure of one or all MSIVs is categorised as a DBC-3 which can be initiated from states in which steam is being raised (Plant Operating States (POS) A and B). The accident is characterised by a sudden decrease in steam transmission causing the SG pressure to increase, increasing the saturation temperature within the SG and rapidly reducing heat removal from the primary side. This leads to an increase in temperature and pressure in both the primary and secondary circuits.

158. Upon closure of the MSIV, the secondary pressure and temperature in the affected* SGs rises until the SG pressure high 1 signal set point is reached. As heat removal is lost, the temperature and pressure of the primary side also increases. Depending on the number of MSIVs that close in the initiating event, the PSVs may open. The SG pressure high 1 signal is received by the RPS [PS] and the reactor trip and VDA [ASDS] are initiated. Once negative reactivity is inserted by the reactor trip and heat removal is restored by VDA [ASDS] the margin to fuel failure increases significantly.

159. The associated signals, RPS [PS] and safety systems credited to reach the controlled state are all designated as F-SC1. As they provide the primary means of protection of a FC1 safety function, this meets my expectations for ECS.1 and ECS.2.

160. Whilst this fault can be initiated in POS A or B, the RP simply states that POS A is more limiting because it is initiated from a higher power. The explanation for choosing POS A is limited; however, in my opinion, faults initiated from full power, where pressure and temperature are high and where the reduction in heat removal will be most significant are likely the most limiting. I am therefore satisfied that the RP's approach is aligned with the expectations of SAPs FA.6 (Ref. 2).

161. The analysis has been performed using the GINKGO and LINDEN codes. My presentation of the V&V of these codes is presented in Appendix 1. This approach is consistent with other intact circuit faults and I judge that these codes are appropriate for analysis of the closure of one or all MSIVs.

162. The RP has analysed two cases:

- Case 1: All MSIVs close simultaneously during full power operations
- Case 2: One MSIV closes during full power operations

163. The RP has grouped these as one DBC. Whilst the closure of all MSIVs may have a much lower frequency than inadvertent closure of one MSIV, the progression of both cases is similar and the faults are generally terminated by tripping the reactor and restoring heat removal through the VDA [ASDS]. I am therefore satisfied with the grouping of these accidents.

* *affected SG means the SG in the train in which the fault occurs.*

164. The VDA [ASDS] provides the primary means of heat removal during this accident. As the signal to actuate the VDA [ASDS] is the SG pressure high 1 signal, the RP has chosen one channel of this signal as the single failure. This single failure does not affect the progression of the fault sequence and the RP has not demonstrated that this is the most limiting single failure. However, in my opinion, choosing another single failure is unlikely to have a significant impact on the progression of the accident as the FC1 systems are single failure tolerant and other passive means of heat removal (e.g. PSVs, MSSVs) would be available. Moreover, whilst not identified as a single failure the RP has also assumed that the RCCA with the highest worth is stuck out of the core. This has an impact on the negative reactivity added to the core and should have a significant bearing on the DNB analysis. I am, therefore, satisfied with the RP's application of the single failure criterion and I am satisfied that my expectations for FA.6 have been met.

165. The RP claims that the following conservative assumptions have been made in order to penalise the DNBR:

- The initial power is the full power plus uncertainty.
- The initial coolant temperature is the nominal value plus uncertainty.
- The initial pressuriser pressure is the nominal value minus uncertainty.
- The initial flowrate is the thermal design flowrate, considering that 10% of the SG tubes are plugged.
- The moderator temperature coefficient is assumed to be the minimum absolute value.
- The Doppler power coefficient is assumed to be the maximum absolute value.
- The most conservative negative reactivity insertion on curve as a function of time is used.
- A conservative axial power distribution, radial power distribution and conservative hot channel enthalpy rise factor is adopted in the DNB analysis.
- A consequential loss of off-site power is assumed.
- The trip signals and delays are set to maximum or minimum values to penalise the plant response.

166. I am satisfied that the assumptions related to initial thermal hydraulic conditions will result in the most penalising conditions for DNB. The selection of a minimum moderator temperature coefficient, and maximum doppler coefficient maximise the core power as the temperature of the primary coolant and fuel increase and I judge that this is a conservative assumption.

167. The application of the consequential LOOP has several effects:

- It delays the start-up of the ASG [EFWS] by [redacted] seconds. However, as the DNBR is lowest in both cases at around 12 seconds, the availability of ASG [EFWS] has no effect on the most challenging time of the transient.
- It leads to loss of RCPs, normal feedwater pumps and condensate pumps which impairs heat removal.

168. The detailed assessment of the generic assumptions related to core neutronics are within the scope of the Fuel and Core assessment (Ref. 20). However, I note that the approach of using values based on the worst location in core as an input in the sub-channel analysis is consistent with that of other accidents.

169. With the above in mind, I am satisfied that the RP has used conservative assumptions in the analyses of both cases, and therefore meets my expectations for SAP FA.7.

170. In both cases, the results show that the minimum DNBR occurs around 1 second after RCCAs begin to insert. After this point, the minimum DNBR increases slightly as the

RCCAs continue to insert. A slight reduction in DNBR is observed as the RCPs and FW pumps begin to coast down. However, the DNBR increases sharply as power reduces rapidly and the primary circuit is cooled by the opening of the VDA [ASDS]. Counterintuitively, the closure of one MSIV results in a slightly lower DNBR ([redacted]) than the closure of all MSIVs ([redacted]), i.e. Case 2 is more challenging. Whilst not explained by the RP, it is likely that the reason is related to the fact that the pressure remains much higher in Case 1 than Case 2 throughout the most challenging part of the transient, by around 7 bar. Nevertheless, the difference in DNBR is negligible.

171. Another consequence of the difference in pressure is that in Case 1 the PSV setpoint is reached, whereas in Case 2 the pressure remains below the lowest setpoint of the PSVs. The potential for a stuck open PSV and consequential LOCA is discussed in Section 4.3.6.1. The opening of the PSV in Case 1 returns the pressure to below the setpoint, and the thermal hydraulics behaviour of the two accidents is similar from closure of the PSV onwards.

172. In addition to DNBR, the RP has also identified PCT and fuel temperature as acceptance criteria. However, the maximum values of these are not reported in Ref. 44. Whilst these values are not provided the RP has stated that the criteria are not challenged. I agree that the accident should not lead to challenging fuel and cladding temperatures because the power does not increase throughout the accident. I am satisfied that the most limiting criterion is the DNBR criterion applied; therefore I have chosen not to pursue this further.

173. Ref. 44 claims that the long-term analysis of the fault is bounded by other faults, and provided bounding arguments for reactivity, confinement and heat removal. As the accident results in a temperature and pressure excursion the most important argument relates to the heat removal. The RP claims that a large feedwater line break is bounding as that accident leads to the loss of two trains of ASG [EFWS] (consequential failure plus single failure), whereas only one train of ASG [EFWS] would be lost in the long-term analysis of closure of the MSIVs (single failure). I am satisfied with the arguments provided.

174. The RP has also presented separate analysis of this fault using GINKGO with parameters chosen to penalise primary circuit overpressure (Ref. 45). Within Ref. 45 the maximum pressure remains below the maximum integrity criteria, for cases with all PSVs available and also assuming that the first PSV fails to lift.

175. With the above in mind, I am satisfied that the RP has adequately demonstrated that safety criteria are met and therefore demonstrated that no damage to containment barriers will occur during this accident. The RP has therefore met my expectations for SAP FA.7. Moreover, the RP has demonstrated that the systems are capable of bringing the plant to a safe, stable state, meeting my expectations for FA.8.

Radiological Consequences

176. Given that the acceptance criteria are met and there is no fuel damage the RP has not undertaken any specific radiological consequence assessment of this fault. Instead the RP argue that the consequences can be represented by a turbine trip because it is an intact circuit fault without fuel damage or pressurisation of the containment. I am content that this is appropriate and that the consequences of this fault are acceptable (the radiological consequences are further discussed in Section 4.7).

Diverse Protection

177. The RP has identified closure of one or all MSIVs as a frequent fault. Therefore, the RP has identified means of providing diverse protection in the fault schedule (Ref. 10).

To demonstrate the adequacy of those diverse safety measures, the RP has chosen the most limiting faults which can bound all loss of heat removal faults (Ref. 34). For each fault, the RP considers each safety function in turn and a bounding sequence is identified. The RP has determined that closure of the MSIVs is not the limiting fault for reactivity and heat removal safety functions. My assessment of this claim is presented below.

178. For reactivity safety functions the RP claims that mechanical failure to insert rods is the limiting failure. The RP claims that diverse protection is provided via the RBS [EBS], which is automatically actuated by the Anticipated Transient Without Scram (ATWS) signal. This signal is generated following a reactor trip without confirmation that the RCCAs have been fully inserted. Mechanical failure to insert rods results in a longer delay to insert negative reactivity than any other failure (e.g. failure of C&I signals to initiate reactor trip), and therefore I judge that the RP's reasoning is sensible.

179. The RP has identified loss of normal feedwater flow (LOFW) and medium-term LOOP with mechanical failure to insert the RCCAs as the bounding cases. The reasons provided relate to timing of RCP trip, availability of feedwater and timing of reactor trip. The RP has provided limited detail, and the bounding case it has selected has a significantly larger DNBR ([redacted]) than the closure of MSIV faults ([redacted]). However, I judge that the most challenging time of the closure of one or more MSIVs fault would not be significantly impacted by mechanical failure to insert rods, as the reduction in DNBR is halted by negative reactivity feedback, rather than RCCA insertion. I am therefore satisfied that a demonstration of diverse protection for the LOFW and LOOP demonstrates that diverse protection can be provided for the inadvertent closure of MSIV faults.

180. For heat removal safety functions, the RP claims that a CCF of the ASG [EFWS] is the most limiting failure (Ref. 34) and that the bleed and feed function (using the PSVs and RIS [SIS]) will deliver the safety functions. The RP has chosen to analyse the LOFW fault with CCF of ASG [EFWS] as the bounding sequence for increase in primary side temperature faults, rather than closure of one or all MSIVs with CCF of the ASG [EFWS]. As the most limiting time of the closure of MSIVs fault occurs prior to the initiation of the ASG [EFWS], I am content that loss of the ASG [EFWS] would not affect the short-term transient. I am therefore satisfied with the RP's arguments that a demonstration of the effectiveness of bleed and feed for the sequence relating to LOFW or LOOP with CCF of the ASG [EFWS] also demonstrates that it can protect against closure of one or all MSIVs with CCF of the ASG [EFWS], meeting my expectations for EDR.3 and FA.5. My assessment of the RP's analysis of the bleed and feed function is presented in Section 4.4.

181. For the confinement safety function, the RP has identified inadvertent closure of all MSIVs as the bounding case with failure of the PSV's to lift. I am satisfied that the arguments provided are sensible. This has been analysed within Ref. 47 which demonstrates that the secondary side relief valves are sufficient to keep the primary pressure below the integrity criteria.

182. I am therefore satisfied that the RP has identified adequate diverse protection to deliver the safety functions and provided sufficient analysis of these, consistent with the expectations of NS-TAST-GD-006 (Ref. 4).

4.3.1.2 Large Feedwater System Break Including Breaks in Connecting Lines to SG

183. The RP has split the analysis of the FLB into two parts. One analysis from the initiating event to a controlled state, and one analysis from the controlled state to a safe state. Both sets of analyses are presented in Ref. 47. I have therefore separated my assessment of the two analyses in the following sections.

From Initiating Event to Controlled State

184. The large FLB can only impact plant safety whilst feedwater is being fed to the SGs (POS A and B).

185. Breaks in the SG feedwater system or connecting pipes have the potential to result in loss of feed to an SG and loss of inventory from an SG. The size of the break determines how much of the coolant is in the liquid / steam phase. There can therefore be two competing effects: the loss of feedwater leads to loss of heat removal, but the loss of inventory can lead to over cooling of the primary circuit. A feedwater line break can therefore lead to an overcooling of the primary circuit and/or an increase in temperature of the primary circuit, depending on the break size. The overcooling effect of a feedwater line break, however, is bounded by steam line breaks where only saturated steam is considered to leak from the break. The RP has chosen, therefore, to simplify the feedwater line break and assume that only loss of heat removal occurs. This is common when performing analysis of feedwater line breaks and I am content with this approach.

186. The break is assumed to occur between the SG and a non-return valve on the feedwater line, resulting in an unisolable loss of SG inventory. When break occurs, normal feedwater is lost through the break. At the same time, the pressure differential between the steam side and the break is established. This results in a reversal of steam flow from the unaffected SGs to the affected SG via the common steam header and the SG is blowndown. The sub-cooled feedwater to all SG is assumed to be lost through the break, resulting in both a raise in temperature of the secondary side and a gradual reduction in inventory to all SG's. The loss of heat removal results in a gradual increase in average temperature of the coolant (i.e. the bulk temperature), potentially challenging fuel integrity criteria.

187. The controlled state is reached by reactor trip, heat removal via the ASG [EFWS] and VDA [ASDS], MSIV closure to isolate the SG and the PSVs to prevent overpressure of the RCP [RCS]. Other than the PSVs, these systems are actuated by the RPS [PS] upon receiving the SG level (narrow range) low 1, SG level (wide range) low 2, SG pressure low 1, and SG pressure high 1 signals. The PSVs are opened passively once the RCP [RCS] pressure reaches the set-point. The signals, C&I system and the safety systems all perform FC1 safety functions and are FSC-1 SSCs. This categorisation of safety functions and SSCs is consistent with the expectations of SAPs ECS.1, ECS.2 and NS-TAST-GD-094 (Ref. 4).

188. Whilst the fault can be initiated in POS B, the RP claims that the most challenging scenario occurs in POS A as the initial power is higher and the initial SG level is lower than in POS B. In my opinion the lower initial temperature, lower heat input (lower decay heat) and larger initial heat sink (due to the larger initial SG inventory) associated with POS B will lead to a smaller rise in temperature and therefore a larger margin to bulk boiling than in POS A. I therefore consider that the RP's argument for only performing analysis of the full power state is reasonable.

189. Compared to the faults involving inadvertent closure of the MSIVs, the large FLB results in a relatively slow increase in the primary circuit bulk temperature. The reactor trip occurs whilst the conditions are not challenging. This is because reactor trip occurs on the SG level (narrow range) low 1 signal for the affected SG, whilst the other SG's still have sufficient inventory for heat removal. Because of this the heat flux is relatively low before the primary circuit temperature rises and margin to DNB is large. Therefore, the most challenging phenomena is bulk boiling of the primary coolant. The RP has therefore used the margin to saturation temperature as the success criterion (bulk boiling leads to dry-out). As the bulk temperature of the primary circuit is the limiting

factor (rather than the heat flux), the heat input from the RCPs has a significant effect on the progression of the accident. The RP has therefore analysed two cases:

- Case 1a: Initiating event to the controlled state (no LOOP, RCPs run on)
- Case 1b: Initiating event to the controlled state (with LOOP and RCP trip)

190. The RP explains that there is a competing effect between the heat input from the RCPs when LOOP does not occur, and the reduction in heat removal from the SGs due to the coast down in flow when LOOP does occur. This sensitivity study is commonly performed for FLB accident analysis and meets my expectations for FA.6 regarding consequential failures and FA.7 for applying conservatism in the analysis.

191. The RP has applied the following initial conditions and conservatisms in its analysis:

- The initial power is the full power plus 2% uncertainty.
- The initial coolant temperature is nominal value plus 2.5 °C uncertainty.
- The initial pressuriser pressure is nominal value plus 0.25 MPa uncertainty.
- The initial pressuriser level is nominal value plus 7% uncertainty.
- The initial SG water level is nominal level minus 10% uncertainty.
- The trip signals and delays are set to maximum or minimum values to penalise the plant response.
- Minimum capacity of safety systems (e.g. minimum flow rate of ASG [EFWS]).
- All main feedwater is lost at the beginning of the transient.

192. Whilst not listed as a conservatism, the analysis only considers the heating effects of the large FLB. This is a conservatism as only water is lost through the break to maximise the loss of inventory and is a similar methodology applied in previous GDAs.

193. As stated, the RP has selected the largest initial pressure. Whilst selection of the largest initial pressure will have the effect of increasing the initial saturation temperature, it will also cause the PRV set point to be reached earlier, reducing the saturation temperature. Whilst justification is not provided, I judge that the impact of this will likely only impact the timing of the most limiting point of the transient. The other conservatisms applied clearly penalise the transient, and I am satisfied that the RP has applied appropriate conservatisms meeting my expectations for FA.7.

194. The RP has chosen one unaffected train of ASG [EFWS] as the single failure assumed within the analysis. After dryout of the associated SG, this reduces the heat removal capacity down to one SG. I judge the single failure applied to an SG is appropriate. I judge that the choice of applying the single failure to the feedwater system (ASG [EFWS]) over the steam release system (VDA [ASDS]) is appropriate as it totally inhibits heat removal from the SG. I therefore consider the application of the single failure criterion appropriate and meets my expectations for FA.6.

195. Whilst not explained in detail, the RP's analysis shows that after the initial drop in temperature due to the reactor trip, the temperature gradually rises as heat removal from a single SG (and heat losses) is less than the heat input from the decay heat (and other heat sources). Because of this, the PSVs periodically lift until the close set-point is reached. This causes a saw-tooth like curve in saturation temperature, dropping every time the PSVs open. The pressuriser level gradually increases as the average primary circuit temperature increases and there is potential for the RCP [RCS] going water solid. Eventually, as decay heat decreases and the SG level of the one remaining SG is restored by the ASG [EFWS], a balance between heat input and output converges and the average coolant temperature and pressuriser level starts to plateau. Filling of the pressuriser (i.e. going water solid) would lead to a loss of control of the confinement safety function. I judge, therefore, that the analysis demonstrates

that control of the safety functions has been regained through the automated safety systems.

196. The analyses show that the minimum margin to saturation temperature for Case 1a and 1b is calculated as [redacted] °C and [redacted] °C, respectively, and that the core is not uncovered as a result of repeated opening of the PSVs. For comparison, during normal operation, the margin to saturation is approximately [redacted] °C. The analysis demonstrates that margin to saturation are not significantly lower than those in full power and are mainly dependent on the reset setpoint of the PSV. Ultimately, I judge that the analyses demonstrate that the fuel integrity criteria should not be challenged during a large FLB, meeting my expectations for FA.7.

From the Controlled State to the Safe State

197. Whilst the short-term analyses are performed to demonstrate that fuel criteria are met, the RP presents long term analyses to demonstrate that sufficient capacity is available to bring the plant to a safe state in which longer term control of the safety functions can be secured.

198. The RP has performed analyses of two cases:

- Case 2a: initiating event to safe state (no LOOP, RCPs run on)
- Case 2b: initiating event to safe state (with LOOP and RCP trip)

199. The reasons for analysing these are similar to those set out for the short-term analysis and relates to heat balances and rate of consumption of initial SG and ASG [EFWS] tank inventory. The initial conditions are mainly the same as those presented above and are chosen to maximise the energy in the primary circuit. The more energy in the primary circuit, the more ASG [EFWS] feedwater is used up to remove that energy.

200. The single failure is chosen as:

- Case 2a: one train of RBS [EBS] – this reduces the allowable cooldown rate, prolonging the time RCPs run for and allowing more heat to be added by the running RCPs, consuming more secondary coolant.
- Case 2b: one EDG in the unaffected train – the loss of the heat removal capacity of a second SG prolongs the cooldown process and consumes more ASG [EFWS] feedwater.

201. In the long term, two SG's are required to bring the plant to a safe state. In Case 2b, the unaffected train has failed due to the failure to start the EDG. Operator action to cross connect the affected train with the unaffected SG is required. The difference between the single failure for case 1b (short-term – loss of ASG [EFWS]) and case 2b (long-term – loss of EDG) is not explained. However, it is likely that the failure of the EDG, as opposed to the ASG [EFWS], leads to pressure losses whilst cross connected (this is not important for the short-term analysis).

202. As stated previously, the RP states that the ASG [EFWS] is sized based on the FLB accident. This is because the FLB leads to both a loss of inventory of the ASG [EFWS] tanks and a total loss of feedwater. The total capacity of the ASG [EFWS] tanks is [redacted] tonnes. In case 2a and 2b, the RP demonstrate that only [redacted] tonnes and [redacted] tonnes of water is used to reach the safe state, respectively. Therefore, the analysis demonstrates that the capacity of the ASG [EFWS] is sufficient to bring the most limiting cases to the safe state. This meets my expectations for FA.8 and FA.9 for a demonstration of the adequacy of safety measures. Moreover, the analysis demonstrates that only two tanks of ASG [EFWS] are required to reach a safe state.

This demonstrates that a passive failure of the ASG [EFWS] pipework or tank would also be tolerable.

203. A large feedwater piping break is also the limiting fault for the primary side overpressure and additional analysis, to penalise overpressure, is presented in Ref 48. This analysis, conducted using LOCUST and assuming a single failure of one PSV, shows that operation of the PSVs limits the maximum pressure to below the 130% of the Design Pressure (as set by the RCCM methodology). I am content that this analysis demonstrates that the overpressure resulting from this fault is acceptable and satisfies the expectation of FA.7.

Radiological Consequences

204. As the decoupled criteria are met, there is no fuel damage and hence any radiological consequences will be limited to leakage of primary coolant through containment due to pressurisation of the containment. The RP states that the radiological consequences of a feedwater piping break are bounded by the main steam line break (SLB). The reasons for this are not provided within Ref. 47. In response to RQ-UKHPR1000-0244 (Ref. 6), the RP states that the containment overpressure transient of the FLB is bounded by the SLB as the SLB releases significantly higher energy. I judge that the RP's arguments are sensible, and that the radiological consequences of the FLB will be bounded by the SLB.

4.3.1.3 Loss of Off-site Power

205. A LOOP can be caused by a complete loss of external grid, a fault with the power distribution system failure and an external grid disturbance. There are three EDGs which each supply electrical power to corresponding trains of safety systems, including ASG [EFWS] and RIS [SIS], along with RRI [CCWS] and SEC [ESWS]. Each EDG has sufficient fuel to last for 7 days.

206. The RP has identified three LOOP accidents which vary in both frequency and length. The RP has identified a short term (2 hours) and medium term (24 hours) LOOP as a frequent design basis fault and long term (168 hours) LOOP as an infrequent design basis fault.

207. The RP's analyses have two different purposes. The short term analysis is aimed at demonstrating that a controlled state is reached and that the fuel integrity criteria are met, whereas the medium term analysis aims to demonstrate that subcriticality is maintained and that safe state can be reached before the ASG [EFWS] tanks are exhausted. For the long term LOOP, the RP has not performed analysis and instead simply argued that sufficient fuel oil and water is available to maintain heat removal through RHR.

208. A LOOP results in a loss of heat removal and a coast down of the RCPs. Upon receiving a LOOP signal all three EDGs start after a short time delay (around 50 seconds). A coast down of the RCPs results in a reactor trip and a subsequent turbine trip. Protection is initially provided by reactor trip and the automatic opening of the battery powered VDA [ASDS]. Once the SG level low 2 level is reached the ASG [EFWS] starts and the plant is brought to a controlled state.

209. All of the associated C&I, sensors and safety measures are assigned F-SC1. As they are the primary means of providing Category 1 safety functions, I judge that this meets my expectations for ECS.1 and ECS.2.

210. Since the short term and medium-term LOOPs are identified as a frequent fault the RP has identified diverse protection for these faults. The F-SC2 SBO diesel generators

provide backup power to safety measures in the event of CCF of the EDGs. My analysis of the SBO fault is presented in sub-section 4.4.1.3.

211. In the following sections I present my assessment of the RP's safety case for short term, medium term and long-term LOOP. My assessment of short- and medium-term LOOPs examines the analyses provided by the RP, whereas my assessment of the long term LOOP considers the available fuel stocks.

Short Term LOOP

212. The RP identifies the short-term LOOP as a DBC-2 fault. The RP's transient analysis for a LOOP from the initiating event to the controlled state is presented in Ref. 49. The analysis from the controlled state to the safe state, is presented in Ref. 50 (see below section).

213. The RP has only performed analysis of the full power case. This is because the power is high and is most limiting for the fuel integrity criteria. I judge that this is sensible as low power cases would progress in a similar way and that for states in which the RHR is connected the controlled state is reached as soon as RHR is powered back up by the EDGs. The single failure is applied to one EDG, resulting in a loss of one train of RBS [EBS], loss of all feed to one SG and loss of one train of RIS [SIS].

214. The RP's analysis demonstrates that following the initial loss of power the RCPs begin to coast down and reactor trip occurs. During this time the DNBR slightly decreases and rises significantly after the rods are fully inserted. The minimum DNBR remains above the criteria.

215. I am content to judge that the RP has applied conservative assumptions, considered all configurations and used the most limiting case, and the appropriate single failure, therefore meeting my expectations for FA.6 and FA.7.

Medium Term LOOP

216. The RP has identified the medium term LOOP (up to 24 hours) as a DBC-3 fault (Ref. 50). The aim of the analysis is to demonstrate that the conditions required for RHR connection can be met before the ASG [EFWS] tanks are depleted and that sub-criticality is maintained throughout.

217. The RP has performed analysis from full power and in several configurations during cold shutdown modes when RHR is in service. For shutdown modes, the RP has used the most penalising temperatures, pressures and decay heat. As with the short term LOOP, the RP has applied the single failure to one EDG. I judge that the RP has adequately considered the worst permissible configurations and has appropriately applied the single failure criterion, meeting my expectations for FA.6.

218. The RP states that reinstating RHR provides the protection against LOOP during RHR modes. The RP states that RHR is the means of bringing the initiating event to the controlled state. The RP states that RHR is automatically reinstated when the EDGs are started up. The RP's analysis demonstrates large margin to saturation and that the water level remains above the top of the fuel. Whilst RHR is F-SC2, I note that the conditions for the safe state are maintained throughout the analysis. I am therefore satisfied that the RP's analysis demonstrates that for shutdown states the safe state is reached, meeting my expectations for FA.8.

219. For the full power case, Ref. 50 demonstrates that sufficient cooling is initially provided by the two trains of VDA [ASDS]. The SG level drops as steam is lost through the VDA [ASDS] and the SG level 2 signal is generated, actuating the ASG [EFWS]. Following

this, the manual operation of the RBS [EBS], ASG [EFWS] and VDA [ASDS] result in the conditions for connection of RHR being met at [redacted] hours. Once the RHR conditions are met the RP claims that power provided by the EDGs is sufficient to maintain RHR in the long term. The RP reports that [redacted] tonnes of [redacted] tonnes of feedwater are used during the cooldown period. This is consistent with the RP's claim that the accident is less onerous than the feedwater line break. I am content with the RP's analysis and claims that sufficient time, water and power is available to bring the plant to a safe state, meeting my expectations for FA.8.

Long Term LOOP

220. Since the Fukushima Daiichi accident, there has been growing emphasis on reactor plants self-sufficiency and reducing dependency of off-site power and supplies. ONR's Chief Nuclear Inspector's report on the lessons learnt from Fukushima (Ref. 51) made recommendations that a robust, on-site, diverse means (i.e. not grid) for providing power and water supplies should be implemented. The report also recommended that licensees work with National Grid to determine the potential severity and frequency of loss of offsite power events.

221. The RP identifies a long-term LOOP (168 hours) as a DBC-4 fault, which is an infrequent fault. The length of the long-term station black out varies on geographical location. For the UK fleet, it is currently generally expected that a LOOP of five days should be considered as a frequent fault. The frequency of such events will be determined by the licensee; however, it should be noted that whether the RP consider the long-term LOOP as a frequent or infrequent fault will likely have limited impact on the design (see sub-section 4.4.1.3).

222. The RP has not explicitly analysed the long-term LOOP (168 hours). This is because the RP claim that the medium-term analysis demonstrates that the RHR connection requirements are met and that RHR continuously removes heat from this point. I judge that this is a sensible claim. The focus of my assessment has been on whether sufficient provisions are available to reduce dependency on off-site provisions. In coming to this judgement, I have considered the capacity of other new reactors and available RGP. The European Utility Requirements state that on-site provisions should be available to ensure heat removal and power is supplied for at least seven days. I have used this as a benchmark for my expectations.

223. Ref. 50 argues fuel oil is the limiting factor for maintaining heat removal during a LOOP. The RP states that sufficient water is available to provide cooling by the normal cooling chain (RRI [CCWS]), and that the components can provide safety functions for several weeks following a LOOP. When fuel oil for the EDGs is depleted after 7 days the RRI [CCWS] is no longer available. At this point, the RP claim that further heat removal can be performed via the ECS [ECS], which can be powered by the SBO generators. These are also limited by the available fuel oil, which lasts for a further three days.

224. The RP has provided a summary of the rated power consumption and available fuel oil for the EDGs (Ref. 50). The RP has also provided a comparison of the rated power and expected power consumption against the expected power and expected power consumption. The RP claims that for a Large Break LOCA (LB-LOCA) with loss of offsite power and coincident fire, using summer conditions, that the maximum fuel oil consumption rate and required power is less than the design specification. In this low frequency condition, the RP states that the Divisions A, B and C would provide power for [redacted], [redacted] and [redacted] days, respectively. In the less severe scenario where no LB-LOCA is assumed, the equivalent mission times are [redacted], [redacted] and [redacted] days, respectively.

225. As the RP claims that the SBO generators can support heat removal via the ECS [ECS] for three additional days, the RP concludes that using more realistic fuel oil consumptions and required power levels, that the safe state could be maintained for [redacted] days for non-LOCA conditions.

226. The SBO generators are not capable of providing power to the normal cooling chain RRI [CCWS] (and SEC [ESWS]). Whilst not explained by the RP, I therefore assume that in scenarios where the RCP [RCS] was closed and pressurisable heat removal would be performed via the VDA [ASDS] and ASG [EFWS]. However, I note that there are multiple ways in which cooling could be provided and that this is the choice for the licensee once the detailed emergency operating procedures are compiled. I am content that the development of this aspect of the safety case will be progressed as normal business.

227. Regardless of the lack of detail in the RP's claims regarding the SBO generators, the RP has nevertheless demonstrated that the EDGs enable heat removal via RHR for longer than a week. This is comparable with other new reactors, longer than the capability of the UK's existing fleet, and is aligned with the EURs, which the RP has used as a benchmark of good practice. I am therefore content that the generic UK HPR1000 design meets RGP for self-sufficiency in terms of power supply.

4.3.2 Decrease in Primary Side Temperature Faults

228. The RP has identified the following decrease in primary side temperature faults:

- Excessive increase in secondary steam flow.
- Inadvertent opening of one SG relief train or of one safety valve.
- Increase in feedwater flow due to feedwater system malfunctions.
- Steam system piping small break including breaks in connecting lines.
- Reduction in feedwater temperature due to feedwater system malfunctions.
- Large steam system piping break.

229. The above faults range from DBC-2 to DBC-4 faults. I have chosen to sample the above accidents to gain confidence that the RP has demonstrated that the generic UK HPR1000 design is tolerant to decrease in primary side temperature faults. My reasoning for sampling is presented below.

230. Of the above, the 'large steam system piping break' (referred to as large SLB herein) and 'reduction in feedwater temperature due to feedwater system malfunction' are identified as infrequent faults. I have chosen to sample the large SLB as it is the most challenging in terms of margin to fuel failure (DNB).

231. Out of the frequent faults, only the increase in feedwater flow fault results in reactor trip. The other frequent faults result in a small increase in reactor power until a new steady state is reached. I have therefore chosen to sample the increase in feedwater flow fault.

232. No transient analysis has been presented for the demonstration of diverse protection for frequent faults. This is because the RP claims that the other accidents bound the increase in heat removal faults. I have therefore considered the diverse protection demonstration based on the information provided in the fault schedule. My assessment of diverse protection for these frequent faults is therefore presented against all increase in heat removal faults, in a separate sub-section.

233. It should be noted that the RP has designated the main steam line as a High Integrity Component (HIC) within the reactor building and safeguard building. Although the pipes downstream of the safeguard building are not designated HIC, breaks of these

pipes lead to less severe cooldown accidents because of frictional losses along the pipe and because all three SGs can be isolated. However, it is a common design basis assumption to consider the break as unisolable, occurring within the reactor building, so that at least one SG fully blows down (empties) into the containment, which sets design limits on the containment. Given the HIC classification, the RP considers that the large SLB as a specific case outside of the design basis but it has been analysed as a DBC-4 fault. I note that this position aligns with the European Utilities Requirements (Ref. 52) and I consider it to be a satisfactory approach.

234. In addition to the analysis of the large SLB considered in the DBC analysis, the RP also performed analysis of a SLB within the safeguard building to support its structural integrity classification assessment. I have also included my assessment of this aspect below.

235. In the following sub-sections, I present my assessment of the analysis presented to demonstrate the UK HPR1000 is tolerant against increase in feedwater flow and large SLB accidents. In addition, I present my assessment of the diverse protection provided for frequent faults.

4.3.2.1 Increase in Feedwater Flow due to Feedwater System Malfunctions

236. The RP has performed transient analysis of increase in feedwater flow faults from the initiating event to the controlled state. The transient analysis is presented in Ref. 53.

237. An increase in feedwater flow fault can be initiated by increase in pump speed of the motor-driven feedwater pumps system (APA [MFPS]) or the start-up and shutdown feedwater system (AAD [SSFS]), loss of control of the valves within the main feedwater flow control system (ARE [MFFCS]), or spurious initiation of ASG [EFWS]. In POS C - F the full load isolation valves (FLIV) and low load isolation valves (LLIV) are closed. Therefore, the accident can only occur in POS A and B.

238. An increase in feedwater flow results in an increase in inventory of the SG which cools the primary circuit. At full power, moderator feedback causes an addition of reactivity and the core power to increase. At hot zero power, the accident has the potential to result in criticality. In both cases there is potential for the heat flux, fuel temperature and cladding temperature to increase rapidly. The fuel integrity criteria can therefore be challenged.

239. Protection is mainly provided by the reactor trip and closure of the FLIV. Closure of the FLIV is actuated if SG level (narrow range) high 1 or the reactor trip signal is reached. Closure of the LLIV is actuated if the SG level (narrow range) high 0 signal is received in coincidence with the reactor trip signal and sustained for 10 seconds. These safety systems provide the primary means of protection to the controlled state. All of the safety functions are identified as Category 1, and the SSCs that deliver the safety functions are F-SC1. This meets my expectations for ECS.1 and ECS.2.

240. The analysis is performed for full power states and from hot zero power, both of which are covered by POS A. The RP states that full power envelopes any at power faults (0-100 %FP) because the plant response is similar and the temperature and core power are higher (making DNBR smaller). In addition, the plant response from hot zero power is similar to that in POS B, and more limiting because the shutdown margin is smaller and the initial temperature is higher (allowing for potentially larger temperature drop and more reactivity to be added). The RP's arguments appear reasonable and aligns with my expectations for FA.6 in that the worst possible plant operating state has been chosen as an initial condition.

241. The RP has used the GINKGO code to analyse the system transient. My assessment of the V&V of this code is presented in Appendix 1. The RP has used the LINDEN code to analyse cases in which the DNB criteria may be challenged (i.e. the full power cases). The V&V of the LINDEN code is discussed in ONR's Fuel & Core assessment report (Ref. 20). I am satisfied that the increase in feedwater flow does not require detailed two-phase modelling to understand the system response and that the GINKGO code is appropriate for analysing the system response. I am also content that the LINDEN code can be used appropriately with the output of the thermal hydraulics response from GINKGO. Therefore, I judge that the use of both GINKGO and LINDEN is appropriate for this analysis.

242. The RP has combined differing causes for increase in feedwater flow. However, the main cause is a sudden opening of the Full Load Control Valve (FLCV) to its maximum position. The RP has analysed four cases:

- Case 1: full power; one ARE [MFFCS] train fully opens; three trains of APA [MFPS] at full speed; one ASG [EFWS] spuriously actuates.
- Case 2: full power; three ARE [MFFCS] train fully opens; three trains of APA [MFPS] at full speed; three ASG [EFWS] spuriously actuates.
- Case 3: hot zero power, one ARE [MFFCS] train fully opens; three trains of APA [MFPS] at full speed; one ASG [EFWS] spuriously actuates.
- Case 4: hot zero power; three ARE [MFFCS] train fully opens; three trains of APA [MFPS] at full speed; three ASG [EFWS] spuriously actuates.

243. No explanation as to why these cases have been chosen has been provided. However, it can be seen that in cases 1 and 3, in which only one SG is affected, the maximum feedwater flow to that SG is significantly larger than to any SG in cases 2 and 4. This is likely because the flow of the three APA [MFPS] trains is divided amongst all three SGs in cases 2 and 4. Therefore, cases 1 and 3 will likely lead to power tilting and possible worse local power peaking. The RP states, however, that cases 2 and 4, in which the core temperature will be uniformly reduced, are the bounding cases for both at power and hot shutdown states. The evidence for this is not provided, but I judge that because the temperature transient of this fault is relatively slow, mixing from the warmer water in the unaffected loops will counteract the larger drop in temperature of the affected loop and lessen the reactivity insertion. I am therefore content that the RP has chosen the most onerous initial conditions for the accident. Only cases 2 and 4 are referred to henceforth. As I consider that this is only a presentational matter in the safety case, I have identified the lack of evidence and reasoning as a minor shortfall.

244. In both cases, there is an initial large step change in flow rate and then the flow rate is further increased, linearly, to the point at which the FLIV closes. Depending on the power of the reactor, whether the plant is being started or shutdown, various pumps and valves are available to limit or finely control the feedwater flow. The different configurations result in varying initial flow rates and varying effects of the isolation of valves. For example, the signal to close the LLIV will not affect feedwater flow if the LLCV is already closed. The RP has not provided the initial configurations of the valves and pumps. Furthermore, no reference is provided for the flow rates of the APA [MFPS], FLIV or LLIV. As a result, the initial conditions and plant response are difficult to understand. I judge, however, based on my wider assessment that the engineering data used in the transient analysis is generally consistent with the requirements in the system design manuals. I therefore only consider this a minor shortfall in the safety case.

245. Instead of providing precise information, the RP provides a description in terms of relative flow which can be used to infer the necessary information. The RP explains that in each case, there is a large step change in feedwater by a factor of [redacted] (case 2)

and [redacted] (case 4). After the sudden increase the feedwater flow is then linearly increased until isolation of the FLIV occurs on SG level high 1 signal. For case 2, when the full load line is closed, the flow rate is significantly reduced and only the flow through the low load line is fed to the SGs. For case 4, after isolation of the full load line the flow reduces to zero, implying that the LLIV is closed from the start of the transient. During hot zero power (as in case 4), the Low Load Control Valve (LLCV) or the FLCV can be used to control the feed flow. Whilst not stated, it is likely that the RP has chosen the FLCV to fully open (instead of the LLCV) as it allows for the greatest step increase in flow. I judge that this is a conservative assumption.

246. The following initial conditions are specific to the full power case:

- The unit is initially operated at 100% full power (FP);
- Initial reactor coolant average temperature is at its nominal value (307 °C);
- Initial pressuriser pressure is at its nominal value (15.5 MPa);

247. The following initial conditions are specific to the hot zero power case:

- The unit is initially operated at hot shutdown state;
- Initial reactor coolant average temperature is at its zero power value minus uncertainty (291.5 °C);
- Initial pressuriser pressure is at its nominal value minus uncertainty (15.25 MPa);

248. The reason for choosing nominal values for the full power case is not provided in Ref. 53 but this is related to the use of the statistical method of DNB analysis. As the uncertainties of power, temperature and pressure are considered in DNBR design limit, I am content with the use of nominal values.

249. The initial conditions and conservatisms common to both analyses are as follows:

- Initial reactor coolant flowrate is equal to the mechanical design flow (26500m^3/h/loop), considering 0% pipe plugging of SGs, so as to increase the heat removal by secondary system.
- The moderator density coefficient is considered as its the maximum value (0.58 Δk/k/(g/cm3)) so as to maximise the increase of nuclear power.
- The Doppler power coefficient is considered as its minimum absolute value so as to maximise the increase of core power.
- The RCCA with the highest worth is assumed to be stuck out of the core to minimise the negative reactivity after the reactor trip. For the full power case, the most conservative negative reactivity insertion curve as a function of time is used.
- Simultaneous spurious actuation of all ASG [EFWS] from the start of the transient.
- Reactor trip is triggered on SG level (narrow range) high 1 signal. The setpoint is assumed to be the rated value minus uncertainties. A conservative delay between setpoint actuation and the beginning of rod drop is considered.

250. Except for the final point, all of the above are self-explanatory, and I am satisfied that the assumptions will lead to a conservative result. The final point related to the SG level high is less obvious, as it initially appears that if the SG level setpoint is reached earlier then the accident will be less penalising. However, it is likely related to competing effects between the rate of change of the feedwater flow rate and the total SG inventory at reactor trip. As such, I am content to judge it will have limited bearing on the transient.

251. The consequential LOOP and subsequent coast down of the RCPs is not applied to either analyses. For the full power case, the RP claims that the core power will be reduced (due to reactor trip) by the time the coast down of the RCPs would present a challenge. For the hot zero power case, the turbine is not in service and therefore the accident will not have any consequences for the grid. I judge that these arguments are appropriate. With this in mind, and the above judgments on the conservatisms included in the analysis, I consider that the expectations of FA.7 have been met.

252. The single failure for the full power case has been chosen by the RP as failure of one of the SG level (narrow range) high 1 signals. This does not affect the transient as there is redundancy in the channels. The single failure for the hot zero power case is one train of MHSI. This is because the MHSI plays a role in arresting the reactivity addition caused by the cooling of the RCP [RCS].

253. There is limited discussion in Ref. 53 for why these are the most limiting single failures. I judge that other failures for example failure to isolate a train of ARE [MFFCS] may lead to a more rapid cooldown and faster return to criticality in the hot zero power case. However, the power excursion in the hot zero power case is limited by the Doppler feedback, and in my opinion it is likely that other candidates for the most limiting single failure would make little impact on the maximum core power reached. For the full power case, the most limiting point during the transient is just before reactor trip After the trip, the DNBR increases significantly, therefore any other single failure would not have a significant impact on the transient. I am therefore satisfied with the application of the single failure criterion and I am satisfied that the expectations for FA.6 have been met.

254. For the full power case, the analysis results show that the minimum DNBR occurs just before reactor trip and as the core power rise is stabilising. Following reactor trip and isolation of the ARE [MFFCS] the decay heat is removed by the inventory of the SG and continued ASG [EFWS]. The temperature and pressures of the primary circuit become stable. The minimum DNBR remains above the criteria. No fuel temperatures are presented, although I judge that the temperature will not be challenging at the maximum powers reached (~[redacted] FP). The analysis therefore demonstrates that no fuel failure is predicted meeting my expectations for FA.7.

255. For the hot zero power case, the analysis demonstrates that the continued cooldown of the plant via the ASG [EFWS] and the large inventory of the SGs causes a return to criticality. The power is limited by the Doppler feedback, and negative reactivity of the MHSI returns the plant temporarily to slightly subcritical. However, criticality is once again reached and the core power levels out at around [redacted] FP. As the RP has not demonstrated that sub-criticality is maintained, the RP has not demonstrated that the controlled state is achieved by the actuation of the automatic systems. It should be noted, however, that the cause of this is the conservative assumption that ASG [EFWS] spuriously actuates at the beginning of the accident. Since an increase in feedwater flow results in a larger SG inventory, it is more realistic that the low SG (wide range) level 2 signal which actuates the ASG [EFWS] would not be reached. This illustrates how the RP's approach to apply pessimistic assumptions to demonstrate that the acceptance criteria are met can mask the realistic plant response.

256. Throughout the transient, the maximum power reached is around [redacted] FP. The RP concludes that this does not challenge the fuel integrity criteria but has not presented any comparisons to fuel integrity criteria. However, based on a comparison with the DNB analysis presented for the main steam line breaks, I judge that the peak power should not challenge the DNB criteria nor the fuel/cladding temperature limits. On this basis, I am content that the RP's analysis is consistent with the expectations for FA.7.

257. With the above in mind the RP has demonstrated that the trip settings of the SG level (narrow range) high 0 signal and the safety measures are suitable to protect against increase in feedwater flow accidents. Moreover, further protection signals are described in the fault schedule. This meets my expectations for FA.8 and FA.9.

Radiological Consequences

258. The RP states that there is no fuel damage predicted during this accident. Therefore, the RP has not undertaken any specific radiological consequence assessment of this fault. Instead the RP argue that the consequences can be represented by a Turbine Trip because this too is an intact circuit fault with no fuel damage and no pressurisation of the containment. I am content that this is appropriate and that the consequences of this fault are acceptable when judged against SAP FA.7.

4.3.2.2 Large Steam System Piping Break

259. A break in the main steam pipework can lead to a large release of energy into the surroundings and cause a severe transient within the reactor. As such it is one of the most onerous faults for the protection systems and for the design of the containment. As stated in the introduction to this section, as well as the analysis of a large SLB within containment (DBC-4 fault) the RP has also analysed a large SLB within the safeguard building (to support the Structural Integrity Classification analysis).

260. I have chosen to target my assessment of the tolerance of the plant to SLB and therefore my assessment of the DBC-4 fault makes up the majority of the following section. However, I have also briefly discussed the consequence analysis that informs the structural integrity classification, which is considered in detail in ONR's Structural Integrity topic assessment (Ref. 32).

Design Basis Condition Analysis

261. The RP performed transient analysis of large SLBs from the initiating event to the controlled state. The transient analysis is presented in Ref. 55. The RP claim that the long-term analysis is bounded by the feedwater line break accident due to the more penalising availability assumptions related to the ASG [EFWS]. I consider the RP's arguments are reasonable.

262. The large SLB is a DBC-4 fault which can be initiated from either POS A or B. For other states the reactor is cooled by the RHR and a SLB does not have any consequences for the core.

263. The large SLB is characterised by a break equal to or larger than 50 mm diameter up to a double ended guillotine break of the main steam system. A break in the steam line or connecting pipework has the potential to decrease the saturation temperature within the SG and reduce the temperature of the secondary coolant. This results in additional heat removal from the primary side. The reduction in temperature increases moderation and can result in reactivity addition and core power increase.

264. During this accident steam from the unaffected SGs leaks through the affected steam line via the common steam header. Therefore, in the early stages of the transient, before isolation of the unaffected SGs from the break, heat removal from all SGs increases and additional reactivity is added to the core. The main protection for this fault is: reactor trip, isolating the source of heat removal (i.e. feed and steam offtake) and MHSI to counteract the negative reactivity added by the break. Reactor trip occurs on pressuriser pressure low 2, pressure drop of SG high 0 or pressure drop of SG high 1 signals. Closure of the FLIV occurs on reactor trip, and the LLIV of the affected SG closes on SG pressure low 2 signal. The LLIV of all SGs is closed if the pressure

drop SG high 2 signal is reached. The MHSI is triggered on the pressuriser pressure low 3 signal. For continued heat removal after reactor trip the ASG [EFWS] is required, which is triggered by the SG level (wide range) low 2 signal. A manual operation to isolate the ASG [EFWS] of the affected SG is required to reach the controlled state. This action prevents heat removal from the affected SG, prevents further pressurisation of the containment, and preserves ASG [EFWS] inventory.

265. All of the above signals, the associated C&I platform, safety measures and the human action identified are designated as F-SC1. Detailed assessment of Class 1 human based safety claims (HBSC) has been carried out by ONR's Human Factors Inspector (Ref. 55). The RP has simply assumed that operator action can only be performed at 30 minutes, which is shorter than the allowable time to perform this action (as shown in the Level 1 PSA, Ref. 82), and significantly longer than the predicted time to perform the action. The RP's approach aligns with the expectations of ESS.8 in that only automatic actions should act within the first 30 minutes of an accident for fast acting faults. With this in mind, I am content that a human action is credited to reach the controlled state. Moreover, since all of the SSCs are F-SC1, I am satisfied that the expectations for ECS.1 and ECS.2 have been met.

266. The analysis has been performed at full power and hot shutdown for similar reasons described in the previous section. I judge that the reasons are applicable here and meet my expectations for FA.6, in that the worst possible initial plant state has been used.

267. The methodology for analyses of the SLB from hot zero power differs slightly from the methodology at full power:

- The analysis at hot zero power has been performed with the GINKGO, COCO and LINDEN codes. The COCO code is a 3D nuclear design code, which can generate core powers and neutronic data over the lifecycle of the plant. The COCO code is used to input neutronic data into the GINKGO calculation and to input core power distribution to the LINDEN calculation. This approach has been taken so that the asymmetric temperature distribution and subsequent power asymmetry can be accounted for in the analysis.
- For analysis of SLBs at full power, the RP has used only GINKGO and LINDEN. This is because the local power peaking is more significant in the hot zero power case where no nuclear heat is being generated, requiring a detailed analysis of the local power increase.

268. The assessment of the V&V of both LINDEN and COCO is presented in ONR's Fuel & Core assessment report (Ref. 20). My assessment of the V&V of the GINKGO code is presented in Appendix 1. I consider that the analysis approach is appropriate.

269. The RP has performed analysis of a spectrum of nine break sizes from 50 mm to full guillotine break for both the full power and hot zero power case. The smallest connecting pipe size is 25 mm diameter, which is covered by the small SLB analysis. I am satisfied that the range of the analyses covers all possible break sizes, and includes some specific connecting pipe diameters (such as the VDA [ASDS] pipeline). Moreover, I am satisfied that the analysis of both the full power case and the hot zero power case covers the bounding cases for different plant responses and is aligned with RGP. This meets my expectations for FA.6.

270. The following initial conditions apply to both the full power and hot zero power cases:

- The initial reactor coolant flowrate is set as the thermal design flow (24000 m^3/h per loop), considering that 0% of the SG tubes are plugged;
- The most worth rod is assumed to be stuck out of the core;

- No heat transfer from the SGs to RCP [RCS] (no heat reversal)
- Critical flow of steam from all SGs through the break until closure of MSIVs, after which, only critical flow from the affected SG;
- Steam quality equal to 1;
- Penalising system and C&I performance, where applicable
- Low doppler feedback coefficient, low boron differential worth, high moderator feedback.
- Penalising core inlet mixing assumptions

271. I judge that most of the above assumptions are both conservative, to such an extent that in some cases it is physically unrealistic for them to occur together. For example, when the RCP [RCS] cools to a temperature below the SGs the heat transfer should reverse from the SG to the RCP [RCS]; however, the RP has not modelled this phenomenon in order to minimise the core inlet temperature and maximise reactivity addition. Another obvious example of an unrealistic and conservative assumption is that the minimum shutdown margin and DNB analysis is based on a rod fully withdrawn from the core, even for the hot zero power case.

272. Whilst not immediately obvious, the core flow rate has two competing effects: a higher flow increases heat transfer to the secondary system and therefore maximises heat reduction caused by the break, but a low flow rate reduces the critical heat flux. I am therefore content that the RP's choice to maximise flow through the SG tubes (0% plugging) but minimise flow through the core is appropriate.

273. The core inlet mixing is an important factor for asymmetric cold water addition accidents. The lower the mixing, the more asymmetric the core temperature distribution will become. The RP has provided results of a test facility in which a [redacted] scale model of the UK HPR1000 was used to derive a mixing matrix. Whilst limited data are provided, the RP does include empirically derived values of the mixing ratios and provides a comparison to the values used in the analysis. In comparison to other transient analyses that I am aware of, and a comparison to experimental values, the mixing ratios used in the analysis do appear to be conservative.

274. In terms of the neutronics and physics assumptions, ONR's Fuel and Core inspector has confirmed that the assumptions are conservatively applied, and that the RP makes unrealistic combinations to penalise the results for DNB. This approach has resulted in two sets of hot zero power analyses: one with a very conservative core power defect (case A) which is lower than any power defected predicted for all cycles, and one set with a less conservative core power defect (case B), but which is still bounding of all of the cases analysed. In either case, the core power defect is less than the realistic value expected. I judge that the RP's approach is reasonable as the power defects used are bounding of all of the cycles they are applied to.

275. For the pressure, temperature and core power, I am satisfied that the RP has chosen appropriate values to penalise the transient. Specific to the full power case, the RP has applied the most penalising reactor trip reactivity insertion curve, which is clearly penalising. Specific to the hot zero power case, the RP has chosen to maximise overcooling by assuming that the ASG [EFWS] starts up at the beginning of the transient and I am satisfied that this is also conservative.

276. With the above in mind, I am satisfied that the combination of the conservative assumptions leads to a very conservative analysis, and therefore meets my expectations for compliance with the expectations of FA.7.

277. Regarding consequential failures, the RP states that the assumption of consequential LOOP is not appropriate for the hot zero power case. This is because a LOOP would cause the RCPs to trip and would reduce the rate of cold-water addition to the core.

For the full power case, a consequential LOOP has no bearing on the most challenging time of the transient and is not applied. In response to RQ-UKHPR1000-0392 (Ref. 6), the RP explains that although a consequential LOOP may affect the time at which MHSI is started, the coast down of the RCPs means that a consequential LOOP would not result in a challenging situation in the first place. I judge that the RP's reasoning is sensible and meets my expectations for FA.6.

278. For the hot zero power case, the RP states that the most limiting single failure is the MHSI (Ref. 54) as it reduces the rate of increase of boron concentration. For the full power case, the RP has chosen to apply the single failure to one of the channels of the protection signals that lead to reactor trip. I judge that this single failure is likely to have little bearing on the transient, and that the RP has not provided sufficient reasoning for the choice. In response to RQ-UKHPR1000-0392, however, the RP has provided reasoning for why other single failures would not be more limiting. In addition the RP has also applied the stuck rod assumption, which is clearly penalising. I therefore judge that the RP has applied the single failure criterion adequately.

279. With the above in mind, I am satisfied that the combination of the conservative assumptions leads to a very conservative analysis, and therefore meets my expectations for FA.7.

280. For the full power case, the RP presents the calculated DNBR (which is the limiting decoupling criterion) for the spectrum of break sizes. Break sizes of 200 mm and below do not result in reactor trip and are not challenging scenarios. For 210 mm and above, the reactor trips on either the high SG pressure drop, high neutron flux (power range) or the overpower ΔT signal, depending on the break size. In all cases there is an adequate margin to DNB. In my opinion, this demonstrates that the generic UK HPR1000 design is tolerant to a wide range of SLBs.

281. The RP has only presented results for the most liming case (260 mm). The analysis shows that following the initiation of the SLB the core power gradually rises over 20 s until the overpower ΔT and high neutron flux trip setpoints are reached. At this point reactor trip is actuated, however, the power continues to rise until the rods start to insert. The minimum DNBR occurs at the point just before the power decreases due to reactor trip. The calculated minimum DNBR is [redacted], meeting the deterministic limit of [redacted]. After reactor trip the core power drops rapidly, only increasing briefly as the cold water continues to add reactivity to the core. The core remains subcritical and core power stabilises. Heat is removed through the VDA [ASDS] and the ASG [EFWS], and system pressure and temperature decrease gradually.

282. I judge that the RP has performed conservative analysis to demonstrate that the fuel integrity criteria are met for the most onerous cases of SLB at full power, and therefore my expectations for FA.7 have been met.

283. For the accident initiated from hot zero power, the analysis shows that following the SLB and the cooldown of the primary circuit, the shutdown margin is eroded rapidly and the reactivity becomes positive. At this point, nuclear power starts to increase. The temperature of the fuel starts to increase and the Doppler feedback limits the power excursion. The power peaks at [redacted] %FP with a corresponding minimum DNBR of [redacted] against the design limit of [redacted] As pressure continues to drop due to the cooling of the primary circuit, boronated water from the MHSI brings the core subcritical reducing the core power. A large drop in core power is seen after the affected SG dries out and the reduction in primary coolant temperature increases sharply. As heat is continued to be removed by the ASG [EFWS], reactivity is added until the core becomes critical again and the power reduction slows until reaching a new power level at around 4% FP.

284. As the reactor remains critical after the action of the automated systems, it follows that the automated systems are not capable of bringing the plant to a controlled state. In response to RQ-UKHPR1000-1544 (Ref. 6), the RP has provided further arguments as to why it considers its position acceptable. The RP argues that the Class 1 human action to isolate the ASG [EFWS] feed to the affected SG is sufficient to bring the core subcritical, and that this is only credited after 30 minutes. Moreover, the RP argues that there are no other sources of reactivity addition that occur within this 30 minute period which cause an additional challenge. The RP argue therefore that during this time the reactor is in a stable state. As previously stated, I am satisfied that the RP has applied a sufficient delay before taking credit for manual actions. Moreover, I am satisfied that during the 30 minute period, the temperature, pressure and core power appear to be either stable or gradually moving in a safe direction.

285. The double ended guillotine SLB accident at hot zero power is unique in that the Westinghouse DNB correlation (W3) has been applied. During this accident, the most limiting conditions in the fuel arise at elevations lower than the first mixing grid. The W3 correlation is required because it is validated for use in this region of the core. However, the RP has had to extend the W3 correlation to account for the hot zero power analysis where the pressure falls below its validity range. ONR's Fuel and Core Inspector has found that the RP's justification for the use of the W3 correlation fell short of providing the level of confidence usually expected by ONR for design basis analysis, especially when the low margins observed in the analysis are considered (see Ref. 20). However, as the main steam line within the reactor building and safeguards building has been designated as HIC and considering the overly conservative assumptions made in the analysis, together with ONR's Fuel and Core inspector, I am satisfied that the use of the W3 correlation for the analysis of the double ended guillotine SLB at hot zero power is appropriate.

286. As with the increase in feedwater fault, the RP has not presented details of the maximum fuel and cladding temperatures. However, I judge that such lower power excursions should not lead to challenging temperatures.

287. To summarise, the RP has performed analysis of a wide range of break sizes for different plant states, covering the most onerous conditions. The RP has applied consequential failures and the single failure criterion appropriately. In my opinion, in both the full power and hot zero power cases, the RP has applied highly conservative assumptions. Nevertheless, the RP has demonstrated that margin to DNB exists. In my opinion the analysis therefore aligns with the expectations of FA.6 and FA.7.

Confirmatory Analysis

288. To gain further insights into the RP's analysis and to gain confidence in the results I commissioned my TSC to undertake independent analysis of this fault. My TSC performed an analysis of both the most limiting size full power case and the double ended guillotine break at hot zero power (Ref. 56). The ATHLET analysis was coupled with the 3D core neutronics code, QUABOX/CUBBOX for both sets of analyses. A consequence of this approach is that, in contrast to the RP's approach of making unrealistic combinations of neutronic parameters, the TSC analysis was constrained to using physically realistic cycle specific values.

289. For the full power case, the confirmatory analysis has highlighted the large conservatisms that the RP has included in its analysis. In the ATHLET analysis, the reduction in core inlet temperature and the subsequent rise in core power are significantly slower. My TSC considers that this is due to the RP's conservative modelling of the critical flow through the break and conservative assumptions related to the control of the SG level, both of which enhance heat transfer from the primary to the secondary sides. As a result, the TSC analysis also shows that reactor trip occurs on

SG level (narrow range) low 1 signal, rather than high neutron flux / overpower ΔT signal seen in the RP's analysis. The lower rate of power increase, slower thermal hydraulics transient and less pessimistic neutronic data result in a considerably higher DNBR observed in the TSC analysis (~2.2 with a limit of 1.51).

290. A notable difference between the ATHLET and GINKGO simulation of the SLB from full power is the predicted power after reactor trip. In the RP's analysis, the power remains at around 15% Full Power (FP) after reactor trip. The RP has explained that this is due to residual fissions, and does not indicate that the core is critical (Ref. 57).

291. The hot zero power case also highlighted the significance of the conservatisms in the RP's analysis. In particular, the inability of the ATHLET code to inhibit reverse heat transfer from the SGs to the primary circuit, differences in the affected SG blowdown rate, and differences in blowdown of the unaffected SGs (prior to MSIV isolation), results in a significantly slower cooldown of the primary circuit in the ATHLET calculation. In addition, the neutronics used in the TSC analysis are best estimate. The combination of these factors results in a much later return to criticality in the ATHLET calculation with a smaller power excursion. The DNBR calculated in the ATHLET calculations is larger than that in the RP's analysis.

292. My TSC also performed several sensitivity studies to understand the differences in the calculations. Amongst these, the TSC artificially decreased core inlet mixing, used the point kinetics models to better align its analysis with the RP's, and decreased the break size to observe the effect of decreasing the secondary depressurisation rate on the transient. However, in all cases, the TSC's analysis could not reproduce an early return to criticality and calculated a DNBR far greater than the RP's.

293. To conclude, the TSC analysis has highlighted that whilst the plant behaviour in the RP's analysis may not be fully representative of a realistic steam line break accident, the RP's analysis is conservative and sufficient for its purposes. Moreover, in my view the TSC's analysis demonstrates that when the accident is modelled more realistically that the UK HPR1000 is capable of bringing the plant to a safe, stable state, with significantly higher margins than those found in the RP's analysis.

Radiological Consequences

294. My assessment of the RP's methodology for the calculation of radiological consequences is presented in Section 4.7. In this section, I only present my assessment against ONR's expectations for SAP NT.1 and Target 4.

295. The RP presents the results of radiological consequence analysis for the large steam line break in Ref. 58. The predicted off-site radiological consequences are reported as being between 10^{-2} and 10^{-1} mSv. With a PIE frequency between 10^{-5} and 10^{-4} pa, the consequences lie well below the BSL, but above the BSO.

296. In considering the acceptability of the consequences I note the following points:

- I have found that the general methodology for radiological consequence calculation is conservative (see Section 4.7)
- The DBC analysis demonstrates that no fuel failure is expected as a result of the accident.
- The PIE frequency is based on industry OPEX and doesn't account for differences in quality assurance or preventative measures that can reduce the failure frequency. This means as the MSL is designated as HIC that the failure frequency is likely to be conservative (this has been considered by ONR's PSA inspector, Ref. 24)

- In addition to the above point, the RP has designated the steam line within the reactor building and the safeguard building as HIC. The radiological consequence analysis is based on the over pressurisation of the containment due to a SLB within the containment, yet the RP has not adjusted the PIE frequency to account for the HIC classification.

297. With the above in mind, I am satisfied that the RP's PIE frequency analysis and radiological consequence analysis is conservative. Should the analysis be refined, I am confident that the BSO of Target 4 could be satisfied. Since the analysis demonstrates that, even when using very conservative assumptions, no fuel failure is predicted for this accident, I am satisfied that the consequences of this fault are minimised, consistent with the expectations of FA.7.

Structural Integrity Classification Analysis

298. As described previously, the RP has undertaken analysis of the large SLB within the safeguard building to inform the classification of the pipework within the safeguard building.

299. A break in the safeguard building presents less onerous conditions for overcooling of the reactor than that considered in the design basis condition analysis because the depressurisation rate is slightly lower and the break is isolable. However, the single failure and consequential failure are applied differently depending on the break locations. A SLB in the safeguard building close to, and downstream of the MSIV has the potential to cause dynamic loads that prevent closure of the MSIV on demand, preventing isolation of a break. In this case, the single failure is applied to a different MSIV. The result is that two SGs blowdown (instead of one considered in the DBA).

300. In response to RQ-UKHPR1000-0969 (Ref. 6), the RP explains that for an accident in which two SGs blow down, the predicted DNBR is only slightly below the design limit. However, the RP has also explained that an accident in which two SGs blow down is predicted to lead to core instability and therefore concludes that an accident involving the blowdown of two SGs is intolerable. As such the RP has concluded that the MSL pipework close to the MSIVs should be designated HIC. This claim has been considered in detail by ONR's Structural Integrity assessment, which is reported in Ref. 32.

301. In cooperation with ONR's Fuel and Core inspector, from a fault analysis perspective, I judge that the RP's conclusion is reasonable, and that the conclusion supports the decision to designate the MSL pipework in the safeguard building as HIC.

4.3.2.3 Diverse Protection

302. In this section, I present my assessment of whether the RP has demonstrated that diverse protection for frequent decrease in primary circuit temperature faults in which CCF of the primary means of protection occurs.

303. The RP has not identified any increase in heat removal faults for demonstration of effectiveness of diverse protection for frequent faults. Put simply, this is because the reactivity transient is bounded by rod movement accidents, and the nature of the accidents (a decrease in primary circuit temperature) means that heat removal and RCP [RCS] confinement safety functions are not challenged. I judge that the RP's reasoning is sound.

304. The RP has identified diverse protection for all frequent faults in the fault schedule (Ref. 10). Diverse protection for C&I failure, signal failure and mechanical failure are identified for each safety function, for both reaching the controlled and the safe state.

305. As stated previously, the most important safety functions required for protection against reduction of primary circuit temperatures are related to isolation of the cause of the temperature reduction and the insertion of negative reactivity. I have therefore sampled these safety functions in my assessment of the diverse protection for the small SLB.

306. For signal failures, the RP has identified many signals which can both actuate reactor trip and actuate systems to isolate the steam line and/or main feedwater lines. Taking reactor trip as an example, for the small SLB, the fault schedule identifies pressure drop of SG high 0, pressure drop of SG high 1, SG pressure low 1 (and permissive signal P11), or the Safety Injection signal as the primary means to actuate reactor trip. In addition, the RP has also identified the pressuriser pressure low 2 + P7 as a diverse signal.

307. For C&I failures, the RP has identified diverse means of detection and actuation of necessary systems. Taking the safety function “prevention of overcooling” during a small SLB as an example, the RP has identified that turbine trip, isolation of the high and low feedwater lines and closure of the MSIV is necessary. For each of these, the RP has identified a corresponding signal and action taken by the KDS [DAS] to fulfil the safety function.

308. For mechanical failure related to rod insertion, the RP identifies the F-SC2 RBS [EBS] system to arrest reactivity excursions. For diverse protection for reactivity in the long term, the RP identifies the F-SC3 chemical volume and control system (RCV [CVCS]).

309. For mechanical failure, the RP identifies that failure to close the MSIV, FLIV or LLIV may result in overcooling. For mechanical failure to isolate the ARE [MFFCS] full load lines, the RP identifies “isolation of the full load lines and the low load lines” as the diverse protection function, which initially appears to be a shortfall in diversity. However, whilst not explained, the ARE [MFFCS] incorporates both control valves and isolation valves for both the low load and full load lines, and a main isolation valve, which completely isolates the ARE [MFFCS] from the SG. This requires knowledge of the wider safety case, and only presents a minor shortfall in my expectations for FA.9.

310. The RP has not identified diverse protection for mechanical failure to close the MSIVs. However, it should be noted that the small SLB does not actually place a demand on closure of the MSIVs.

311. To conclude, the RP has identified diverse protection for the short term and long-term safety functions for frequent faults. The RP has analysed bounding cases, which demonstrate that the plant is tolerant to sequences in which the primary means of protection fails. With the above in mind, I am satisfied that the RP’s safety case for decrease in primary circuit temperatures meets my expectations for demonstrating diverse protection for frequent faults.

4.3.3 Decrease in Core Coolant System Flow

312. The RP has identified the following loss of flow faults:

- Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump
- Forced Reduction in Reactor Coolant Flow
- Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft break

313. These faults are of decreasing likelihood and increasing severity relative to each other. The first two faults are frequent faults (DBC-2 and DBC-3 respectively) and the third fault is a DBC-4. I have chosen to sample the transient analysis of the locked rotor fault

and consider the diverse protection available for the frequent faults. I have not considered the transient analysis for the frequent faults in detail as the results show margin to the acceptance criteria. A locked rotor is a DBC-4 fault and relates to the instantaneous stop of an RCP due to seizure or break of the shaft and it is the limiting decrease in flow fault for DNB.

4.3.3.1 Locked Rotor

314. Reactor coolant pump seizure (locked rotor) or reactor coolant pump shaft break is caused by a mechanical failure and causes a rapid reduction in flow, a sharp decrease in heat removal and increase in reactor coolant temperature. This may result in fuel rods experiencing DNB and subsequent possible fuel damage. The RP presents the analysis of this fault in Ref. 59. The RP argues that the RCP seizure (locked rotor) is more onerous than a shaft break as the coolant flow reduction rate is higher. I am content to accept this argument.

315. The thermal hydraulic transient has been analysed using GINKGO, and LINDEN is used to perform the DNB analysis. BIRCH is used to analyse thermal behaviour of the fuel at the hot spot. I am content that these codes are appropriate for this analysis.

316. The RP has analysed two cases to cover different moderator density coefficients. Case 1 uses a bounding moderator density coefficient to cover 80%FP to 100% FP and the locked rotor occurs at full power. For Case 2 the moderator density coefficient covers 0% FP to 100% FP and the locked rotor occurs at 80% FP.

317. Reactor trip is actuated by the low flow in one primary loop signal and a LOOP is assumed to occur at the time of the turbine trip (which is initiated by reactor trip). The LOOP leads to a loss of power to all RCPs causing them to coast down. Due to the fast nature of the accident, the most limiting time in the accident occurs prior to the initiation of safety systems. However, the RP explains that ASG [EFWS] and VDA [ASDS] are essential for the long-term heat removal.

318. For Case 1 [redacted]% of rods experience DNB and the PCT is [redacted] °C. For Case 2, the minimum DNBR remains above the limit.

319. I have reviewed the main assumptions within Ref. 59 and I am satisfied that they are appropriate and consistent with the expectations of FA.7. Whilst a significant number of fuel rods experience DNB during this transient the maximum off-site radiological consequences of 14 mSv is below the BSL of RPT-4 and Target 4 of the SAPs (100 mSv). To gain confidence that the consequences of this fault are ALARP I instructed my TSC to undertake confirmatory analysis of this fault and I engaged with the RP to seek improvements in the design and analysis to reduce the number of rods that would experience DNB.

Confirmatory Analysis

320. My TSC undertook the analysis of Case 1 using ATHLET (which is a best estimate code with integrated point kinetics model) and QUABOX/CUBBOX (used for 3D neutronics coupled calculations) (Ref. 60). After an initial evaluation using ATHLET and QUABOX/CUBBOX, my TSC undertook a range of sensitivity studies to better understand the RP's analysis methods and reproduce the results.

321. The occurrence of DNB causes a significant decrease of heat transfer coefficient and a large increase of the cladding temperature. In the coupled cases using QUABOX/CUBBOX, my TSC's analysis did not show any noticeable increase of the peak cladding temperature as no DNB was predicted. In other sensitivity calculations with the point kinetics model, my TSC modified the axial power peaking and found that

the peak cladding temperature increases with a range of 300 - 500 K. Unlike the RP's results, which show DNB occurrence at the very beginning of the transient, my TSC's analysis shows that there is a slight delay in DNB, indicating that the RP's analysis includes additional conservatisms that could not be accounted for in the TSC analysis.

322. My TSC has advised (Ref. 60) that the RP's prediction (of DNB at the beginning of the transient) is unphysical and very conservative and, as such, the RP's results can be considered as conservative regarding PCT. Together with my TSC's finding of no DNB when using the more sophisticated and best-estimate 3D model this gives me confidence that the RP's analysis is conservative.

ALARP

323. The second part of my assessment of this fault was to engage with the RP to seek potential improvements in the design and analysis. The RP has specifically considered the locked rotor fault within both the supporting report on ALARP for DNB (Ref. 21) and the ALARP assessment for DBC (Ref. 61).

324. I have considered the adequacy of the radiological consequence assessment methodology in Section 4.7 of this report. The focus of my assessment for this fault has been to gain confidence in the conservative assessment of radiological consequences and to seek a demonstration that the risks are reduced ALARP.

325. The RP has identified 4 potential improvements within Ref. 21: reduction in the amount of fuel failure assumed in the consequences analysis, reducing the primary to secondary leakage limit, reducing the secondary steam release and measures to reduce worker dose.

326. Within the transient analysis report (Ref. 59) the RP has calculated that [redacted]% of rods will enter DNB. In Ref. 21 the RP has concluded that this can be reduced to [redacted]% by optimising the conservatisms in the analysis. This has been considered in ONR's Fuel and Core Assessment Report (Ref. 20) which concludes that the data used remains appropriate for use in DBA. However, for the radiological consequences analysis (Ref. 58) it is assumed that 10% of the rods experience DNB and [redacted] of the fuel is melted. The RP has therefore recalculated the radiological consequences assuming [redacted]% of rods in DNB and no fuel melting. As a result the maximum off site dose is reduced from [redacted] to [redacted] (Ref. 61).

327. The release path in a locked rotor fault is via primary to secondary leakage and then through the VDA [ASDS] which releases steam to atmosphere to remove secondary side heat. Any measures which release the amount of activity carry over from primary to secondary side would be beneficial for this fault. The RP has considered within Ref. 61 the maximum primary to secondary leakage considered within the radiological consequence analysis and compared to that used for similar PWR and concluded that it is appropriate and that any reduction in this limit would impact operational flexibility. The RP has also considered increasing the secondary cooldown rate which would reduce the total amount of steam released from VDA [ASDS] but concluded that the detriments in terms of impact on RBS [EBS] design and stresses on components outweigh the potential benefits. The RP has therefore not progressed any changes related to these factors. I am content to support these conclusions.

328. As a result of the updated fuel failure data, the off-site radiological consequences of the locked rotor are well below the BSL and approaching the BSO of Target 4 of the SAPs. The on-site doses are also below the BSL. I am content that the RP has undertaken a thorough review of the analysis to evaluate conservatisms and of the design to identify and evaluate potential improvements, consistent with ONR's expectations for the demonstration that risks are reduced ALARP. I am satisfied that

the RP has demonstrated a conservative assessment of the consequences (in accordance with the expectations of FA.7) and that there are no further reasonably practicable improvements that could be made.

4.3.3.2 Diverse Protection for Flow Reduction Faults

329. For the frequent faults of partial loss of core coolant flow due to loss of one reactor coolant pump and forced reduction in reactor coolant flow (3 pumps), the decrease in reactor coolant flow causes a rapid increase in coolant temperature and pressure, potentially resulting in DNB and subsequent fuel damage.

330. Protection against the partial loss of flow fault is provided by reactor trip on Low flow rate in one primary loop (if nuclear power is higher than 30% FP) or pressuriser pressure high 2 if the power is lower than 30% FP and via operation of VDA [ASDS] for heat removal. For forced reduction in flow the reactor trip is on the low RCP speed or pressuriser pressure high 2 signal, depending on whether the power is above 10% FP or not. In both sequences the PSVs may be required to control primary circuit pressure. The RP has submitted analyses (Refs. 62 and 63) which show that there is significant margin to DNB for both faults.

331. The fault schedule includes diverse means of delivering the safety function for these faults:

- For failure of reactor trip the ATWS system will insert negative reactivity.
- For a failure of the secondary side heat removal (due to either failure of ASG [EFWS] or failure of VDA [ASDS]) the operator can manually feed and bleed the primary circuit.
- For a failure of the PSVs to open the pressure can be controlled using the secondary side depressurisation.

332. Within Ref. 34 the RP has systematically reviewed the possible sequence to identify bounding scenarios to demonstrate the effectiveness of the claimed measures. Within Ref. 34 forced reduction in reactor coolant flow (3 pumps) is considered to bound partial loss of core coolant flow. Given that the forced reduction in flow is a more severe transient I am content that this is reasonable.

333. Ref. 34 draws the following conclusions:

- A reduction in coolant flow with failure of reactor trip needs to be explicitly analysed.
- A reduction in flow with a failure of heat removal can be bounded by a total loss of feedwater fault.
- A reduction in flow with a failure of PSVs can be bounded by an inadvertent closure of all MSIVs with failure of PSVs.

334. The rationale within Ref. 34 is brief but essentially the RP argues that reduction in flow faults are less onerous than those involving a loss of secondary cooling as the pressure increase is higher for the latter group of faults. I have briefly examined the relevant analyses and I am content that this argument is reasonable.

335. I have discussed the analysis of ATWS events within Section 4.4.2 of this report and the adequacy of the bleed and feed function in sub-section 4.4.1.1.

336. The RP has not presented any specific radiological consequence assessment for these sequences involving a failure of a SC1 safety system. In Ref. 12 the RP argues that these sequences can be bounded by the consequences of a SB-LOCA or a turbine trip (depending on whether the PSVs open or not). I have discussed the radiological

consequences of these faults in the relevant section of this report but they are well below the SAPs Target 4 BSL for infrequent faults and are within an order of magnitude of the BSO.

337. I am therefore satisfied that the RP has adequately demonstrated diverse protection for flow reduction faults. Whilst the safety case for these faults is contained within many documents without an overall discussion of the available protection or conclusion that risks are ALARP, I am satisfied that the relevant information is available within the safety case. I therefore consider that the failure to fully meet the expectations for the presentation of ALARP arguments set out in NS-TAST-GD-005 (Ref. 4) to be a minor shortfall.

4.3.4 Reactivity and Power Distribution Anomalies

338. The RP has identified the following reactivity and power distribution faults:

- Uncontrolled RCCA Bank Withdrawal at power
- Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition
- RCCA misalignment up to Rod Drop
- Startup of an Inactive Reactor Coolant Loop at an Improper Temperature
- Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV[CVCS], REA[RBWMS] and TEP[CSTS]
- Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV[CVCS], REA[RBWMS] and TEP[CSTS] (State A/B/C Shutdown Conditions)
- Inadvertent Core Loading of Fuel Assemblies (State A/B/C/D/E)
- Uncontrolled Single RCCA Withdrawal
- Spectrum of RCCA Ejection Accidents
- Boron Dilution due to Rupture of One Heat Exchanger Tube

339. The majority of these faults are DBC-2 faults with the exception of Inadvertent core loading of fuel assemblies and uncontrolled single RCCA withdrawal (which are DBC-3) and RCCA ejection accidents and Boron dilution due to a rupture of one heat exchanger tube (which are DBC-4 faults). I have chosen to sample four of the above faults. The first is the Uncontrolled RCCA Bank Withdrawal since this is a frequent fault which challenges protection systems over a range of initial powers and reactivity insertion rates. The second is a decrease in boron concentration in the reactor coolant due to a malfunction in one of the connecting systems as this fault can be difficult to detect and requires operator actions to isolate the source of the diluted coolant. The third fault is the RCCA misalignment which includes the most extreme version of this fault which is a rod drop. The fourth fault I have sampled is the RCCA ejection accident as this is the limiting DBC-4 fault.

340. Whilst I have not sampled the inadvertent core loading fault, I have supported ONR's Fuel & Core inspector's assessment of the relevant transient analysis report and sought improvements to the safety case to demonstrate continued fault tolerance following the occurrence of an undetected core mis-load, rather than just a demonstration that the mis-load itself does not cause acceptance criteria to be breached. The RP subsequently provided adequate evidence of this. The assessment of this fault is reported in ONR's Fuel & Core assessment (Ref. 20.)

341. In the following sub-sections I consider each of the faults that I have sampled in turn.

4.3.4.1 Uncontrolled RCCA Bank Withdrawal

342. An Uncontrolled RCCA Bank Withdrawal is classified as a DBC-2 event. The transient is characterised by an uncontrolled reactivity insertion in the core, caused by the withdrawal of one or more RCCA banks at the maximum speed.

343. During power operation, the core is protected by either the Overtemperature ΔT or high neutron flux (power range, high setpoint) signal, depending on the rate of withdrawal. For a high reactivity insertion rate (i.e. a rapid withdrawal of RCCA banks), the neutron flux rises rapidly while core heat flux and reactor coolant temperature lags behind due to the thermal capacity of the primary circuit, and the high neutron flux signal triggers the reactor trip. For lower reactivity insertion rates, the overtemperature ΔT and high neutron flux trips become equally effective. For the lowest reactivity insertion rates (i.e. slowest withdrawal of RCCA banks), the increase of the coolant temperature follows the nuclear power increase and overtemperature ΔT signal become more effective.

344. Whilst the fault can occur in any operating mode, the RP has identified that shutdown conditions present the greatest challenge. In these conditions, if the RCCA bank worth is high enough, prompt criticality is possible. Protection against these faults is provided by the negative Doppler feedback which limits the power excursion before the reactor trip to insert any banks not fully inserted is triggered. For hot standby or hot shutdown conditions (POS A) the reactor is protected by high neutron flux (power range, low setpoint) and high neutron flux (intermediate range). For lower shutdown states the reactor is protected by high neutron flux (source range). As this trip setting is much lower than the intermediate range and power range trips the power increase caused by this fault will be halted before it increases significantly. Therefore, the bounding case analysed by the RP in Ref. 64 is withdrawal of two RCCA banks at hot shutdown in POS A.

345. From consideration of the above I am content that the RP has considered a range of conditions for the assessment of uncontrolled RCCA bank withdrawal faults and has provided sufficient assessment of these cases in accordance with ONR's general expectations for DBA (SAPs FA.5 and FA.6). Given that the margins to DNBR are smallest for the low power startup conditions I have focused my assessment on the relevant analysis presented in Ref. 64.

346. In Ref. 64, the RP considers two cases: the "DNB case" and the "fuel temperature" case. The two cases differ in the initial thermal-hydraulic conditions, namely inlet moderator temperature and primary pressure, which are changed from the nominal value according to the uncertainties in order to minimize DNB (+3.5 °C and -0.25 MPa) or maximize the power peak and thus the fuel temperature (-3.5 °C and +0.25 MPa). In practice, the results show that both cases lead to very similar results: [redacted] % peak nuclear power for the DNB case vs. [redacted] % peak nuclear power for the fuel temperature case.

347. SAP FA.7 sets the expectation that the analysis of design basis fault sequences should be conducted on a conservative basis. For the uncontrolled RCCA bank withdrawal fault the RP has made the following assumptions:

- Initial reactor coolant average temperature is at its nominal value plus uncertainty to penalise DNBR;
- Initial pressuriser pressure is at its nominal value minus uncertainty to penalise DNBR;
- Initial reactor coolant flowrate is equal to the thermal design flow with 10% SG tube plugging to penalise heat removal;
- The initiating event is the uncontrolled withdrawal of two RCCA banks with the maximum integral reactivity worth. For the zero power case they are fully

inserted at the beginning of the transient and assumed to be withdrawn simultaneously at the maximum speed;
- The Doppler feedback is set at the minimum enveloped absolute value of each cycle;
- The FΔH is calculated for the most penalising position and is fixed for the duration of the transient;
- A single RCCA with the highest worth is assumed to be stuck out of the core to minimise the negative reactivity after reactor trip.

348. In response to RQ-UKHPR1000-0720 (Ref. 6) the RP has confirmed that as the thermal power lags behind the nuclear power the influence of the moderator coefficient is limited and not as strong as the Doppler effect. However, the RP has also used conservative assumptions for the moderator coefficients. Overall, I am content to judge that the RP has used a suitable set of assumptions to ensure conservative results.

349. The results of the RP's analysis show that the fuel temperature remains below the acceptance criteria and that the minimum DNBR remains above the limit.

Confirmatory analysis

350. To gain confidence in the RP's modelling of this fault, I commissioned my TSC to undertake confirmatory analysis of the limiting uncontrolled RCCA bank withdrawal (Ref. 65). The RP and my TSC use different analysis approaches due to the different codes and modelling used. For the RP's analysis, a multi-step approach is applied. GINKGO (a system transient analysis code) is used coupled with a 1D neutron kinetics model POPLAR. The power calculated by POPLAR is then used in LINDEN for DNB analysis and in BIRCH for fuel temperature analysis.

351. The TSC utilised a realistic modelling approach with conservative parameters. The transient is modelled with an open core model using ATHLET, a best-estimate thermal-hydraulics system code coupled with the 3D neutron diffusion code QUABOX/CUBBOX. In order to achieve more limiting results, an ATHLET stand-alone hot channel model was developed for DNB and fuel temperature analysis.

352. As the RP's margins to DNB were smaller than those to fuel temperature, my TSC used similar initial and boundary conditions to penalise the model for DNB. My TSC found that even with the maximum possible RCCA withdrawal speed, the reactivity insertion rate was lower than that used by the RP. GRS attributed this to the RP using an axial power distribution which is tilted towards the core bottom. In GRS' model the reactivity insertion cannot be influenced in this way so GRS used a higher rod withdrawal speed to match the reactivity insertion rate and presented this as a sensitivity study.

353. My TSC found that the RP predicated an earlier and higher power peak than the ATHLET model and that maximum temperature and minimum DNBR were limiting in the RP's analysis. With the increased RCCA withdrawal speed implemented, the TSC results are closer to the RP's power peak (both in timing and magnitude) however the DNBR and peak temperature are lower than those from the RP's analysis and there is significant margin to the acceptance criteria.

354. Given that the acceptance criteria are met and there is no fuel damage, the RP has not undertaken any specific radiological consequence assessment of this fault. Instead the RP argue that the consequences can be represented by a Turbine Trip (as an intact circuit fault with no fuel damage). I am content that this is appropriate and that the consequences of this fault are acceptable when judged against SAP FA.7. This fault is not limiting for the longer-term analysis of criticality control or cooling and is bound by decrease in boron fault and loss of normal feedwater respectively.

355. Taking into account the results of the confirmatory analysis and my own assessment of Ref. 64 I am satisfied that the RP has demonstrated adequate margin to the acceptance criteria and that the methods used are appropriately conservative in line with the expectations of FA.7.

Diverse Protection

356. As an Uncontrolled RCCA bank withdrawal is a frequent fault, the RP has also considered a failure of the RCCAs to insert as a result of mechanical blockage of the rods. As with the main case the RP has presented separate analyses of the at power and shutdown conditions. Within this analysis, the at power case is more challenging and the RP calculates (Ref. 66) that 1% of the fuel rods will experience DNB. This meets the RP's acceptance criteria for infrequent faults which is that less than 10% of rods experience DNBR. The RP argues that the radiological consequences of this ATWS fault can be represented by an RCCA ejection as in both faults some DNB occurs and there is a direct release to containment. Whilst this is true, the release paths to containment are different. In the RCCA ejection the release is via the leak site while in the uncontrolled RCCA withdrawal ATWS the release is via the PSVs which are required to mitigate the pressure rise.

357. I have therefore considered the modelling of the source term for RCCA ejection (Ref. 67) and note that it considers only the total activity released from the primary circuit which is independent of the leak size or duration. The RP has also considered 10% cladding failure fraction and [redacted] of the fuel rods have melted, despite the transient results showing only [redacted] DNBR and no fuel melt for RCCA bank withdrawal. As such I am content that the radiological consequence assessment of RCCA ejection is appropriate to bound the consequences of an uncontrolled RCCA withdrawal ATWS. The consequences of RCCA ejection and comparison against Target 4 of the SAPs are discussed in detail in sub-section 4.4.5.4.

4.3.4.2 Decrease in Boron Concentration in Reactor Coolant due to Malfunction of RCV[CVCS], REA[RBWMS] and TEP[CSTS]

358. An uncontrolled boron dilution event may result from a number of causes, including operator error, failure of the REA [RBWMS] or RCV [CVCS] or a leak from the RRI [CCWS] through TEP [CSTS] to RCV [CVCS] and into the primary circuit. These faults result in a uniform reduction of the boron concentration in the core (homogeneous dilution) and a consequential rise in core reactivity. The RP has assigned these as DBC-2 faults and I agree that this is appropriate Unlike some other designs, the generic UK HPR1000 design does not have safety classified boron meters to directly detect a change in boron concentration. Instead, the protection is provided via detection of changes in core parameters.

359. The RP submitted a report on boron dilution safety functions (Ref. 68) which describes the safety features that are in place to detect and protect against boron dilution events. For the scenarios considered in this section the principal functions are to insert negative reactivity and to isolate the source of the dilution.

360. It should be noted that heterogeneous boron dilution faults, where a slug of unborated water is introduced into the primary circuit, are discussed within Section 4.3.9 of this report.

361. Ref. 69 presents analysis for three different homogenous boron dilution events:

- The reactor at power and the RCCAs in manual operation. In this case the reactor trips on Overtemperature ΔT or Overpower ΔT and isolation of the dilution source is also automatically triggered by this signal.

- The reactor at power and the RCCAs in automatic operation. In this case the RCCAs (R Bank) will automatically move to compensate for the reactivity addition and the operator is required to trip the reactor when the R Bank rods reach Bank R position low 3. Isolation of the dilution source is automatically triggered by this signal (in conjunction with permissive signal P10).
- The reactor in State A/B/C Shutdown conditions. In shutdown conditions the reactor trip signal on high neutron flux (source range) which actuates a reactor trip and isolation of the dilution source.

362. The analysis of these boron dilution events is calculated using COCO. The assessment of this code is reported within ONR's Fuel and Core report (Ref. 20). SAP FA.7 sets the expectation that the fault sequences should be analysed on a conservative basis. The most important parameters for the analysis are the initial boron concentration (which is minimised) and the dilution flow rate (which is maximised). I am satisfied that the assumptions used by the RP in the analysis (Ref. 69) seem reasonable and should produce conservative results, consistent with the expectations set by FA.7.

363. The conclusions of the RP's analysis of this fault (Ref. 69) are:

- For the uncontrolled boron dilution of reactivity control case at power operation conditions in manual control mode, the calculation results for all fuel cycles analysed show that the automatic isolation of the dilution source ensures that the core remains subcritical after reactor trip and that the minimum DNBR remains greater than the design limit.
- In automatic control mode, the isolation of the dilution source can be achieved before the rods reach Bank R position low 4 (at this position they no longer insert and cannot compensate for any further increases in reactivity). During power operation, the DNBR is always greater than the design limit.
- For shutdown conditions, the reactor always remains subcritical following reactor trip.

364. Boron dilution faults are most onerous when the plant is shutdown at the start of cycle due to the excess reactivity needed to run for the cycle. The excess reactivity requires a high boron concentration within the primary coolant to prevent criticality. ONR's Fuel and Core assessment has identified (Ref. 20) that this high boron concentration causes the moderator temperature coefficient to be positive in some plant states. In these conditions a fault that causes boron dilution to the point of criticality may escalate due to the positive temperature feedback.

365. I have discussed the implications of this with the RP as a return to criticality will cause a reactor power transient which would normally be limited in extent by reactivity feedback. However, when the transient initiates from cold temperatures with a positive moderator temperature coefficient, significant heat input may be required before the total reactivity feedback is sufficiently strong to reverse the power rise. In response to this challenge the RP has supplemented the base case analysis with additional information (contained within Appendix A of Ref. 69) to demonstrate the capability of reactor trip triggered by the high neutron flux (source range) signal for a boron dilution in cold shutdown conditions.

366. This additional analysis shows that, in some cases the high neutron flux (source range) signal will be triggered after the core reaches criticality. In these circumstances the RP suggests that the core power is around [redacted] % FP when high neutron flux (source range) signal is triggered (based on experience from CPR1000 reactors). Given this low power the RP argues that there are no consequences for the core. I am in principle, content to accept this conclusion. However, this safety case argument is very brief and is based upon a judgement from the CPR1000 reactor design. The neutron

flux is increasing rapidly at time of the trip and there is potential for a power overshoot following reactor trip and this is not addressed. Furthermore, the trip levels for UK HPR1000 will need to be confirmed once the design of the source range detectors has been confirmed. I have therefore raised the following assessment finding:

AF-UKHPR1000-0032 – The licensee shall, as part of detailed design demonstrate that the high neutron flux (source range) trip setting can protect against homogeneous boron dilution faults from shutdown conditions at the start of cycle.

367. Given that the acceptance criteria are met and there is no fuel damage, the RP has not undertaken any specific radiological consequence assessment of a boron dilution fault. Instead the RP argues that the consequences can be represented by a Turbine Trip (as an intact circuit fault with no fuel damage). I am content that this is appropriate and, given that there is no fuel damage that the consequences of this fault are acceptable when judged against SAP FA.7. This fault is not limiting for the longer-term analysis of cooling and is bounded by a loss of normal feedwater fault.

Diverse protection

368. The RP has considered a failure of the primary means of reactor trip within the Fault Schedule (Ref. 10) and identified alternative protection measures. In the event of a failure of reactor trip due to a RPS failure the fault schedule (Ref. 2, Table 14) claims:

- For the reactor at power and the RCCAs in manual operation the diverse protection is provided by high neutron flux (power range, high setpoint).
- For the reactor at power and the RCCAs in automatic operation the diverse protection is provided by the hot leg pressure high 2 signal.
- For the reactor in POS A/B/C shutdown conditions the diverse protection is provided by manual reactor trip (via the KDS [DAS]) on Bank R position low 3.

369. The Bank R position Low 3 signal is limited by an interlock which only becomes effective once core power is above [redacted]%. The core power is determined from the power range detector channel of the RPN [NIS]; the primary and diverse means of reactor trip therefore both rely on measurements of neutron flux. I sought evidence to demonstrate that the source range and power range detectors can be considered diverse to support the claims made for shutdown faults. In response the RP has indicated that in the Fangchenggang reference plant uses different technologies for the source range, intermediate range and power range detectors. [redacted] The use of such diverse technologies should reduce the risk of a CCF of these detectors, however the types of detectors to be used within the generic UK HPR1000 design are not specified and these choices will need to be confirmed by the licensee during detailed design. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-00394 – The licensee shall, as part of detailed design, demonstrate that the source range, intermediate range and power range detectors can be considered as diverse and that the risks of common cause failures are reduced to as low as reasonably practicable.

370. There was no explicit analysis of any sequences involving failure of the RPS [PS] or sensor failure in the original submissions as the RP argues that they are bounded by other, more severe reactivity insertion events (Ref. 34). I sought more information to support this and the response to RQ-UKHPR1000-1755 (Ref. 6) presents additional evidence; the RP has presented the results of analysis which show that, in the event of RPS failure or sensor failure, alternative reactor trip signals will be triggered faster than

an ATWS event and therefore can be bounded by this. I am satisfied that this additional information provides adequate evidence to support the RP's claims.

371. In Ref. 34 the RP argues that CVCS malfunction leading to boron dilution with a failure of the RCCAs to insert can be bounded by the uncontrolled RCCA bank withdrawal with failure of the RCCAs to insert. Whilst no supporting arguments are given, I accept that a boron dilution event is a slow transient and that the reactivity increase from an RCCA bank withdrawal will be much greater. I was content to accept the RP's argument for power faults, however it was not clear that the original analysis conducted by the RP for uncontrolled RCCA bank withdrawal with failure of the RCCAs to insert bounds a boron dilution event at cold shutdown conditions. As a results, Appendices B and C have been added to Ref. 69 which consider:

- A homogenous boron dilution fault at Cold Zero Power with RCCA failure to insert due to mechanical blockage.
- A homogenous boron dilution fault at Cold Zero Power with RCCA failure to insert due to RPS [PS] failure.

372. I have not examined all of the assumptions used in these Appendices in detail but I note that for the ATWS scenario due to mechanical blockage the results show that the plant can be brought to a controlled state using the automatic FC1 and FC2 means. During this transient the core is predicted to return to criticality until the RBS [EBS] system injects sufficient borated water to induce subcriticality but the core power remains below [redacted]% FP. Heat removal is via RIS [SIS] in RHR mode.

373. For the ATWS due to RPS [PS] failure the operators are required to manually trip the reactor via KDS [DAS] on Bank R position low 3 signal which will also automatically isolate the dilution source via the KDS [DAS]. The Bank R position low 3 signal will only become effective once power exceeds [redacted]% FP therefore the core will return to criticality and experience a power peak. Whilst this power peak is only short it increases secondary side pressure such that the VDA [ASDS] will open to remove the heat.

374. A typical design basis criterion for reactivity faults during shutdown would be to show that there is no return to criticality (SAP ECR.1). However, for these sequences, which involve a failure of the FC1 protection systems, the RP has set a more relaxed criteria of no significant core heat up (thereby meeting DNB, PCT and fuel pellet melting criteria). Whilst the RP's acceptance criteria for both of these ATWS scenarios are met, I note that there are ways in which protection could be improved. The operator can manually isolate the boron dilution sooner if they respond to the REN [NSS] boron concentration signal. This is an FC3 signal which is not credited in the main analyses in Appendices B or C but is included as a sensitivity. If this operation is successfully achieved then a return to criticality is prevented. In my opinion a licensee should consider whether earlier, automatic isolation of the boron dilution source can be achieved. I have therefore raised the following assessment finding:

AF-UKHPR1000-0050 – The licensee shall, as part of detailed design, justify whether it is reasonably practicable to provide automatic isolation of the boron dilution source via the nuclear sampling system boron concentration signal to prevent a return to criticality in the event of a homogeneous boron dilution fault at cold shutdown with a failure of the reactor protection system.

375. The RP has also considered the need for diverse means of isolating the dilution source. Early in GDA (and in response to RO-UKHPR1000-0023, Ref. 7) the RP identified that there was a shortfall against its deterministic rules for demonstrating diverse protection for the isolation of the dilution source, should there be CCF of the isolation valves. Following a reactor trip and to prevent continuing dilution of the

primary coolant the RCV [CVCS] is isolated either automatically or manually. RCV [CVCS] is isolated if RCV3413VP- or both RCV3411VP- and RCV3412VP- are shut. If a CCF occurs which prevents the closure of these valves the RP has identified that the operator can manually isolate CVCS using alternative valves:

- Isolate RCV [CVCS] charging line by closing RCV8211VP- or RCV6512/6314VP-
- Isolate RCP[RCS] seal injection line by closing RCV8311VP-
- Stop the charging pumps manually in the main control room.

376. This sequence has been analysed for both at power operation and shutdown within Ref. 70 in which the RP shows that the existing reactor trips are sufficient to ensure that the core remains protected (and there remains a positive margin to DNB) and that the operator has sufficient time to perform the isolation of the dilution source before the core returns to criticality. The analysis reported in Ref. 70 uses the acceptance criteria and analysis rules for DBC-4 faults and I am content that this is appropriate and consistent with the expectations of FA.7 and NS-TAST-GD-006. An additional single failure has not been considered as the sequence already includes a CCF of an F-SC1 system and I am content that this is appropriate. For the most limiting conditions analysed the operator has at least [redacted] minutes to perform the isolation during power operation and [redacted] minutes during shutdown operations. Whilst no substantiation of this operation has been cited by Ref. 70 I am content that this should be ample time to perform these actions. I welcome the RP's consideration of failure of the isolation valves, and I am satisfied that the additional analysis demonstrates that the generic UK HPR1000 design is tolerant to such failures.

4.3.4.3 RCCA Misalignment up to Rod Drop

377. RCCA misalignment covers a range of faults from statically misaligned RCCA up to one or more dropped RCCAs within the same group. These are considered DBC-2 events. One or more RCCAs in one sub-bank dropping into the reactor core may cause a negative reactivity insertion which leads to a decrease in the primary average coolant temperature. Without reactor trip, the core power decreases and the mismatch in primary and secondary power results in a thermal hydraulic transient which is determined by the reactivity feedback and the average coolant temperature. Core power may return to the original level and overshoot; the combination of high power level and distorted power distribution may lead to DNB if the reactor core is not protected.

378. Ref. 71 describes the RP's transient analysis of an RCCA misalignment without limitation up to rod drop. The initiating event is the drop of one or several RCCAs. If the transient is severe a reactor trip would be triggered by the high negative neutron flux rate signal. However, there are some conditions for which reactor trip is not automatically actuated. In this case the core power first decreases and then due to both doppler and moderator feedback effects the average coolant temperature control returns to almost its initial value. Nevertheless, the RCCAs misalignment results in a distortion of the power distribution, which at nominal power condition can cause DNB and fuel pellet damage. To demonstrate the robustness of the generic UK HPR1000 design to all variations of this fault, the RP has analysed RCCA misalignment faults where a reactor trip is not triggered, to demonstrate that there is no DNB or fuel pellet damage.

379. To analyse this fault the RP takes a three-step approach:

- Firstly, COCO is used to identify those cases where reactor trip is not triggered then specific bounding neutronic data is developed.

- GINKGO and POPLAR are then used to evaluate the system response during the transient for the most penalising cases.
- Finally, LINDEN is used to perform DNB analysis.

380. The data generated in the first step of this process does not represent a real scenario, rather it is a set of bounding data which envelops all of the scenarios that the RP has identified. The validity of the COCO and POPLAR codes and the way they have been applied in this transient is considered in ONR's Fuel and Core Assessment Report (Ref. 20). The RP has analysed a range of core burn ups across a range of cycles and calculate that the minimum DNBR remains above the minimum value, albeit with a small margin for the most limiting case (the minimum DNBR is [redacted] against a criteria of [redacted]). The use of bounding data in this way is consistent with the expectation of FA.7 for conservative analysis and I am satisfied the RP has demonstrated that the acceptance criteria are met for the bounding scenario that has been analysed.

Confirmatory Analysis

381. Given the small margin for the limiting case and to gain additional confidence in the RP's analysis of this fault I commissioned my TSC to undertake independent modelling . My TSC performed the analysis using ATHLET (Ref. 72), a physically realistic system code coupled with the 3D neutron diffusion code QUABOX/CUBBOX.

382. As the RP's analysis case is a conservative bounding case my TSC were not able to reproduce the analysis exactly. Nevertheless, my TSC were able to reproduce the dynamics of the scenario and the differences observed between the two approaches are caused mainly by the differences in the reactivity feedback and control rod model. The TSC undertook a number of sensitivity cases to identify a limiting realistic case. All the TSC's calculation results, including the sensitivity analyses, show larger margins to acceptance criteria than the RP's results. My TSC therefore advised that the results obtained with LINDEN are more conservative than the ATHLET results.

383. I am therefore content that the RP has undertaken the analysis of RCCA misalignment faults using methods and assumptions consistent with the expectations of FA.6. This analysis demonstrates that reactor trip on high negative neutron flux rate will provide protection or, if reactor trip is not triggered that the resulting transient will not result in DNB..I am therefore satisfied that the consequences of this fault are acceptable when judged against the expectations set by FA.7.

Diverse Protection

384. As RCCA misalignment is a frequent fault, it is my expectation that the RP will have considered diverse protection against potential failures of the ex-core neutron detectors or the RPS, for those scenarios identified in Ref. 71 that would trigger a reactor trip. Early versions of Ref. 34 (the identification of bounding cases for demonstrating the capability of diverse protection) claimed reactor trip on either the pressuriser low 2 signal or high neutron flux (power range, high setpoint) signal. However, Ref. 34 also noted that the decoupling criterion could still be met without reactor trip (based on a preliminary study). I sought further justification to support this claim and the RP has since provided additional analysis in an update to Ref. 71. This analysis concludes that no DNB occurs following a RCCA rod misalignment up to rod drop without a reactor trip. I have not assessed this analysis in detail but it gives me confidence that the generic UK HPR1000 design is tolerant to RCCA misalignment faults, even if the protection systems are not actuated or there is a failure of reactor trip.

Radiological Consequences

385. Given that the acceptance criteria are met for the RCCA misalignment fault and there is no fuel damage, the RP has not undertaken any specific radiological consequence analysis of this fault. Instead the RP argue that the consequences can be represented by a Turbine Trip (as an intact circuit fault with no fuel damage). I am content that this is appropriate and that the consequences of this fault are acceptable when judged against SAP FA.7.

4.3.4.4 Spectrum of RCCA Ejection Accidents

386. RCCA ejection accidents are defined as the mechanical failure of the pressure housing of an RCCA drive mechanism resulting in the ejection of an RCCA and drive shaft. The consequences of this mechanical failure are a rapid positive reactivity insertion together with an adverse core power distribution, with the potential to lead to localised fuel rod damage.

387. The RP has treated the fault as an infrequent DBC-4 event with an initiating frequency that can range as high as 1×10^{-4} pa. As this is a passive failure, involving the failure of a pressure retaining component, this seems reasonable. The transient analysis aims to demonstrate that the inherent characteristics of the reactor core, coupled with the protection system can successfully control the fault sufficiently quickly to avoid significant fuel damage. The fault is primarily a race between the rate of increase in the stored energy in the affected fuel rods as the RCCA is ejected and the Doppler feedback coefficient which counter acts the reactivity insertion. As such, the assessment of this fault has been undertaken in conjunction with ONR's Fuel and Core Inspector (Ref. 20).

388. The RP's transient analysis for this fault is presented in Ref. 73. Reactor trip is triggered by the high neutron flux or the high positive neutron flux rate signal. The RP has assumed a random single failure of the high neutron flux (power range signal) or high positive neutron flux rate signal (sensor or channel). LOOP is considered as it reduces the primary flow.

389. I note the following key assumptions from the transient analysis (Ref. 73):

- The delayed neutron fraction is set as to the minimum value;
- The moderator temperature coefficient is set to the minimum absolute value for each burnup;
- The doppler temperature coefficient is set to the minimum value;
- The minimum absolute value is applied to the prompt neutron life
- The RCCA with the maximum worth is assumed to be stuck out of the core to minimise reactivity after reactor trip;
- A conservative negative reactivity insertion curve is used;
- The RCCA is conservatively assumed to be ejected within [redacted];

390. I am satisfied that these assumptions are reasonable and conservative, in accordance with the requirements of SAP FA.7.

391. The analysis results show that all the RP's acceptance criteria are met. However, the maximum fuel pellet temperature for the hotspot is close to the limit and the RP predicts that [redacted] of rods will experience DNB. The off-site radiological consequences of an RCCA ejection accident are calculated as [redacted] and [redacted] for adult, child and infant respectively. Worker doses are predicted as 335 mSv. These are the largest off-site radiological consequences for any of the design basis faults. ONR's Target 4 BSL is 100 mSv for off-site consequences and 500 mSv for on-site. Together with ONR's Fuel and Core Inspector I have therefore had significant engagement with

the RP to understand the analysis in detail and to seek reasonably practicable improvements to demonstrate that the consequences are ALARP.

392. The RP has considered each of the main assumptions used within Ref. 73 and performed sensitivity studies to investigate the effect of using less conservative assumptions. The RP has also reviewed the significant factors to evaluate whether there are any changes which could reduce the RCCA ejection fault. This work is reported in Ref. 21 which is assessed in detail in ONR's Fuel and Core Assessment Report (Ref. 20). Whilst this assessment was satisfied with the RP's conclusion that improvements to the fuel and core design are not reasonably practicable, Assessment Finding AF-UKHPR1000-0010 has been raised by the Fuel and Core topic area to ensure that rod insertion limits are optimised by the licensee to ensure that the consequences are ALARP.

393. I have considered the adequacy of the radiological consequence analysis methodology in Section 4.7 of this report. The focus of my assessment for this fault has been to gain confidence in the conservative modelling of radiological consequences and to seek a demonstration that the risks are reduced ALARP. In addition to the ALARP assessment for DNB (Ref. 21) the RP has also produced a report to examine the radiological consequences and consider options to reduce the consequences (Ref. 61), either by reducing conservatisms in the analysis or implementing improvements to design or operation.

394. The RP has identified four potential improvements within Ref. 61: reduction in the amount of fuel failure assumed in the consequences analysis, upgrading the EHR [CHRS], reducing the time to reach a negative pressure in safeguard building/fuel building and measures to reduce worker dose. For this fault the RP has chosen to re-examine the amount of fuel damage assumed in the analysis. My view on the other potential options is discussed in Section 4.8 of this report.

395. Within the transient analysis report (Ref. 73) the RP has calculated that [redacted] of rods will enter DNB. In Ref. 21 the RP has concluded that this can be reduced to [redacted] by optimising the conservatisms in the analysis. However, for the radiological consequences analysis it is assumed that 10% of the rods experience DNB and 1% of the fuel is melted. The RP has therefore recalculated the radiological consequences assuming [redacted] of rods in DNB and no fuel melting. As a result the maximum off site dose (infant) is reduced to [redacted].

396. If the updated fuel failure data is taken into account, the consequences of the RCCA ejection are between ONR's Target 4 BSL and BSO. In my opinion, the RP has undertaken a thorough review of the analysis and demonstrated that the consequences have been assessed conservatively. This judgement will need to be confirmed once Assessment Finding AF-UKHPR1000-0010 has been addressed.

397. This fault is not limiting for the longer-term analysis of criticality control or cooling and is bounded by decrease in boron fault and feedwater system large break respectively.

4.3.5 Decrease in Reactor Coolant System Inventory

398. The RP has identified the following faults which result in a decrease in reactor coolant system inventory:

- Decrease in RCP[RCS] Inventory due to RCV [CVCS] malfunction.
- Inadvertent opening of a Pressuriser Safety Valve (State A).
- Rupture of a Line Carrying Primary Coolant outside containment.
- Steam Generator Tube Rupture (SGTR) (one tube).
- SB-LOCA (State A).

- Uncontrolled RCP [RCS] Level drop.
- Inadvertent opening of a Pressuriser Safety Valve (State B/C).
- SGTR (two tubes in one SG).
- Intermediate Break LOCA (IB-LOCA) (State A/B).
- SB-LOCA (State B).
- SB-LOCA (State C/D/E).
- RHR System Piping Break inside or outside containment (State (C/D/E).
- Inadvertent opening of Severe Accident Dedicated Valves (one Train) (State A/B/C).

399. The first two faults are DBC-2 faults, SB-LOCA (State A) is a DBC-3 fault while the other LOCA faults are DBC-4. The RP has categorised SGTR (one tube) as DBC-3 while a two-tube fault is DBC-4. I have structured my assessment of these faults as follows. The uncontrolled RCP [RCS] level drop and RHR piping break faults have been sampled as part of my consideration of shutdown faults (Section 4.3.6). In this section I consider the safety case for small break (State A), intermediate and large break LOCAs, along with SGTRs. The last part of this section considers the potential for debris in the IRWST to affect cooling during a LOCA.

400. The RP has evaluated the short-term plant transient for all LOCAs against the same four acceptance criteria:

- the peaking cladding temperature (PCT) remains lower than 1204 °C
- the maximum cladding oxidation is lower than 17 % of the cladding thickness
- the maximum hydrogen generation is lower than 1 % of the amount that would be generated if the whole active part of the cladding were to react
- the ability to cool the core geometry shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling

401. The adequacy of these acceptance criteria has been assessed within ONR's Fuel and Core Assessment Report (Ref. 20). The RP assumes that as the first three criteria are met, then the fourth criterion (core geometry coolability) is met as well.

402. In my view, the first three criteria being met is a necessary but not sufficient condition for the core coolability criterion being met. The first three criteria being met does not preclude the occurrence of fuel cladding deformations, such as to clad ballooning and rupture. The fuel cladding deformation would cause reductions in the interrod flow area (brokage) for RIS[SIS] water to cool the fuel rods and can occur at the elevated temperatures experienced during a LB-LOCA. Whilst the Fuel and Core assessment report (Ref. 20) has concluded that the acceptance criteria are appropriate, some shortfalls have been identified in the way in which the fuel assemblies have been assessed against the core coolability criterion for LB-LOCA. I have considered the implications of this below when considering the adequacy of the safety case for LB-LOCA.

4.3.5.1 SB-LOCA

403. The RP defines a SB-LOCA (State A) as a break no larger than 5.0 cm equivalent diameter on the pipes of the reactor coolant system or on the upstream line of the second isolation valve connected to it. The RP considers it as a DBC-3 (frequent fault) and it is analysed within Ref. 74 and summarised within Chapter 12 of the PCSR. As a frequent fault the RP has considered the need to demonstrate diverse means of delivering the main safety functions. I am content the identification and categorisation of this fault is consistent with the general expectations of SAP FA.5.

404. A SB-LOCA can lead to a loss of primary coolant, a decrease in reactor coolant system pressure and a radioactive release to the environment. Following reactor trip, the Safety Injection signal is triggered by the Pressuriser pressure low 3 signal which initiates Medium Pressure Rapid Cooldown (MCD). The MCD is carried out by reducing the VDA [ASDS] setpoint to cool the primary coolant at [redacted]° C/h. With the safety injection signal the Medium Head Safety Injection (MHSI) and Low Head Safety Injection (LHSI) pumps are started and inject water when the reactor system pressure is below the pump injection flow. A controlled state is reached when the residual heat is removed via the break and VDA [ASDS], core sub-criticality is ensured, and the core coolant inventory is stable or increasing.

405. To achieve a safe state the cooldown continues until RHR conditions are met, the operator stops MHSI pumps to depressurise the primary circuit and the operator uses RBS [EBS] to compensate for the reactivity addition from the reactor cooldown,

406. The RP has analysed SB-LOCA using the LOCUST-K code, with conservative initial and boundary conditions for the short-term analysis and LOCUST for the long-term analysis. My assessment of the LOCUST-K is discussed within Appendix 1 of this report. The RP has assumed a coincident LOOP and applied a single failure to one EDG, as a result one train of RIS [SIS], RBS [EBS] and ASG [EFWS] are unavailable. The analysis assumes that the break is located such that injection flow from another train of RIS [SIS] will leak from the break. Therefore, only one train of RIS [SIS] is credited in the analysis.

407. The RP claims within Ref. 74 that if the core remains covered during the transient then the criteria described in para 400 above have been met. The RP has therefore analysed the ability to maintain RPV water level and the ability to take the plant to a safe state. The RP's analysis (Ref. 74) shows that, with penalising assumptions on key parameters the core remains covered throughout the transient and that the RHR connection conditions are met. The cooldown is manually initiated after 30 minutes and one or two trains of RBS [EBS] can be used to ensure sub-criticality during the cooldown to RHR conditions, depending on the cooldown rate. I have reviewed the assumptions used in the transient analysis and I am satisfied that they are appropriate for this analysis, consistent with the expectations of FA.6.

Confirmatory Analysis

408. To gain confidence in the RP's modelling of this fault, I commissioned my TSC to undertake confirmatory analysis of a SB-LOCA. My TSC used the ATHLET code to model a 5cm equivalent diameter break on the cold leg to the controlled state (Ref. 75). The TSC modelling used similar initial and boundary conditions and system performance assumptions to those used by the RP in Ref. 74.

409. My TSC made the following observations from comparison of its analysis with the RP's analysis:

- There is a higher break mass flow in my TSC's analysis in the early LOCA phase. The TSC uses the ATHLET specific discharge model CDR1D to calculate the break flow, whereas CGN uses the 0D Moody model, which tends to overestimate the critical flow of low-quality two-phase mixtures and of subcooled flow.
- There is a faster depressurisation of the primary side in my TSC calculation, which causes the early triggering of safety injection signal. Possible causes are the different discharge model for the calculation of the break flow and the phase separation model for horizontal and vertical pipes.
- Pump seal closure and clearance have been observed in my TSC calculation in two different simulation phases:

- in loop 2 and 3 between 1300 s and 2200 s, which causes primary pressure oscillation;
- closure in all loops (observed between 2600 s and 4000 s), in which the natural circulation is inhibited and the collapsed level in the core falls below the top of active core until the loop seal clearance.

- Total liquid mass in primary side and in SGs are comparable in the TSC and RP's analyses, however the liquid mass in primary system in GRS calculation is lower than the RP. During the second loop seal closure (between 2 600 s and 4 100 s), natural circulation stops in all 3 loops and more water is pushed out of the break than injected into the primary loop through RIS, causing a drop of the total water inventory in primary side to lower values than the RP.
- ACT behaviour in loop 1 in the RP's analysis indicates an oscillating water flow in cold leg due to the RIS injection, whereas a continuous flow is calculated by ATHLET due to the consideration of thermal mix phenomena.
- No core uncovery with heat-up is calculated in either the RP's or my TSC's analysis, however the core (collapsed) level drops below the top of active core in my TSC's analysis.

410. The SB-LOCA confirmatory analysis results of my TSC show that the initial and boundary conditions selected by the RP to maximise primary heat and penalise core heat-up are conservative, particularly the core related assumptions such as axial power profile, peaking factors and decay heat data. Despite the collapsed level dropping below the top of the active core in my TSC's analysis, the PCT does not exceed [redacted] °C and so remains significantly below the acceptance criteria limit of 1204 °C.

411. Although there are some differences between the confirmatory analysis and the RP's analysis, given the significant margin to the acceptance criteria I am content not to investigate this further for GDA. I am satisfied that the RP's analysis of SB-LOCA is consistent with the expectations of FA.6 and FA.7 and demonstrates that a controlled state can be achieved with a single train of RIS [SIS].

Diverse Protection

412. As a frequent fault, the RP has also considered the failure to deliver primary safety functions (Ref. 34) and has undertaken explicit analysis of a number of bounding scenarios. For those scenarios without explicit analysis, Ref. 34 provides the arguments as to why they are less onerous than the bounding transients.

413. Some of these analysis are contained with Chapter 12 of the PCSR (Ref. 4), others form part of the RP's analysis of DEC-A events and are discussed within Chapter 13 of the PCSR (Ref. 4). Within Chapter 12, the RP has summarised the analysis of a SB-LOCA with failure of reactor trip sensor (Ref. 76). Within Chapter 13, the RP has summarised the analysis of the following sequences:

- SB-LOCA with Failure of MCD (Ref. 77)
- SB-LOCA with Total Loss of LHSI (State A) (Ref. 78)
- SB-LOCA with Total Loss of MHSI (State A) (Ref. 79)
- SB-LOCA with ATWS by Rods Failure (Ref. 80)

414. The protection against these fault sequences can be summarised as follows:

- A failure of pressuriser pressure low 3 signal can be protected against by the hot leg pressure low 3 signal
- A failure of MCD can be protected against by primary bleed and feed via the PSVs

- A failure of LHSI can be protected against by the MHSI and MCD, with longer term cooling provided by the EHR [CHRS]
- A failure of MHSI can be protected against by depressurisation (LCD) and LHSI
- ATWS faults are protected by the RBS [EBS] system.

415. The bleed and feed and LCD functions and the EHR [CHRS] and RBS [EBS] system are included within the generic UK HPR1000 design as DEC-A protection measures, and I have discussed them within Section 4.4 of this report.

416. In the event of an SB-LOCA, safety injection is actuated by pressuriser pressure Low 3 signal. The RP had identified that if the sensor were to fail then, while reactor trip would be triggered by Hot leg Pressure Low 1, there would be no diverse signal available for safety injection actuation. Four potential options to address this shortfall were considered by the RP in Ref. 81. Modification M61 to the generic UK HPR1000 design has introduced a new safety injection signal on hot leg pressure low 3 on the KDS[DAS] to protect against this signal failure. The effectiveness of the diverse signals has been demonstrated in Ref. 76 which shows that the core remains covered from the initiating event to the safe state. This document is referenced from the Fault Schedule (Ref. 10) and as such I am content that the modification has been appropriately integrated into the generic UK HPR1000 safety case.

417. For any SB-LOCA with loss of LHSI or a 2.5cm SB-LOCA with loss of MHSI the RP has demonstrated that the core remains covered (Ref. 79). For a larger (5cm) SB-LOCA with loss of MHSI and for a SB-LOCA with a failure of MCD the RPV level drops below the top of the core but the temperatures remain below the acceptance criteria.

418. I am content that the sequences identified by the RP represent a robust challenge against the potential failures of the primary safety systems and provide a good demonstration of the fault tolerance and defence in depth of the generic UK HPR1000 design. In my opinion the consideration of these additional sequences is consistent with UK practice and the expectations of SAPs FA.6 and NS-TAST-GD-006 (Ref. 4).

Consequential LOCAs as a result of Stuck Open PSV

419. The final part of my assessment of SB-LOCA was to consider the effects of a consequential LOCA as a result of a suck open PSV following an intact circuit fault. Several fault sequences have the potential to lead to an over-pressurisation of the primary circuit. The PSVs are included within the design to provide overpressure relief. ONR's SAPs (FA.6 and supporting paragraph 631) sets the expectation that sequences with a frequency of ~10^{-7} per annum are considered with DBA. Within the Level 1 PSA (Ref. 82) the consequential failure probability for the PSV to close on demand following operation is predicted to be [redacted] per demand. I therefore expected that any intact circuit initiating fault or fault sequence with a frequency greater than 1x10^{-3} per year that causes a PSV to lift should be assumed to result in a consequential LOCA that needs to be considered with DBA.

420. The PCSR considers spurious opening of a PSV as a DBC-2 event and other, more onerous LOCAs are assessed within the PCSR. However, in the case of a consequential LOCA case the initiating event is itself a fault condition which may result in more onerous initial conditions when compared with the nominal initial conditions assumed for the spurious opening of the PSV event and the other LOCA events. As part of my assessment I therefore sought confidence that the RP has undertaken sufficient analysis to demonstrate that there is not an escalation of consequences should the PSVs fail to open or reseat.

421. In response to the above the RP has (RQ-UKHPR1000-0746, Ref. 6)) reviewed the frequent intact circuit DBCs for which PSVs may lift and the plant conditions and

compared those against the conditions experienced during a SB-LOCA. From this the RP has identified that a Feedwater System Small Piping Break presents the most onerous conditions for a frequent intact circuit fault where a PSV fails to reseat. However, from consideration of these conditions and the transient progression the RP considers that this sequence can be bounded by the SB-LOCA scenario.

422. On the basis of my review of the additional information provided (which has subsequently been incorporated into the final safety case), I am content that the RP has adopted a reasonable approach to the consideration of stuck PSVs following an intact circuit fault and I am satisfied that the consequences of such a scenario would not be more onerous than those of a SB-LOCA.

Radiological Consequences

423. The RP has undertaken analysis of the radiological consequences of a SB-LOCA and used it as a representative fault for some other DBCs (I have discussed these in the relevant sections of this report). The RP has calculated off-site consequences of 5.93×10^{-1} mSv (infant) (Ref. 58) which is below ONR's Target 4 BSL. The RP has considered the main contributors to these consequences and has concluded that there are no reasonably practicable measures to further reduce them (Ref. 61). From my review of Ref. 61 I am content to support this conclusion and I discuss the general aspects of the demonstration of ALARP within Section 4.8 of this report.

4.3.5.2 IB-LOCA

424. The IB-LOCA fault is classified as a DBC-4 event and is defined as breaks greater than 5cm up to the surge line diameter of [redacted]cm. The RP's analysis is contained in Ref. 83. The IB-LOCA is characterised by a rapid depressurisation of the primary side due to the large amount of coolant ejected into the containment through the break. The analysed IB-LOCA can be divided into three phases similar to LB-LOCA scenarios because of the relatively large break cross section area with respect to the cold leg pipe:

- Blowdown.
- Refill.
- Reflood.

425. Different phenomena such as flow stagnation and reversal, water entrainment and steam binding, as well as counter-current flow limitation, are related to each of the phases, and have an influence on the plant behaviour and the coolability of the core. The distribution of pressure losses and flow resistances in the reactor coolant system are two of the most important parameters that influence the IB-LOCA evolution.

426. Reactor trip is actuated by the Pressuriser pressure low 2 signal if core power is higher than 10%FP or the Hot leg pressure low 1 signal otherwise. MHSI and LHSI are actuated on the Safety Injection signal which is triggered by the pressuriser pressure low 3 signal or Hot let ΔP_{sat} low 1 (at low pressures). Following the safety injection signal MCD is initiated to cool the primary circuit at a rate of [redacted]°C/hr. After reactor trip the residual heat is removed by the break flow, the RIS [SIS] and VDA [ASDS]. The controlled state is achieved when the primary residual heat is removed in this way, core sub-criticality is ensured and core coolant inventory stabilises or increases.

427. The RP consider that the safe state is reached when the sub-criticality is maintained by RBS [EBS] injection and RIS [SIS] is connected in RHR mode. If RHR conditions cannot be met (as there is not enough safety injection flow to compensate for the break flow and flood the hot legs) the LHSI pumps will be switched to inject into both hot and cold legs simultaneously. This limits the containment pressure increase in the long

term, prevents boron precipitation inside the core and prevents boron dilution inside the IRWST.

Transient Analysis

428. To identify the most limiting cases, the RP has undertaken a range of analysis in Ref. 83. The RP has considered three main cases:

- Case 1 State A from the initiating event to the controlled state
- Case 2 State A from the controlled state to the safe state
- Case 3 State B from the initiating event to the controlled state.

429. Within Ref. 83 the RP argues that it is not necessary to analyse State B from the controlled state to the safe state as the safety functions are the same as those from State A and the decay heat to be removed will be lower. From examination of these arguments I am content to agree with the RP's reasoning.

430. For both of the short-term analysis (to the controlled state) the RP has undertaken sensitivity studies on the break size and the fuel burn up. For the long-term analysis (to the safe state) the RP has used the most limiting scenario identified from the short-term analysis as the starting conditions. I am content that this is appropriate and I welcome the range of sensitivity studies that have been carried out.

431. The original submission provided by the RP assumed a single failure of one EDG for the analysis of the initiating event to the controlled state. This results in a loss of one MHSI and LHSI pump in one loop in addition to those lost as a result of the break location. As a result one MHSI pump, one LHSI pump and two accumulators were available for safety injection. Following my request for the RP to include consideration of non-return valves (check valves) within the determination of the single failure the analysis within Ref. 83 has been updated and considers failure of the check valve on the intact loop injection line. As such, only one safety injection line (with one MHSI pump, one LHSI pump and one accumulator) is taken into account in the updated analysis.

432. The success of the IB-LOCA protection relies heavily on the performance of the MCD function. I have therefore sought assurance of the integrity of this function to gain confidence that the check valve is the most limiting single failure. MCD is an FC1 safety function and is delivered by the simultaneous opening of the F-SC1 VDA [ASDS] valves and the reduction in pressure setpoint to maintain the cooling rate. The system design manual for VDA [ASDS] (Ref. 84) confirms that each train is capable of discharging at least [redacted] of the nominal steam rate and therefore tolerant of a single failure within one VDA [ASDS] train. It was not however clear that the C&I which controls the MCD function is also single failure tolerant. In response to a query on this point the RP has confirmed (RQ-UKHPR1000-1249 Ref. 6) that the RPS architecture is designed to satisfy the single failure criterion and that specifically that the architecture that delivers the MCD function complies with this. Through discussion with ONR's C&I Inspector I am satisfied with the additional clarification that has been provided and that this a random single failure does not need to be assumed for this system.

433. The results show Case 1 is the most limiting and that the maximum PCT increases with break size but remains well below the criteria of 1204°C. The oxidation ratio also remains well below the limit for all of the burnups considered.

434. From my review of Ref. 83 I am content that the fault sequences are clearly described and that the RP has undertaken an appropriate range of sensitivity studies to identify the most onerous scenarios. Whilst the initial and boundary conditions are clearly stated, there is little explanation of why these are conservative. Through discussion of

a sample of some key parameters (including pressuriser level, SG level and MCD delay times) (RQ-UKHPR1000-1733, Ref. 6) I have gained confidence that the RP has undertaken a range of studies to support the choice of analysis conditions, even though they are not explicitly referenced from the analysis report.

Confirmatory Analysis

435. To gain further confidence in the RP's analysis methods and to gain assurance of the margins to the acceptance criteria I commissioned my TSC to undertake confirmatory analysis of the most limiting IB-LOCA identified in Ref. 83 against the fuel criteria.

436. The TSC analysis of IB-LOCA is reported in Ref. 75. My TSC analysed the intermediate break on the cold leg (27.5 cm equivalent diameter) from initiating event to controlled state from State A (short term analysis). The TSC modelling used similar initial and boundary conditions and system performance assumptions to those used by the RP in Ref. 83. The TSC noted the following discrepancies between the analysis using ATHLET and the RP's analysis using LOCUST-K:

- There is a higher break mass flow in the TSC analysis in the early LOCA phase. The TSC uses the ATHLET specific discharge model CDR1D to calculate the break flow, whereas the RP uses the 0D Moody model, which tends to overestimate the critical flow of low-quality two-phase mixtures and of subcooled flow.
- Primary side depressurisation in the TSC analysis leads to a fast power reduction due to density reactivity feedback. Whilst the depressurisation is slightly faster in the RP's analysis it does not lead to a power reduction, as the RP has not considered the effect of coolant density reactivity feedback.
- Concerning the reactor trip:
  - In the TSC analysis reactor trip is initiated on the Hot leg pressure (WR) < low1 signal. In the RP's analysis the reactor trip is on Pressuriser pressure low 2; this occurs later (at t = 7.5 s) in the TSC calculation.
  - The signal High negative neutron flux rate was set as unavailable in the TSC analysis to allow comparable reactor trip timings.
- Reactor and turbine trip signals occur simultaneously in the TSC analysis but the RP's results suggest a delayed turbine trip signal.
- My TSC calculates a lower safety injection flow rate mainly due to higher primary pressure. RIS [SIS] injection is influenced by steam binding in SG-U-tubes and counter-current flow limitation in hot legs. Both phenomena cause an intensive steam production in the core, which results in an increase in pressure drop along the steam flow path and an increased pressure in the core region compared to the pressure at the break or in the downcomer. This local pressure build-up above the water/vapour mixture level in the core has a delaying effect on the refilling of the core.
- Concerning the secondary side:
  - The RP calculates a higher SG pressure compared to the TSC in the early LOCA phase. This is due to the higher energy level in the primary system during the first seconds after the occurrence of the break in the RP's analysis.
  - MCD signal is triggered later in the TSC's analysis because of the required delay (8s) from the moment that safety injection signal occurs to the moment that MCD is entirely actuated.
  - In the TSC analysis the SGs are isolated due to the reactor protection system signal Containment pressure > MAX4. The RP's results do not

indicate a closing of MSIV. Different behaviour of pressure in SGs compared to the RP are influenced by condensation effects when the ASG injection starts and thermal mixing effect in riser (only in SG1 and SG3).

- Concerning the PCT:
  - My TSC calculates critical heat flux conditions on the hot rods in the early LOCA phase, causing the fuel rods to experience DNB and a sharp temperature excursion. The PCT1 reaches a maximum value of 992°C. Because of the slightly higher void fraction and lower mass flow rate in hot channel, the TSC calculates earlier DNB condition on the hot rod compared to the RP.
  - Core uncovery with core heat-up is calculated in both the RP's and the TSC's analysis. My TSC calculated a maximum value of 528 °C for the max. peak cladding temperature (PCT2), the RP's PCT2 value was [redacted] °C.
- Fuel pellet temperature at the beginning of the analysis shows a lower value ([redacted] °C) by the RP with respect to the TSC (1970 °C). Both the TSC and the RP calculate the fuel temperature at the centre of the pellet at the elevation of PCT, where the maximum temperature is reached. Such difference would suggest that slightly higher values of the energy stored in fuel pellet have been calculated by the TSC in steady state and during the early LOCA phase than the RP. After the break opening the energy stored is higher in the RP's analysis till the triggering of reactor trip because of the lack of neutronic density feedback with respect to the TSC results.
- The Average Coolant Temperature (ACT) of the primary side decreases in my TSC's analysis slower than in the RP's and no oscillations are observed in the TSC results due to thermal mixing phenomena calculated by ATHLET in the cold leg.

437. In conclusion, my TSC was content that the confirmatory analysis results for IB-LOCA show that the initial and boundary conditions selected by the RP are conservative, especially regarding core related assumptions such as axial power profile, peaking factors and decay heat data, which were selected to maximise primary heat and penalise core heat-up. This provides me with confidence in the RP's choice of these conditions.

438. However, whilst PCT remains below the acceptance criteria limit for both the TSC and the RP's analyses, there are significant discrepancies in the magnitude of the first PCT peak (PCT1). From discussion with the RP and my TSC, differences in Critical Heat Flux (CHF) correlation as well as post-CHF heat transfer models may be the cause for the differences in the calculated Heat Transfer Coefficient (HTC) in saturation film boiling regime, and thus of the maximum PCT1. The HTC value in the RP's analysis is about one order of magnitude higher than that by my TSC, which suggests different post-CHF models and different HTC correlations for saturated film boiling condition. Differences in adopted CHF-correlation could explain the different value of DNBR calculated by my TSC and the RP in the steady state.

439. My TSC therefore recommended that the RP should undertake additional studies into PCT1 and that ONR should seek evidence of the adequacy of the RP's post-CHF heat transfer model (as my TSC did not have access to the validation of the RP's models). These points are discussed in turn below.

440. Following discussion of the results of the TSC's analysis, the RP confirmed that the analysis reported in Ref. 83 is penalised to maximise the PCT2 peak, which it considers dominant. The RP nevertheless agreed to undertake additional studies to investigate the sensitivity of the PCT1 peak to key analysis assumptions. These studies are reported in Appendix A to Ref. 83 and include:

- Break flowrate.
- Initial fuel temperature of hot spot.
- Core power.
- Core axial power profile.
- Fuel cladding deformation model.
- CHF correlation model.
- The cross flow between average channel and hot channel.

441. These sensitivity studies have been compared by the RP to the base analysis of the short-term analysis from State A. The results show that the PCT1 calculated by the RP is not sensitive to these assumptions and for all of the cases the maximum PCT1 remains below the PCT2 calculated in the base case. I welcome the addition of these sensitivity studies and consider that they represent a comprehensive set of studies on key modelling assumptions. The use of such sensitivity studies is consistent with ONR's expectations that a change in a parameter used in design basis assessment will not lead to a disproportionate increase in consequences (SAPs FA.7, para. 638.). Whilst the studies do not explain the differences in the prediction of PCT1 between GRS and the RP, they do give me additional confidence in the robustness of the RP's analysis.

442. The second recommendation from my TSC related to the adequacy of the RP's post-CHF heat transfer model. However, I have established that this model is described in the validation report for LOCUST (Ref. 17) which explains that the LOCUST-K implements the [redacted] correlations for post-CHF boiling, in accordance with the requirements of US NRC 10 CFR 50. These are well-established correlations and I have no concerns with their use in the prediction of PCT.

443. Overall, I am content that the RP has provided an adequate assessment of IB-LOCAs that meets the expectations of the SAPs FA.4, FA.5 and FA.6. I am satisfied that Ref. 83 has demonstrated that the UK HPR1000 can be taken to a controlled state with a single train of RIS [SIS] and that significant margin to the acceptance criteria is maintained (SAP FA.7). I am also satisfied that a safe state can be reached using the MCD function and RBS [EBS] to maintain control of reactivity.

4.3.5.3 LB-LOCA

444. The RP defines a LB-LOCA as an accident with the break size of equivalent diameter over 27.5 cm and up to a double-ended guillotine break of the Main Coolant Line (MCL). In the original submissions this fault was categorised as a DBC-4 fault. However, the RP's case has developed during the course of GDA. The MCL is now classified as a HIC and the RP argues that the gross failures of MCL can be discounted as a design basis fault (Ref. 85). As a result, LB-LOCA is not included within the DBC list.

445. In the generic UK HPR1000 safety case LB-LOCA is instead categorised as a "specific studies" event. The RP defines the term "specific studies" as an initiating event which cannot be bounded by the extant DBC and DEC-A events but requires deterministic safety analysis to demonstrate the resilience of the plant and the absence of 'cliff edge' effects.

446. SAP FA.5 sets ONR's expectations for which faults should be included within the design basis. It notes that failures of SSCs for which appropriate specific arguments for preventing the initiating fault have been made need not be included. As the MCL has been classified as HIC then the RP's position is generally consistent with ONR's expectations as set out in FA.5.

447. However, just because a fault is not included within the RP's design basis does not remove the requirement for an adequate safety case. ONR NS-TAST-GD-0051 (Ref. 4) sets out the expectation that the evidence used within a safety case should be of sufficient quality, commensurate with the magnitude of potential risks and complexity of the system of interest and that an adequate demonstration of key safety claims usually needs the support of multiple legs with different types of evidence.

448. In addition, IAEA guidance (paragraph 3.20 of SSG-2) states that significant faults such as LB-LOCA should not be excluded from the category of design basis accidents unless careful analysis and quantitative assessment of their potential contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release, indicate that they can be excluded.

449. Noting this guidance and the key role of the LB-LOCA analysis in defining performance requirements for the RIS [SIS] system and the containment I have therefore sought clarity on the additional arguments and evidence available in the safety case to strengthen the case for excluding it from the list of DBCs.

450. In response to discussions on this, the RP has produced Ref. 85 which is essentially a head document for the LB-LOCA safety case which summarises the various analyses which have been undertaken. The principal arguments within this document are:

- The main coolant line is classified as HIC. The RP has undertaken analysis of the direct and indirect consequences of a LB-LOCA and concluded that this classification is a reasonably practicable measure to reduce the risks arising from the LB-LOCA ALARP.
- Transient analysis has been undertaken for LB-LOCA using the US NRC 10 CFR 50 Appendix K analysis rules. This analysis is used to inform
    - the performance requirements of the safety injection system;
    - the containment design requirement; and
    - the environmental requirements for equipment qualification.
- LB-LOCA with additional failures of safety injection systems have been considered within the Severe Accident Analysis which demonstrates the effectiveness of safety features specifically designed for severe accidents.
- The Level 1 and Level 2 PSA conclude that the LB-LOCA does not contribute disproportionately to the overall plant risk of a large radiological release.
- Analysis to demonstrate that a coolable geometry will be maintained within the fuel assemblies during a LB-LOCA has been undertaken for the UK HPR1000 reference plant.
- The radiological consequences of a LB-LOCA are acceptable with regard to deterministic criteria.

451. I am content that this scope of work is adequate to meet the ONR's expectations for a balanced safety case (NS-TAST-GD-0051 51, Ref. 4) and the expectations of IAEA SSG-2. ONR's assessment of the evidence underpinning the arguments regarding HIC, the SAA and the PSA are reported within the Structural Integrity, SAA and PSA assessment reports respectively (Refs 32, 86 and 24) and these assessments are content with the claims made by the RP. ONR's assessment of the ability of the core to

maintain a coolable geometry during a LB-LOCA has been considered within the Fuel and Core assessment report (Ref. 20) and an Assessment Finding has been raised in relation to clad ballooning. I have considered this in coming to an overall view on the adequacy of the safety case and I have discussed their significance below.

452. My assessment reported in this section has focussed on the short-term transient analysis to demonstrate the effectiveness of the safety measures and the radiological consequences of this fault. The long-term analysis consists of mass and energy calculations to show that long term cooling and control of criticality can be ensured by switching the safety injection flow into the hot and cold legs simultaneously. The calculations reported in Ref. 87 show that there is significant margin for the operators to perform the manual switchover of safety injection before the relevant criteria are met. As such this has not been a significant focus of my assessment.

453. The longer-term analysis is also important for demonstrating the adequacy of the containment following a LB-LOCA. This has been analysed separately by the RP using different methods and my assessment of this is reported separately in Section 4.3.11 below.

Transient Analysis

454. The analysis of LB-LOCA has been undertaken using LOCUST-K and uses conservative initial and boundary conditions and assumptions on system performance. My assessment of LOCUST-K is reported in Appendix 1 to this report. Similar to the other fault analysis, the RP's analysis approach is to split the transient into the short term and the long term to assess the faults against different acceptance criteria. The analysis results (Ref. 87) show that all acceptance criteria are met.

455. The LB LOCA causes the RPV water to flash to steam. The increased voiding causes a neutronic shutdown. When combined with the loss of inventory the decreasing RPV water level leads to uncovery of the fuel. This phase is often called the blowdown phase.

456. The RIS [SIS] system will inject boronated water into the reactor coolant system to replace the water lost through the break. While some of this water may bypass the RPV, the water that does not will begin to refill the RPV. However, during this refilling phase the core has a stationary steam atmosphere. This has a poor heat removal capability, so the fuel's temperature rises significantly. The phase of a LOCA where the water level increases above the bottom of fuel is known as the reflood phase. During the reflood, the rising water level quenches the fuel rods and continues to rise until the long-term cooling is assured by the RIS [SIS] flow.

457. The principal safety systems and signals are:

- Reactor trip on pressuriser pressure low 2 signal.
- Safety Injection on pressuriser pressure low 3 signal.
- Accumulators injection of borated water when the primary circuit pressure reduces to the accumulator setpoint.
- Containment isolation is triggered by either the containment Pressure High 1 signal or the Safety Injection signal.

458. The RP has considered the most onerous initial operating state in its analysis, including:

- assuming full power operation plus uncertainties to maximise the decay heat
- delay safety injection via the delay of reactor trip to penalise the heat removal condition at the early stage of the transient; and

- the minimum initial reactor primary circuit water inventory and the safety injection flow rate to penalise primary coolant inventory.

459. In my opinion, the RP's use of the most onerous initial plant conditions is consistent with the analysis performed for design basis faults. As with the IB-LOCA analysis the RP has updated the LB-LOCA analysis during GDA to consider the failure of the check valve in one RIS [SIS] train as the limiting single failure. In this way the whole safety injection train (including MHSI, LHSI and accumulator) is assumed to be unavailable. I am content that this is an appropriate assumption to support a demonstration of the fault tolerance of the generic UK HPR1000 design.

460. For LB-LOCA fault, the break size and break location are two critical parameters which have a significant influence on the fault progress and severity of the consequence.

461. In Ref. 87 the break is assumed to be located on cold leg safety injection point, between the reactor coolant pump and the RPV inlet. The break is assumed to be in the loop containing the pressuriser. This break location presents the worst cooling condition to the core as the safety injection flow in the broken loop and pressuriser water is lost as it is assumed to be discharging directly through the break. I am satisfied that the assumption of break location is conservative for this fault.

462. In the generic UK HPR1000 safety case, the base case for the short-term transient analysis is assumed to be the double ended guillotine break. The RP has undertaken a break spectrum analysis, following the US NRC's safety approach. The break sizes considered ranging 40% to 100% of the double-ended guillotine break size, with a 10% interval. In total, 7 cases are considered in the break spectrum analysis. From this the RP has established that 70% of the double ended leg break is the most limiting break size for the blowdown stage and 50%for the refill and reflood stage. The RP has then carried these break sizes forward into other sensitivity studies.

463. These several sensitivity studies have been performed by the RP to identify the conservative assumptions for those parameters which are either difficult to make by engineering judgment or may have a significant influence on the fault progress in different transient phases. These parameters include:

- initial average RCP [RCS] temperature
- initial ACC water temperature
- ACC water discharge rate
- initial MSHI and LHSI injection water temperature
- reactor core burnup
- axial power shape

464. A combination of the six parameters above, together with the break size, are analysed by the RP to ensure a conservative calculation in respect of these phenomenon to identify the worst peak cladding temperature during the blowdown, refill and reflood phases during the short-term stage. The RP calculates that for the limiting cases, all acceptance criteria are met in the short-term analysis with a maximum PCT of [redacted] °C.

465. I am satisfied that the use of a break spectrum analysis and sensitivity studies to ensure conservative results is consistent with the expectations of NS-TAST-GD-006, FA.6 and FA.7. Whilst the RP does not consider a LB-LOCA to be either a DBC or a DEC-A event, in my opinion, noting the conservative assumptions used, the use of LOCUST-K and the same acceptance criteria as the other LOCA faults, the analysis is consistent with the approaches used for DBC events and the results can be considered as conservative. I am satisfied that this is appropriate to demonstrate the adequacy of the RIS [SIS] to protect against this fault.

Overall Safety Case

466. To form an overall view on the adequacy of the case for LB-LOCA and the demonstration of ALARP, it has been necessary for me to consider how the transient analysis discussed above supports and is supported by the other arguments within the LB-LOCA safety case.

467. As noted above, ONR's Fuel and Core assessment (Ref. 20) has concluded that there are shortfalls in the demonstration that a coolable geometry will be maintained during a LB-LOCA. Firstly, the evidence that the forces that the core will experience will not challenge the structural integrity of the fuel assemblies is based upon the reference plant and only a summary of the evidence has been provided during GDA.

468. Secondly, and more significantly for my assessment, Ref.20 has concluded that there is a shortfall in the predictions of flow blockage that could result from the predicted levels of clad strain due to ballooning in LB-LOCA. As a result, AF-UKHPR1000-0005 has been raised which requires adequate analysis of the impact of flow blockage due to clad ballooning.

469. To form a view on the significance of this shortfall and the implications for the conclusions reported in Ref. 87 I have considered other aspects of the LB-LOCA safety case summarised in Ref. 85:

- The ONR Structural Integrity specialists have sampled and assessed the RP's arrangements for developing and implementing HIC safety cases (Ref. 32). Whilst the Structural Integrity assessment has raised a number of Assessment Findings, the Structural Integrity specialist concludes that the RP has provided a suitable and sufficient Structural Integrity safety case for the purposes of GDA, and that any identified shortfalls related to the completeness of evidence presented can be more appropriately dealt with during licensing.
- ONR's assessment of the SAA measures has concluded that they are adequate to mitigate the consequences of a LB-LOCA with failures of the RIS [SIS] (Ref. 86).
- ONR's assessment of the PSA supports the RP's argument that LB-LOCA is not a significant contributor to plant risk (Ref. 24). ONR's assessment also noted that the analysis supporting the PSA has been conducted on a best-estimate basis and that local fuel damage would not be likely to significantly alter the risk estimates.

470. I am content to judge that these conclusions give confidence that a LB-LOCA is a very unlikely event and that the overall safety case for this fault as presented in Ref. 85 is not undermined by the conclusions of Ref. 20.

471. To further understand the significance of clad ballooning, at ONR's request the RP has provided some sensitivity analyses on the radiological consequences assuming that there is some core melt during LB-LOCA. The RP has calculated the consequences assuming between 0% and 100% core melt (response to RQ-UKHPR1000-1742, Ref. 6) and 100% cladding damage. For 100% core melt, the RP predicts off-site doses of 113 mSv to an infant, with adult doses of approximately 49 mSv, assuming that mitigation measures such as containment and filtration function correctly.

472. A comparison against Target 4 of the SAPs would suggest that the BSL of 100 mSv is marginally exceeded for infants. However, this target is met for all cases up to 50% core melt case (the limiting infant doses are 97.4 mSv). It should also be noted that the Target 4 BSL of 100 mSv is only applicable for fault frequencies between 10^{-4} pa and 10^{-5} pa. Therefore, in my opinion, if some fuel damage were to occur following a LB-LOCA as a result of the shortfalls identified within Ref. 20 there would not be a step

change in consequences. After careful consideration of the above factors, I am content to judge that the safety case for LB-LOCA is adequate for GDA and that there are no fundamental shortfalls with the design of the safety systems. However, AF-UKHPR1000-0005 will need to be addressed before it can be concluded that the risks are reduced ALARP.

Modification to MCL Geometry

473. As part of the case for the MCL as a HIC component, the RP submitted modification M51 during GDA to modify the geometry of the MCL (Ref. 88) to improve access for inspections. The RP has not updated its transient analysis as it claims that the modification will only have a minor influence on the results. I have sought additional information to support this claim. The response to RQ-UKHPR1000-1613 (Ref. 6) shows that the impact is likely to be minor and will not invalidate the conclusions of Ref. 87. I am therefore satisfied that the RP has submitted adequate analysis during GDA and that the implications of the modification of the MCL geometry can be confirmed during normal business as part of detailed design.

4.3.5.4 SGTR

474. A steam generator tube rupture (SGTR) is a particular type of SB-LOCA in which the primary coolant leaks into the secondary side of the steam generators which leads to an increase in secondary pressure, and a potential release of radioactivity via the secondary side relief valves.

475. The RP has identified 4 SGTR faults:

- SG tube rupture (one tube) (State A, B and C)
- SG tube rupture (two tubes in one SG) (State A, B and C)
- Multiple SG tubes rupture (10 tubes) (State A)
- SGTR (1 tube) with VDA [ASDS] stuck open in the affected SG (State A)

476. The first and second of these faults have been categorised by the RP as DBC-3 and DBC-4 respectively. The last two fault have been categorised as DEC-A events. I have chosen to sample the first fault in detail, noting that as a frequent fault the RP has had to consider the diverse means of protection. I have considered all four of these faults to inform my assessment of the SGTR ALARP case.

SGTR Overview

477. When an SGTR fault occurs it leads to a decrease in primary circuit pressure. A reactor trip is triggered by either the pressuriser pressure Low 2 signal when the reactor is operating at full power, or a SG level high 1 signal generated from the affected SG when the reactor is operating at a low power condition. The reactor trip automatically trips the turbine and the SG pressure rapidly increases. Isolation of the main feed water control system full load lines for all steam generators are initiated automatically following the reactor trip.

478. After reactor trip and turbine trip, the secondary pressure increases rapidly to reach the setpoint of the Atmospheric Steam Dump System (VDA [ADS]). If the Turbine Bypass System (GCT [TBS]) is unavailable, then contaminated steam will be discharged to the atmosphere when the VDA [ADS] pressure setpoints are reached. The protection against the loss of primary coolant is the same as for SB-LOCA (described in sub-section 4.3.5.1).

479. The controlled state is reached when the MHSI injection and RCV [CVCS] (if available) are able to match the SGTR flow rate. The RCV [CVCS] charging line is isolated

automatically upon receipt of the SG level (narrow range) high 2 signal after the completion of MCD. However, at this point the affected SG continues to fill with contaminated water and radioactivity release to the atmosphere continues.

480. From the controlled state, the affected SG is identified and isolated automatically (or manually if the operator can respond before the high SG level setpoint is reached). The isolation involves manually raising the VDA [ADS] setpoint above the MHSI shutoff head (but below the Main Steam Safety Valve (MSSV) pressure setpoint) and closing the Main Steam Isolation Valve (MSIV) and the Emergency Feedwater system (ASG [EFWS]). The isolation of the affected SG causes the flow via the break to increase the pressure in the affected SG. Once the primary and secondary side of the affected SG pressures equalise, the flow via the break is terminated.

481. The RP defines the safe shutdown state as a state where the affected SG is isolated and one safety injection system train is connected to the RCS in RHR mode. When the reactor coolant temperature is below 180°C, the MHSI is manually stopped and the operator performs final depressurisation via the affected SG until the RHR conditions are reached. However, if the affected SG water level is too high, the operator needs to first manually open the transfer line between the affected SG and its partner SG to lower the level. This prevents overfilling the affected SG and the risk of a large activity release to atmosphere.

482. The primary safety systems claimed to protect the SGTR fault, trip signals to actuate the safety measures, safety system actuation mode (auto or manual) and C&I platform, alongside the safety function required to be delivered (fundamental, high level and low level) and the category of the safety function are summarised in Table 37 of the fault schedule (Ref. 10).

Transient Analysis

483. The RP has performed two separate analysis cases to assess the SGTR against two different acceptance criteria. The objectives of the RP's safety analysis are to calculate the maximum radioactivity release (Case 1) and to demonstrate a margin to steam generator overfill (Case 2). The transient analyses for these two cases are presented in Ref. 89. The RP has performed the analyses using the LOCUST code. The assessment of the suitability of LOCUST code is presented in Appendix 1 of this report.

484. In Case 1, the analysis results show that the total steam released into the environment is about [redacted] tonnes and that the reactor core remains covered during the transient with a water level margin over [redacted] m (from the top of active core). The case 2 results demonstrate that the reactor core remains covered during the fault progression and the minimum steam space is [redacted] m^3, which indicates no overfilling occurs during the fault transient. I am content that the RP's selection of these cases for analysis is appropriate and consistent with the expectations of SAP FA.6 and that they should provide a robust demonstration of protection available against this fault (SAP FA.4).

485. Based on the analysis results, the RP concludes that for design basis SGTR with one tube rupture there will be no fuel damage, the controlled state can be achieved using only F-SC1 systems, and the safe shutdown states using only F-SC1 and F-SC2 systems.

Assumptions and Uncertainties

486. For case 1, the maximum flow rate of MHSI and RBS [EBS] and the minimum flowrate of ASG [EFWS] for all three SGs is assumed to maximise the radioactivity release into the environment. For case 2, the performance assumptions of F-SC1 and F-SC2

systems are the same as the case 1 except that the maximum flowrate of ASG [EFWS] is assumed for the affected steam generator to maximise the potential for overfill of the affected SG.

487. The correct performance of F-SC3 safety system and non-safety equipment is not assumed where this would alleviate the consequences. For example, in case 1, the correct performance of the pressuriser heaters, GCT [TBS] and pressuriser sprays are not credited.

488. Within Ref. 89 the RP has considered conservative uncertainties on equipment characteristics and actuation of the control signals. The uncertainty range considered for initial conditions appear to be typical of other PWR plant safety cases. For example, 2% of rated reactor power and 10% of the normal narrow range SG water level are assumed. The RP then applies the uncertainty range value in such a way it is biased on the side which could penalise the analysis results with regards to the acceptance criterion in question. For example, in case 1, the initial power is assumed to be 102% (100% + 2%) and the initial SG water level (NR) of 40% (50%-10%).

489. Through the examination of the assumptions made of the performance of safety system, safety related system and non-safety systems, I am satisfied that the RP's safety analysis approach and assumptions made are aligned with the expectations of ONR SAP FA.6.

Operator Actions

490. In the generic UK HPR1000 safety case, the RP claims a number of operator actions to reach a safe state following an SGTR. ONR SAP FA.6 (para 633.) sets out the expectation that operator action can be claimed as part of the safety measures if sufficient time is available and adequate information for fault diagnosis is presented. This principal also states that appropriate analysis should be carried out on any claimed actions (see SAP EHF.5).

491. In Ref. 89, a number of operator actions (initiation of MCD, start-up of one MHSI train, start 2 RBS [EBS] trains, isolation of RCV charging line) were assumed to occur simultaneously, 30 minutes after the break. This assumption is consistent with the RP's design basis rule that no human intervention is required in the main control room (MCR) for 30 minutes from the start of the safety system initiation, and no earlier than 1 hour for local manual action.

492. However, there was no consideration as to whether there is sufficient time available to allow the operator to take those actions. In addition, it is difficult to justify whether the assumption of a number of operator actions taken simultaneously is conservative with regard to the acceptance criterion in question. This is because each operator action may affect the fault progress in a different way, some of the effects re-enforce each other while some of them cancel out. Therefore, I requested the RP to substantiate the claims made on the operator within the transient analysis.

493. In response, the RP performed a task analysis on the claimed operator actions which is documented in Ref. 90. I have worked closely with ONR's Human Factor specialist to support their assessment of this report which is recorded within ONR's Human Factor's Assessment Report (Ref. 55). Ref. 90 presents updated timings for the start and completion of the operator actions.

494. The RP has presented revised Case 1 analysis results, based on these updated timings, Ref. 91. In this new analysis the steam release has increased to [redacted] tonnes. I am content to judge that the RP's revised SGTR safety analysis is consistent with the expectation of ONR SAP FA.6 and NS-TAST-GD-006 (Ref. 4) with regards to the

consideration of operator actions in DBA transient analysis. I have considered the effect of this on the radiological consequences below.

SGTR Fault Detection

495. In the SGTR fault analysis, the RP assumes that SGTR is detected by a high activity in the plant radiation monitoring system (KRT [PRMS]) signal. However there is no detailed information about the SGTR fault detection systems in either the fault schedule (Ref. 10) or the analysis (Ref. 91).

496. In response to the RQ-UKHPR1000-0612 and RQ-UKHPR1000-1626 (Ref. 6), the RP has clarified that in the generic UK HPR1000 design there are three means of detection of an SGTR fault. The RP also claims that the three different types of monitoring have adopted an appropriate design and equipment installation rules to eliminate CCFs. These three fault detection systems are briefly described below.

- Radiation Monitoring of Main Steam System (VVP [MSS]) Radiation Monitoring of Main Steam System is a F-SC1 classified safety system and its design can fulfil redundancy requirement and meet the single failure criterion requirement. Two redundant monitoring channels are arranged outside each main steam line of VVP [MSS] to continuously monitor the radioactive concentration of N-16 and noble gases.
- Radiation Monitoring of Steam Generator Blowdown System (APG [SGBS]) is a F-SC2 classified system. Normal range and high range monitoring channels are installed on the sampling branches for steam generator blowdown, and each steam generator blowdown is provided with one normal range and one high range channel.
- The monitoring channel of the Condenser Vacuum System CVI [CVS] is F-SC3 classified, designed to continuously monitor radioactive concentration of the exhaust air of CVI [CVS] to detect the leakage from steam generators at an early stage.

497. In the generic UK HPR1000 safety case, the SGTR fault detection is claimed to alert the operators and aid the operators in the fault diagnosis. It is not claimed to initiate any safety systems to protect or mitigate the SGTR fault. The fault detection systems are however important for protecting against less serious SGTR faults when the break flow is not significant enough to automatically trip the reactor.

498. Whilst I am content that sufficient information has been provided by the RP for GDA, I consider that additional analysis is likely to be required for smaller SGTR faults where reliance is placed on the operator responding to radiation monitoring to initiate a plant shutdown. This will be needed to inform the development of operating procedures, which I consider to be normal business for the licensee.

Confirmatory Analysis

499. To gain confidence in the RP's analysis of this complex fault, I commissioned my TSC to perform independent confirmatory analysis of the one tube SGTR fault. The confirmatory analysis was carried out using the same initial plant conditions, plant configurations and geometries as the RP's analysis (so far as was possible). The assumptions of rector core decay heat, operation of safety-related systems and non-safety systems are also the same. My TSC performed the calculation using its ATHLET code.

500. The total amount of steam released into the environment calculated by the TSC is 116 tonnes, compared with [redacted] tonnes in the RP's safety analysis. The confirmatory analysis results (Ref. 92) demonstrate a good general agreement with the RP's safety

analysis. Whilst it is encouraging that there is good agreement between the analysis results, the TSC confirmatory analysis has also provided further insights into some phenomena which SGTR fault would experience but were not explained in the RP's safety case.

- My TSC's confirmatory analysis shows that the operation of APG [SGBS] system would remove about 40% of the break flow. An equivalent amount of radioactive material may be removed from the affected steam generator through this system. The TSC advised that assuming the APG [SGBS] system is in operation may be an optimistic assumption regarding steam release.
- The contaminated steam can flow through the main steam header from the affected steam generator to the unaffected steam generators due to condensation effects during the injection of emergency feed water. As a result, the contaminated steam released from the affected SG may be under-estimated.

501. In the RP's transient analysis, the APG [SGBS] system is assumed to be in operation prior to the occurrence of the fault until a trip signal is generated and received to close the APG [SGBS] isolation valve. The trip signal is generated by either the wide range water level low 2 or the start-up of the emergency feedwater system (ASG [EFWS]). In response to RQ-UKHPR1000-1626 (Ref. 6) the RP provided the following clarification:

- The steam header is located downstream of the MSIV. After the turbine trip and before the closure of MSIV, the steam can flow from the unaffected SG to the affected SG and vice versa, depending on the pressure balance between the SGs. The radioactivity level in the affected SG and unaffected SG is different. In source term analysis, it is the steam release from the SG outlet in both affected SG and intact SGs, instead of the steam release via VDA [ASDS] that is used as input for the source term calculation. Therefore, the steam flows between SGs would not lead to an underestimation of the radiological consequence.
- In the UK HPR1000 safety analysis, the APG [SGBS] system is modelled as a boundary condition, without considering the decontamination effect of the APG [SGBS] system as per design.
- The purpose of assuming APG [SGBS] system being in operation is to penalise the break uncovery duration. When the SGTR break is not covered by the liquid in the SG secondary side, a portion of break flow fluid from the SG primary side would flash into steam and then released into the environment directly without considering the water scrubbing effect. This approach would penalise the radiological consequence.

502. Based on the explanation above, the RP concludes that the assumption of APG [SGBS] system operation is conservative with regards to the radiological consequence, and the steam flow from the affected SG to the intact SGs would not lead to underestimating the radiological consequence. I am satisfied with the RP's explanation above which is clear and plausible. It reinforces my assessment conclusion that through SGTR safety analysis, the RP has provided a robust demonstration of engineering design and effectiveness of the safety measures claimed to protect SGTR fault with a high degree of confidence.

Diverse Protection

503. Within the fault schedule (Ref. 10) the RP presents diverse protection for each of the safety functions required to protect against SGTR. Within Ref. 34 the RP claims that sequences involving an SGTR and failure of the reactivity control and heat removal systems can be bounded by similar sequences for SB-LOCA. I am content that this is a reasonable argument.

504. The RP has recognised that there are some shortfalls in the provision of diverse signals to initiate automatic protection but has instead claimed that there is sufficient diversity for each principal signal. This claim has been considered by ONR's C&I assessment report (Ref. 109).

505. The RP has identified a shortfall in the provision of diversity for the containment function. The RP has identified that the Main Steam Isolation Valves (MSIVs) are the only means of isolating the main steam system (VVP [MSS]) and that there is no diverse means of isolation in the event of a CCF of the MSIVs. This is required (in accordance with the RP's rules) following a number of frequent faults (including SGTR, small steam system piping breaks and inadvertent opening of one Steam Generator relief train).

506. The RP has considered in (Ref. 93) two options to reduce the likelihood of a CCF of the MSIVs; mechanical diversity within the MSIVs or different valve type/supplier for the three MSIVs. In Ref. 93 the RP has concluded that introducing diversity via the components within the MSIVs is the most appropriate solution. Whilst the RP has not considered within Ref. 93 whether there is a way to include an independent diverse means of isolating the main steam line (e.g. through additional valves in series) I do not consider this is a significant gap as the implications of such a modification would be substantial and I am not aware of such an arrangement of isolation valves on other similar PWR.

Radiological Consequences and ALARP

507. Although the analysis shows that there is no fuel damage arising from the one tube SGTR there will still be a release of radioactivity from the primary circuit coolant through the secondary circuit relief valves. The amount of radioactivity released will be a function of the total volume of steam released. The quicker the isolation of the affected SG can be achieved, the smaller the release will be.

508. The off-site dose for SGTR fault with one tube rupture was calculated to be about 3 mSv to an infant (Ref. 58), which is above ONR's Target 4 BSL (1 mSv). ONR SAPs paragraph 698 states that it is ONR's policy that a new facility or activity should at least meet the BSLs. ONR's expectation is further clarified in Annex 2 of ONR NS-TAST-GD-005 (Ref. 4) that for new reactor designs, the level of safety must be no less than a comparable facility already working or being constructed in the UK or elsewhere in the world.

509. The RP notes that the off-site dose is dominated by the contribution from ingestion doses and that these would be limited by implementation of a food ban. Without the contribution of ingestion doses the off-site dose are reduced and the RP therefore consider that the relevant RPT-4 and BSL and Target 4 of the SAPs are met. I do not consider that it is appropriate to conclude in GDA that the consequences are acceptable based on the imposition of a food ban for the following reasons:

- The RP would not have any control over a decision to impose a food ban.
- The design should be capable of protecting against faults without reliance on external mitigation measures.
- IAEA SSR2/1 sets an objective that large or early releases (requiring offsite counter measures) are practically eliminated. SGTR is a frequent fault and the current argument does not meet this objective.
- Even if implemented, any food ban would not reduce ingestion doses completely.

510. I therefore sought to understand the dominant factors which influence the off-site release and a justification that the consequences are reduced ALARP. In response,

the RP has submitted Ref. 94, which provides an overview of the main safety arguments and considers options to reduce the consequences of an SGTR. The main arguments from Ref. 94 are:

- The generic UK HPR1000 design has evolved from its original design by incorporating the advanced safety features and the OPEX over the time. Of those safety features, the elimination of high head safety injection and the inclusion of the passive heat removal system ASP [SPHRS] system are particularly relevant to Fault Studies.
- Fault analysis has been carried out in compliance with RGP.
- All acceptance criteria, including RPT-4, against which all design basis faults and beyond design basis faults are demonstrably met.
- Design changes identified through the demonstration of compliance with diverse line protection requirements for design basis frequent faults have been implemented to enhance the safety of UK HPR1000.

511. From my review of Ref. 94 I am satisfied with the RP's approach to the ALARP justification which is broadly consistent with ONR's expectation set out in NS-TAST-GD-005. Through a systematic review, the RP has identified three options for detailed study:

- Option 1: reduce the primary coolant activity operating limit to [redacted] GBq/t Dose Equivalent Iodine (DEI).
- Option 2: food ban following SGTR accident.
- Option 3: change the assumption made in source term calculation of [redacted] GBq/t DEI primary coolant activity to [redacted] GBq/t DEI.

512. The RP has evaluated these three options and concluded that option 3 is the preferred option and re-evaluated the SGTR fault source term and the radiological consequence analysis (Ref. 58) on this basis. The new radiological consequence analysis results show that:

- the off-site effective doses of adult, child and infant are 0.069 mSv, 0.136 mSv, and 0.565 mSv, respectively, which is below RPT-4 BSL (1 mSv) but above the RPT-4 BSO (0.01mSv).
- the on-site dose to workers is 0.236 mSv, which is below RPT-4 BSL (20 mSv) but above the RPT-4 BSO (0.1mSv).

513. As a result, the RP concludes that there are no further reasonably practicable improvements that could be implemented, and thereby the risk has been reduced to ALARP for SGTR fault.

514. I am satisfied that the change in the assumption made in source term calculation from [redacted] GBq/t DEI primary coolant activity to [redacted] GBq/t DEI is an effective way to reduce the radiological consequence however changing this assumption alone does not change the risk unless it is reflected by appropriate operating limits and conditions. This is the subject of AF-UKHPR1000-0165 which has been raised in ONR's Chemistry Assessment Report (Ref. 37).

AF-UKHPR1000-0165 – The licensee shall ensure that the primary circuit activity limit of 5 GBq t^{-1} assumed during Generic Design Assessment is underpinned within the safety case, and shall justify any associated plant or operator actions.

515. The SGTR ALARP justification is further strengthened through the demonstration of defence in depth and resilience. Along with the assessment of the two-tube fault, the RP has presented the following two DEC-A SGTR faults:

- Multiple SG Tube Rupture (10 tubes).
- SGTR (1 tube) with VDA [ASDS] Stuck Open in the Affected SG.

516. The detailed analyses for these two DEC-A faults are documented in Refs 95 and 96. I have not assessed these documents in detail but I note that the RP concludes that the relevant acceptance criteria are met.

517. It is my judgement that the RP has presented a thorough ALARP justification for SGTR faults, on the basis that it is a holistic (cross-discipline) ALARP justification approach, rather than simply based on a single argument of demonstrably meeting acceptance criteria or limits with analysis. I am content that the SGTR fault ALARP justification is broadly consistent with the ONR's expectation set out in NS-TAST-GD-005, however AF-UKHPR1000-0165 will need to be addressed before it can be concluded that the risks from SGTR faults are ALARP.

4.3.5.5 Debris Effects on Safety Injection

518. During DBCs and DEC-A loss of coolant events the RIS [SIS] and EHR [CHRS] are needed to ensure continued core cooling. Water is drawn from the IRWST and injected into the primary circuit or sprayed into the containment during accident conditions. During an accident, materials can be dislodged and swept in to the IRWST along with other "latent debris". This debris impedes heat removal from the core. Early in GDA I established that the RP had not demonstrated that the risks associated with debris effects had been reduced ALARP. RO-UKHPR1000-0027 (Ref. 7) was raised to address this.

519. The terms 'upstream' and 'downstream' effects or factors are terms which are used as shorthand for effects or factors that are in the containment space (upstream) or after the sump screen and in the RIS [SIS] or reactor coolant system (RCP [RCS]) (downstream). The significant upstream related factors are: the choice of insulating material, the mass of latent debris in the containment, cable tray wrapping, debris transport, design basis accidents or design extension condition accidents and the associated debris source term. The significant downstream factors are: the downstream source term (related to filter efficiency), pressure drop over the filter, qualification of the pumps in a debris field, blockage of the fuel assembly intake nozzles and blockage of the EHR [CHRS] spray nozzles.

520. The safety case presented by the RP in response to RO-UKHPR1000-0027 can be summarised as follows:

- The RP has reviewed RGP for aspects related to the recirculation of sump water for safety injection and containment heat removal (Ref. 97).
- The RP has identified the accidents sequences and safety functions that are potentially impacted by debris in the IRWST during accident conditions (Ref. 98).
- The RP has performed ALARP optioneering and recommended that the 'zero fibre' approach should be adopted (Refs. 99 and 100).
- The RP has demonstrated the feasibility of several design solutions, which will be implemented following GDA (Ref. 101 and 102).
- A design modification (M57) to the in containment insulating material has been incorporated into DR 3.0.

521. Whilst the RP's review of RGP (Ref 9) is, in my opinion, lacking in detail, I am satisfied that the RP has considered all appropriate factors. I am also satisfied that the RP has clearly identified the accidents and systems that will be impacted by debris transported to the IRWST and the related safety functional requirements appear to be aligned with the considerations outlined in IAEA SSG-53 (Ref. 8).

522. The RP presents two options related to the reduction of fibrous material in the containment: the “zero fibre” scheme and the extant design. These options can be summarised as follows:

- The original design has a mixture of fibrous insulation and reflective metallic insulation (RMI) inside the containment. The majority of the large components and piping are insulated with RMI.
- The “zero fibre” scheme eliminates all in-containment fibrous insulation. It also seeks to remove all cable tray wrapping from areas effected by potential breaks (sometimes referred to as the zone of influence)

523. Whilst, technically, it is only necessary to remove fibrous insulation from the zone of influence in order to significantly reduce potential fibrous material in the debris source term, the RP argues that it is simpler and acceptable to replace all fibrous insulation with RMI (Ref. 100).

524. Ref. 100 presents a summary of the optioneering report and concludes that the "zero fibre" configuration is the ALARP choice and should be implemented. The RP has not identified the need for the qualification testing associated with the insulation and filtration system, nor has the RP revisited Ref. 9 to describe the implications of the design choice on the effects that were identified (e.g. if chemistry effects tests are necessary). Much of this work can only be performed once detailed design of the insulation and cable tray wrapping is complete. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0083 – The licensee shall, as part of detailed design, demonstrate that the safety functions of the filtering system, containment heat removal system, and safety injection system can be met, and that adequate heat removal from the core is achieved in the “zero fibre” approach. This should include, but not be limited to:

- A calculation of a more realistic debris source term.
- An optimisation of the in-containment water storage tank filtration system dependent on the potential debris.
- A demonstration that all cable tray wrapping has been removed from the zone of influence for all high energy pipe failures.
- Details of appropriate testing to verify that the design is optimised.
- A demonstration against safety criteria that the safety functions of the safety systems can be met.

525. I am however content that design modification M57 to replace all in containment fibrous insulation with RMI is sufficient for me to make a positive judgement on the adequacy of the fault studies related safety case in GDA.

4.3.6 Shutdown Reactor Faults

526. PCSR Chapter 12 (Ref. 3) does not have a dedicated safety case document for shutdown faults. However, the RP has recognised that faults may progress differently depending on the POS and this has been considered by the RP during the fault identification process (I have discussed this aspect in Section 4.2.2). The RP has identified a number of unique shutdown faults (i.e. faults that can only happen in shutdown conditions) in the generic UK HPR1000 safety case. These are reproduced in Table 3 of this report. In this section I present my assessment of these DBCs that are unique to shutdown conditions. Faults that are bounded by at power faults have already been discussed in other parts of Section 4.3. My assessment of DEC-A events is presented in Section 4. 4.

527. The analysis presented for the unique shutdown faults 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, rather than complex analysis with sophisticated computer codes. I am content that this is acceptable for GDA. For most faults, the objective is to keep the fuel in the RPV covered by water.

528. To inform my assessment of adequacy of the RP's analysis of these faults, I have chosen to sample two DBCs as representative examples. The first is an uncontrolled RCP [RCS] level drop at POS C, D and E which is a frequent design basis fault. This fault can occur when the RCP [RCS] is drained to a ¾ loop level and so there is a lower coolant inventory at the start of the accident. The second fault is a RHR system piping break inside or outside containment at POS C, D and E, which is an infrequent design basis fault and can lead to a loss of coolant and a release of radioactivity outside of the containment building.

4.3.6.1 Uncontrolled RCP [RCS] Level Drop

529. During normal shutdown operation, the cooling of the plant is performed by the RIS [SIS] system in RHR mode. An uncontrolled RCP [RCS] water level drop in shutdown states may be caused by malfunctions or failures within the RCV [CVCS] system. The high-level safety function to protect against this fault is maintaining sufficient reactor coolant system water inventory which is delivered by two low level safety functions (H1-2 water injection into the water reactor coolant system and H1-3 leakage prevention from the RCS through connected auxiliary lines).

530. The primary protection claimed to deliver H1-2 safety function is MHSI with large miniflow pipeline open, automatically initiated by Safety Injection (SI) signal. This safety injection signal is generated by RCP [RCS] loop level low 1, and it is designed to automatically initiate the isolation of low pressure letdown line from RIS/RHR to RCV [CVCS] to deliver the H1-3 low level safety function. The RP has performed safety analysis to demonstrate the fault tolerance and the effectiveness of the safety measures (Ref 103).

531. The RP's safety analysis for the uncontrolled RCP [RCS] level drop fault has been undertaken by a simple hand calculation of mass balance and assuming a single failure of one MSHI pump. The analysis results shows that the primary circuit water inventory can be restored by the RIS [SIS] pumps, the acceptance criterion is met and that the residual heat removal can be ensured in the long term. I am content that this safety analysis approach is reasonable for this fault as the transient is simple without experiencing complex thermal hydraulic phenomena. I also note that within the fault schedule (Ref. 10) the RP has identified diverse means of heat removal should there be a failure of MHSI or RPS [PS], however this is not a bounding sequence for demonstrating the adequacy of these functions (Ref. 34).

532. The RP has determined that the most onerous initial operating state for the uncontrolled RCP [RCS] Level Drop fault is POS C3 and D, at which the plant is designed to operate at ¾ loop condition. At this particular plant condition, the RCP water inventory is smaller, compared with that in other POS. I am satisfied that the RP has considered the most onerous initial conditions in the uncontrolled RCP [RCS] level drop fault sequence, which meets the expectation of ONR SAP FA.6.

533. ONR SAP FA.6 also sets out the expectation that for each initiating fault within the design basis, the relevant design basis fault sequences should be identified and each design basis fault sequence should include the worst normally permitted configuration of equipment outages for maintenance, test or repair. In contrast to the plant operating at full power (POS A), the plant initial conditions and plant configuration vary for POS

C, D and E. The operator needs to perform a series of actions to allow the plant to reach ¾ loop level state. During this process, the plant configuration would be changed. I therefore sought additional information on the operator actions that are needed to bring the plant to State C and then to State D and the plant configuration in each operating mode.

534. In response to RQ-UKHPR1000-1499, the RP has clarified that some safety signals are inhibited during power operation and certain permissive signals need to be enabled to ensure availability of safety functions during the plant shutdown process. Some of these permissive signals are automatically actuated and some require manual initiation. During the plant shutdown process, the operator needs to manually activate or deactivate 4 permissive signals in a certain order to allow the safety injection signal to be generated by the plant parameter as designed. These signals are presented in the response to RQ-UKHPR1000-1499 (Ref. 6) and are based on the operating procedures developed for the UK HPR1000 reference plant. I am satisfied that sufficient protection against this fault is provided within the design; however this will need to be confirmed when the operating instructions are developed. I am content that this can be progressed by a licensee as normal business.

4.3.6.2 RHR System Piping Break

535. An RHR system piping break inside or outside containment is defined as an accident in which an isolable break with a nominal diameter smaller than or equal to [redacted] mm occurs on one RIS [SIS] line during RHR mode. The resulting loss of coolant inventory results in a reactor coolant system pressure decrease and an increase in core temperature. The isolable break can be located inside or outside containment, however from a reactor protection perspective the RP consider that breaks outside containment can be bound by those inside containment. This is because breaks outside of containment can be isolated automatically on Safeguard building sump level high 1 or Safeguard building pressure rise 1 signals. I am content that this is a reasonable approach to assessing the plant performance but the radiological consequences of a break outside of containment will be greater. The RP has assessed the mitigated consequences of a RHR piping break outside containment as 1.76 mSv (infant). I am content that the consequences meet the expectations of FA.7 and SAPs Target 4.

536. In Ref. 104, the RP claims that POS C1 presents the most onerous initial conditions, on the basis that the initial pressure, temperature and power are higher in this state. Failure of the one MHSI pump in an unaffected loop is assumed to be the most limiting single failure. Whilst this appears reasonable, there is no discussion of what has been considered for the identification of the limiting single failure. In response to RQ-UKHPR1000-1576 (Ref. 6), the RP has provided a comprehensive justification why the failure of the one MHSI pump is the most limiting single failure for the acceptance criteria in question. The key factors that the RP has considered in its identification of limiting single failure include:

- the redundancy built in the design of the safety systems claimed to protect this fault.
- the design capacity of each train of the safety system.
- characteristics of the plant transient resulting from the initiating event.
- the effects of the failure of the safety system assumed.
- operator actions claimed in post-accident fault recovery in the longer term, and
- change in plant operating state.
- the acceptance criterion in question.

537. From a review of this response I am content that the RP's justification of the assumed single failure is appropriate and consistent with the expectations of FA.6.

538. I am satisfied that the RP's safety analysis of shutdown faults meets the expectation of ONR SAP FA.4 that DBA should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures.

539. To gain confidence in how the shutdown analysis has informed the operating rules (as expected by SAP FA.9) I have traced the requirements for MHSI with large miniflow pipeline open, automatically initiated by the safety injection signal arising from the uncontrolled RCP [RCS] level drop safety case (as summarised in the Fault Schedule). This safety function is not unique to this fault and is also required for a number of other faults.

540. Ref. 105 summarises the safety functional requirements of the RIS [SIS] safety injection system, with a table providing the information about how these requirements are derived from the relevant safety analysis by referencing out to the related safety analysis reports. Ref. 105 clearly states that the bounding case to inform the requirement of the minimum flowrate of MHSI with large miniflow pipeline open is Small Break - Loss of Coolant Accident (State A) and describes the overpressure analysis which sets the requirements of the maximum flowrate.

541. The RP has used the RIS [SIS] safety injection system as an example within the generic limits and conditions for normal operation (Ref. 23) to illustrate how the operating rules are derived from UK HPR1000 generic safety case. Table T-7-6 of Ref. 23 summarises the operating technical specification requirements, the link to the safety case, along with the applicable operating modes and safety function requirement code for each of those selected SSCs. The safety feature MHSI with large miniflow pipeline open is listed in the table with a clear link to the related analysis by referencing out to the corresponding safety analysis reports. Table T-7-2 Safety System Settings for Automatic ESF Actuation of Ref. 23 lists the setpoints for the parameter designed to generate a safety injection signal when it is reached.

542. Through my review of these documents, I consider that the links between the safety analysis and performance requirements and trip settings are clear and consistent with the expectations of ONR SAP FA.9.

4.3.6.3 Conclusions for Shutdown Reactor Faults

543. Based on my review of the list of unique shutdown faults and my assessment of a sample of these faults, it is my opinion that the RP has submitted an adequate safety case for these faults during GDA. I am content that the fault identification and analysis is adequately described within Chapter 12 of the PCSR, and that these have been carried out consistent with the expectations of SAPs FA.5, FA.6 and FA.7. I am also satisfied that the limits and conditions arising from shutdown faults have been considered by the RP in the development of the generic limits and conditions for normal operation, as expected by SAP FA.9. While there is no single document that brings all of the arguments together, I consider that this is a matter of presentation that can be improved as the safety case develops during detailed design.

4.3.7 Faults Arising within Support Systems

544. The RP has undertaken a significant amount of work to identify the failures arising as a result of support system failures. The RP has undertaken additional PIE identification work for the Heating, Ventilation and Air Conditioning System (HVAC), electrical supply, cooling chain and gas systems. For each system the RP has considered the potential failures that could occur and how these failures would affect the ability of other systems to deliver safety functions during all operating modes (including functions required during normal operations and in response to a fault). It should be

noted that the detailed design of these systems will need to be completed by the licensee and the assumptions made during GDA will need to be confirmed, but I am content that this will be progressed as normal business.

545. Due to the number of systems and the interconnections between them, the interactions between the various support systems are complicated (for example a loss of a one or more trains of a HVAC system could affect one or more trains of the cooling chain or electrical systems) and the RP has produced a number of documents to evaluate and record the potential failures and the effects on other systems. These documents record FMEAs, frequency analysis, PIE lists, functional analysis and the bounding process to identify representative PIES and are referenced from Ref. 11. I am content that the RP has considered an adequate scope of support systems, consistent with the expectations of FA.2 and the guidance to requesting parties (Ref 1) and that the resulting list of representative PIEs is comprehensive.

546. In my opinion the work reported in Ref. 11 (and its supporting references) has been a major undertaking for the RP, is a welcome addition to the safety case and is a good demonstration of the fault tolerance of the design. As a result of this work (and work undertaken in other topic areas) the RP has identified several areas where the diversity within the support systems could be improved and which could reduce the likelihood of CCFs within these systems (the benefits of these modifications are discussed within ONR's PSA Assessment Report (Ref. 24)). Notably, the RP has modified the DEL [SCWS] system (which provides cooling water to some HVAC systems and is a diverse cooling chain for the LHSI pumps) to incorporate diverse chiller units. All of the improvements have been incorporated into DR 3.0 via design modifications and the safety case (including Ref. 11) has been updated to reflect the latest design reference.

547. The categorisation of the representative PIEs has followed a simple process (Ref. 106):

- if the failure involves a loss of one train of a support system then the representative PIE is classified as a DBC.
- if the failure involves a loss of two trains of a support system then the representative PIE is classified for specific study.
- if the failure involves a loss of all trains of a support system then the representative PIE is classified as DEC-A.

548. The use of simple rules for the allocation of faults is sensible when detailed frequency data is not yet available, however the RP does not explain why two of the faults are categorised for specific studies (which use the DEC-A methods and criteria for assessment) rather than as a DBC based on frequency. However, the categorisation of the sequences as specific studies has little practical impact:

- The RP has not undertaken any quantitative analysis of the bounding sequences. Instead, the bounding faults have been compared against existing analysis. This analysis is predominantly that of similar frequency DBCs.
- Whilst the fault schedule (Ref 8) states that functions to protect against DEC-A events are FC3, the safety functions for these sequences are delivered by the same F-SC1 and F-SC2 safety measures available for DBCs.

549. I have raised AF-UKHPR1000-0025 in Section 4.2.2 above on the need to incorporate the specific studies into the list of DBCs and DEC-A events.

550. The RP has identified the following fault conditions within the PCSR (Ref. 3) and these are included within Tables, 3, 4 and 5 of this report:

- Loss of RRI [CCWS] or SEC [ESWS] Train A (POS A/B) DBC-2.

- Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinet Rooms of Safeguard Building Division B (POS A/B) DBC-3.
- Loss of RRI [CCWS] or SEC [ESWS] Train A (POS C/D/E) DBC-3.
- Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinet Rooms of safeguard Building Division B (POS C) DBC-4.
- Loss of two RRI [CCWS] or SEC [ESWS] Trains (POS A/B/C/D/E/F) Specific study.
- Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room (POS C) Specific study.

551. These are included on the fault schedule, with identification of diverse protection for the frequent faults. I am satisfied that this is consistent with the RP's general safety case approach and the expectations of FA.8.

552. Ref. 107 records the RP's consideration of the DBCs, DEC-A and specific studies arising from loss of supporting system faults. This is based on engineering judgement and comparison to existing faults, rather than new transient analysis. The RP concludes that the DBCs can be protected by the extant safety systems designed to protect other design basis faults, with their consequence being bounded by the other design basis faults.

553. To gain confidence in the RP's approach, I chose to review the 'Loss of RRI [CCWS] or SEC [ESWS] Train A fault' as a sample of a loss of cooling chain, as this is a frequent design basis fault. This fault is considered by the RP to be representative of three other faults (loss of LHA [EPDS], loss of LHB [EPDS] and loss of LJA/LJU [SBOPDS]) which would cause similar consequences for the reactor. Through the examination of Ref. 11 and supporting references, I have been able to trace the fault identification from the PIEs to the DBC. The key features of this fault are that it leads to a loss of main feedwater along with a control failure of RCV [CVCS]. In addition, one train (Train A) of the MHSI, LHSI and RIS-RHR is lost. The RP has compared the progression of this fault to other similar DBCs and considered what safety measures are required and what would be available, and this is clearly presented in Ref. 107. The RP notes that all safety functions required to reach the safe state remain available in this fault sequence.

554. The RP concludes that the DBC will progress in a similar manner to the loss of main feedwater DBC. Given that all relevant safety measures will be available, the RP concludes that safety criteria for the Loss of RRI [CCWS] or SEC [ESWS] Train A fault will be met, without needing additional transient analysis. Noting the relatively large safety margin demonstrated in the bounding loss of main feedwater analysis, I am content that the RP's judgement is appropriate and reasonable.

555. Ref. 107 presents similar discussion for each of the additional fault sequences, with consideration of the required and available safety systems and comparison with similar existing analysis. In conclusion, I am satisfied that the fault identification of the loss of support systems has been conducted systematically and the process for the fault identification is auditable and comprehensive. I am also content that the approach of the fault analysis for DBCs derived from the loss of the support systems is appropriate. As such in my opinion the RP has submitted an adequate safety case for faults arising from failures within support systems in GDA, consistent with the expectations set out in ONR SAPs FA.2, FA.5 and FA.6 and NS-TAST-GD-006 (Ref 4), demonstrating that the generic UK HPR1000 design is tolerant to such faults. This will need to be confirmed by a licensee once detailed design of these support systems is complete and I am content that this can be progressed as normal business.

4.3.8 Spurious C&I Actuation Faults

556. The RP has undertaken a significant amount of work during GDA to identify faults which may occur as a result of spurious actuation of equipment by C&I systems. The general fault identification process considers a variety of fault conditions, such as valve closures or inadvertent pump operation, but C&I systems have the potential to initiate multiple failures at the same time. It is also possible that if a system has spuriously actuated an operation then it may not be able to reliably deliver one or more of the safety functions required by the design intent. The RP has therefore developed a methodology to identify potential fault conditions arising from spurious C&I actuation (Ref. 108). ONR's review of this process is recorded in ONR's C&I assessment report (Ref. 109). ONR's C&I Inspector has concluded that the process is reasonable and that the list of PIEs should be appropriate, however AF-UKHPR1000-0037 has been raised for a licensee to detail the measures in place to reduce the frequency of spurious C&I actuation events.

557. Consistent with the main PIE identification process, the RP has grouped similar PIEs together and identified bounding sequences (Ref. 110). Given the confidence that I have gained from other areas of the fault identification, I have chosen not to assess this bounding process in detail.

558. From this process, the RP has identified 19 bounding faults (presented in Table 5 of this report) and considered the potential consequences and available protection. These sequences involve a spurious signal from RPS [PS] or SAS and the RP assumes that these systems are not available to actuate the safety systems required to take the reactor to a safe state. The protection against these sequences is generally provided by the KDS [DAS] which is independent of the RPS [PS] and SAS. Spurious signals from the KDS [DAS] are possible but due to the prioritisation of signals, these will not lead to actuation of equipment if RPS [PS] is giving a contrary signal. The claims on the KDS [DAS] have been considered by ONR's C&I inspector (Ref. 109) who has concluded that this is a reasonable approach.

559. The sequences that have been identified are similar to existing fault sequences that have been assessed elsewhere in the safety case, the principal difference is that RPS [PS] is unavailable and KDS [DAS] delivers the safety functions. Ref. 111 considers each sequence in turn by comparison against existing DBCs or DEC-A fault and makes arguments that the safety functions will be delivered by KDS [DAS] (these arguments are summarised in Table 1 of Ref. 111). The RP also considers the margins to acceptance criteria for similar faults and concludes that the acceptance criteria will also be met for the sequences involving spurious actuation by RPS [PS] or SAS.

560. I have not reviewed all of the arguments within Ref. 111 in detail, but I am content that the overall approach is reasonable. These faults are incorporated into the fault schedule (Ref. 10) which clearly presents the necessary safety functions.

561. Rather than assign the bounding sequences as DBCs based on frequency, the RP has chosen to assess the identified bounding sequences as specific studies. Taken at face value this is a shortfall against the RP's DBC criteria as set out in Chapter 12 of the PCSR (Ref. 3) and ONR's expectations as set out in SAPs FA.5. However, as with the faults arising from support systems, I do not consider this to be significant for GDA for the following reasons:

- The RP has not undertaken any quantitative analysis of the bounding sequences. Instead, the bounding C&I faults have been compared against existing analysis of similar frequency DBCs.
- The detailed design of the C&I systems is out of scope of GDA and the frequency of events will need to be confirmed as the safety case develops.

- Whilst functions to protect against DEC-A events are FC3, the safety functions for these sequences are delivered by the F-SC2 KDS [DAS]. Therefore the categorisation of the sequences as DEC-A has little practical impact.

562. Nevertheless, I consider that it is appropriate for a licensee to confirm the frequencies of the identified sequences and ensure that appropriate assessment is undertaken. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0157 – The licensee shall, as part of detailed design, justify the frequency of spurious control and instrumentation faults, justify the analysis methods and criteria, and demonstrate that these criteria can be satisfied. This should be either by analysis or comparison to other analysis.

563. Notwithstanding this, in my opinion the work undertaken by the RP in GDA to identify and analyse potential fault conditions arising from spurious C&I actuation faults is an important addition to the generic UK HPR1000 safety case and provides good support to the demonstration of the fault tolerance of the design.

4.3.9 Heterogeneous Boron Dilution Faults

564. Heterogeneous boron dilution events are characterised by the formation of a low boron concentration slug in a loop of the RCP [RCS] while the boron concentration in the rest of the RCP [RCS] is unchanged. The dilution can be *external* in origin, where water of low or zero boron concentration is injected into the RCS, or *inherent*, forming as a result of certain accident conditions such as reflux condensation during a SB-LOCA. The risk is that the slug, once formed, could be transported through the core, by for example restarting the RCPs, resulting in a rapid increase in core reactivity.

565. Heterogeneous boron dilution events are distinguished from homogeneous events in the respect that for the latter unborated water is rapidly mixed with the RCS inventory as it is injected so that a slug of dilute coolant does not form. As the large coolant flow rate associated with operational RCPs promotes the rapid mixing of any injected water, heterogeneous boron dilution events are only expected to arise in operational or accident states for which RCPs are stopped.

566. This section presents my assessment of the adequacy of the safety case presented by the RP for heterogeneous boron dilution events, both external and inherent. My assessment of homogeneous dilution events has been presented in Section 4.3.4.2. The basis for the safety cases presented for external and inherent heterogeneous boron dilution are different and are therefore considered separately in the following sections.

4.3.9.1 External Heterogeneous Boron Dilution Events

567. The RP has systematically and comprehensively identified all PIEs which have the potential to lead to a heterogeneous dilution event and has rationalised faults into 8 fault groups associated with the varying dilution pathways (Refs. 26 and 27). The scope of the RP's fault identification analysis includes all systems connected either directly or indirectly to the RCP [RCS] that are supported by a system with unborated water and focuses on POS C, D and E for which the RCPs are stopped.

568. The RP has developed a prevention strategy for each of the 8 identified fault groups based on the implementation of design features including automatic and manual plant isolations to prevent the ingress of unborated water into the RCP [RCS] (Ref. 68). In circumstances where plant isolations fail, the RP claims that RCP start-up procedures will sufficiently drain the RCP [RCS] of an unborated slug to avoid a re-criticality following the restart of the RCPs. The RP has identified and listed prevention functions

and associated safety measures for each fault group within its prevention strategy (Ref. 68).

569. The RCP start-up procedures are not claimed to fully clear an unborated slug from the RCP [RCS], so the RP's safety case relies on a demonstration that the residual slug size, after the RCP start-up procedures are carried out, will not be sufficient to cause a re-criticality. This demonstration has been conducted using the computational fluid dynamics (CFD) code FLUENT (Refs. 68, 112). The RP's analysis provides a demonstration that a slug sized below [redacted] will not cause a re-criticality and that the RCP start-up procedures act to limit residual slug sizes to below this limit with adequate margin.

570. The RP's safety submission excludes PIEs associated with external heterogeneous boron dilution from the list of events for consideration within the plant design basis (Ref. 106). As a consequence, the RP had not initially explicitly applied any DBA techniques to justify the adequacy of countermeasures. Instead, the RP presented a justification for adequacy based on a probabilistic analysis which is claimed to demonstrate that external heterogeneous boron dilution faults are practically eliminated (Ref. 113).

Fault Identification of Heterogenous Boron Dilution from External Sources

571. The RP has simplified the fault identification process by considering functional failures of systems as PIEs instead of identifying and grouping individual component failures. Ref. 27 rationalises PIEs relevant to external heterogeneous boron dilution into 8 groups for which IEFs are estimated using PSA data (Ref. 114).

572. Based on my review of the RP's analysis, I am content that the RP has considered all relevant systems within the scope of the identification process. I have also compared the RP's PIE list with the list considered for the UK EPR in its GDA (Ref. 115), based on which I consider the RP's list to be credible. However, the RP's safety case does not reference any systematic analyses of individual failures.

573. In response to RQ-UKHPR1000-1294 (Ref. 6) the RP has provided a general assurance that PIEs have been reviewed against underlying Failure Modes and Effects Analysis (FMEAs) and, to support this assurance, has provided details of an example demonstrating the link to failures identified within FMEA studies for the RCV [CVCS] (Ref. 6). I am therefore satisfied that the RP's rationalisation of faults results in a list that provides a satisfactory basis for devising a prevention strategy and, to this extent, that the safety case is consistent with the expectations of SAP FA.2 for the purposes of GDA. I consider that it would be preferable for the RP's safety case to explicitly reference underlying failure studies to demonstrate completeness in a way that is auditable, however given that I am confident that these records exist I am satisfied that this is a minor shortfall that can be addressed as the safety case develops.

574. The RP has argued that boron dilution events occurring after an accident which results in tripping of the RCPs (e.g. LOOP and total loss of cooling chain) are beyond the scope of its fault identification analysis because multiple failures would be required for faults to progress (i.e. the initiating event, plus the heterogenous boron dilution, plus restarting the RCPs erroneously). I do not agree with this position since I consider that a dilute slug could, at least in principle, develop in the RCS [RCP] following a loss of RCPs in POS A to C if RCPs are lost during normal make-up from the REA [RBWMS] at reduced boron concentration. I note, however, that this is a limited set of circumstances compared with the wide range of initiators for plant states C to F.

575. Despite not identifying these scenarios explicitly as faults, Revision B of the functional requirements for prevention and protection against boron dilution (Ref. 116) did briefly

outline the countermeasures to prevent boron dilution during accident states, although without a justification of the adequacy of these safety measures. These include system isolations (e.g. anti-dilution protection which automatically isolates the RCV [CVCS] suction and switches to charging from the IRWST if there is insufficient natural circulation within the RCP [RCS]) and a claim on the pump start-up procedures to clear a slug should these measures fail. However, this information has been removed from Revision D of this document (Ref. 68), presumably as the RP has now screened out these faults. Although the RP's safety case does not explicitly identify additional faults associated with accident states, I am content that there are countermeasures identified for the relevant scenarios and I consider this to be an acceptable position for GDA. Nonetheless, once the relevant procedures have been developed a licensee will need to develop a safety case for faults associated with accidental loss of RCPs during normal make-up at low boron concentration regardless of whether the faults are within the design basis or not. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0158 – The licensee shall justify the frequency of boron dilution events following a loss of reactor coolant pumps and ensure that these faults are addressed within the safety case irrespective of whether they are within the design basis or not.

Practical elimination

576. The 8 PIE groups associated with external heterogeneous boron dilution that are identified are not carried forward by the RP as DBCs (Ref. 106). Instead, the RP presented a justification based on a probabilistic analysis to demonstrate that external heterogeneous boron dilution faults are 'practically eliminated' (Ref. 113). In practice, the criterion applied is that the cumulative frequency at which re-criticality can occur for all PIEs, after account is taken of the identified countermeasures, is below 10^{-7} pa. Based on its analysis, the RP estimates that the residual frequency for re-criticality is [redacted] pa and thus concludes that external heterogeneous boron dilution accidents meet the acceptance criterion.

577. I did not consider that this approach aligned with ONR expectations for a demonstration of practical elimination, which should be based on deterministic and probabilistic arguments. I was particularly concerned that countermeasures associated with faults having a very significant unmitigated consequence were not classified with respect to their role in preventing fault progression (SAPs ECS 1 and ECS.2). I discussed this with the RP and following these discussions the RP has revised its safety case such that it better aligns with its methodology for classification and categorisation of safety measures (Ref.13). The revised safety case presented in Ref. 113 includes a modification (M87, Ref. 117) which implements two FC1 interlocks, applying 2 out of 3 logic, to allow the pump start-up procedures to be claimed as a F-SC1 preventative measure (discussed further below).

578. This F-SC1 measure is consistent with ONR's typical expectation for protection of infrequent faults (IEF<1 $x10^{-3}$ pa) (NS-TAST-GD-006 Section 5.7.16, Ref. 4). Only one of the identified faults (A-6-1, with an IEF of 3.35 $x10^{-3}$ pa) would not be considered infrequent, however there are independent manual and automatic plant isolations preventing progression of the fault so I consider that there is sufficient defence in depth for this fault. Overall, I am satisfied that the RP's introduction of a F-SC1 measure meets ONR expectations for protection subject to a demonstration that the pump start-up procedures are functionally capable of meeting the claimed objectives (discussed below).

579. For the majority of the faults under consideration, supporting measures, consisting of manual and automatic system isolations and anti-dilution protection (Ref. 68), provide additional independent lines of defence. The RP has chosen not to classify these

supporting measures with respect to their role in preventing fault progression (although they may be otherwise classified) and makes its primary claim against the RCP start-up procedures. Consistent with the RP's approach, I would therefore expect the RCP start-up procedures to be effective, independent of the success of supporting measures.

580. However, in my opinion, there is a shortfall in the demonstration of this independence for one fault (identified as A-12-1). For this fault, the success of the RCP start-up procedures ais reliant on prior clearance of the RIS [SIS] pipeline. The measures to clear the RIS [SIS] pipeline should therefore attract a similar classification to the RCP start-up procedure. The development of the procedures is out of scope for GDA and I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0213 – The licensee shall, as part of the development of operational procedures, demonstrate that the procedure to clear the safety injection system pipeline of an unborated slug of water is adequate to support the FC1 RCP start-up function.

581. As these further measures essentially strengthen the operational procedures already proposed by the RP, I do not believe that my finding indicates any fundamental weakness in the RP's design and as such it can be addressed by a licensee following GDA.

Adequacy of safety measures

582. The RCP start-up procedures are the principal countermeasure claimed for all external boron dilution faults so I would expect the RP's safety case to demonstrate the effectiveness of the countermeasure on a conservative basis for the most adverse operating conditions (SAP. FA 7). The demonstration of the effectiveness of the RCP start-up procedures is presented in Ref. 68.

583. The modification introducing F-SC1 RCP interlocks ensure, firstly, that the RCV [CVCS] let-down (in loop 2) operates at its nominal flow for a set time before the RCP in loop 2 is started and, secondly, that the RCP in loop 2 is run for a set time prior to starting the RCPs in loops 1 and 3. The first interlock is intended to ensure that RCV [CVCS] let-down sufficiently drains loop 2 of a dilute slug and the second interlock is intended to ensure that the reverse flows in loops 1 and 3, driven by the head of the RCP in loop 2, will mix any dilute slugs in these loops before their RCPs are started.

584. Based on my review of the relevant submissions, the key claims associated with the RP's demonstration of the effectiveness of the countermeasure are:

- A slug forming in loop 2 has a volume less than [redacted], which is the combined volume of the cross-over leg, reactor coolant pump volume and part of the cold leg from reactor coolant pump to RHR injection point (Ref. 68).
- The RCV [CVCS] let-down operated at nominal flow for 1 hr in loop 2 will reduce a dilute slug of maximum volume [redacted] to a size less than [redacted] (the calculated size is [redacted] after 1600s of let-down). The demonstration is performed using CFD over a flow domain encompassing the loop 2 cross-over leg, RCP volume and cold leg with boundary conditions obtained using the thermal hydraulics system code LOCUST (Ref. 68).
- A dilute slug of volume less [redacted] will not cause re-criticality when transported to and through the reactor core. The demonstration is performed using CFD over a flow domain encompassing the RPV and the loop 2 cold leg with boundary conditions obtained using the thermal hydraulics system code LOCUST and using the core neutronics code COCO to compute the potential for re-criticality (Ref. 112).

- The reverse flow in loops 1 and 3 driven by the RCP in loop 2 will sufficiently mix any dilute slugs in these loops with the RCS inventory such that a re-criticality will not occur when the RCPs in loops 1 and 3 are started. The demonstration is performed using the thermal hydraulics system code LOCUST (Ref. 68).

585. As noted above, the RP recognise that the RCP start-up procedures may not fully clear an unborated slug from the RCP [RCS], so the RP's safety case also includes a demonstration that the residual slug size, after the RCP start-up procedures are carried out, will not be sufficient to cause a re-criticality. From consideration of the PIEs, the RP has established a bounding slug size but has not explained why the size analysed conservatively bounds all possibilities. In my opinion, there may be a reasonable basis for the RP's assumption of slug of cooler water filling a U-leg (cross-over leg) under the action of buoyancy since I expect that the size will be limited by overspill into the RPV downcomer. However, I also note that larger slugs do arise for inherent dilution scenarios and so are, at least in principle, possible. I therefore consider that further development of the RP's argument is needed in order to fully justify the assumption of bounding slug size across all potential external dilution scenarios.

586. The RP presents a limited set of results in Ref. 68 obtained for a single scenario modelled using CFD to analyse draining of loop 2 by the RCV [CVCS] let-down, with the most onerous initial conditions from POS C. The results suggest that the let-down is very effective in draining the loop section from the cold leg up to the point of let-down but much less effective in draining the loop section between the point of let-down and the SG inlet plenum resulting in a residual slug of [redacted] after 1600s. A second CFD based analysis is used to demonstrate that this size of slug will not cause a re-criticality.

587. My expectation is that both these analyses should be conducted on a conservative basis (SAP FA.6) and meet the general expectations of the ONR SAPs for the assurance of models (SAPs AV.1-8). Although I note that the RP has conducted basic sensitivities tests for the CFD aspects of the analysis, considering time step, mesh size and turbulence model, I consider that the RP's safety documentation is, in general, insufficiently detailed to allow a full assessment to be made against SAPs AV.1-6. This is particularly the case for the important CFD aspects. I raised RQ-UKHPR1000-1153 (Ref. 6) seeking further information, particularly on validation evidence to underpin the RP's use of CFD. However, the RP's response included only a limited amount of additional information on comparisons with rig testing data which, whilst welcome, was not sufficiently detailed to be meaningfully assessed. Based on my review of the information provided during GDA, I consider that the following items will require further consideration by a licensee:

- the sensitivity of outputs to plant conditions, for example variations in core decay heat, pump start-up rate (SAP AV.6). This is needed to support a demonstration that analyses are conducted on a conservative basis.
- an assessment of uncertainties in its analysis to provide confidence that the assessed residual slug size, which is estimated to be 90% of the critical size, is calculated with sufficient accuracy.
- documentation to facilitate a review of the adequacy of models (SAP AV.5), particularly with regard to validation against test data.

588. Overall, I am content that the RP has presented a substantially complete analysis supporting its functional assessment of the RCP start-up procedures which, in my opinion, gives confidence in the adequacy of the design for the purposes of GDA. However, in my opinion further work is required by a licensee once the procedures are

developed to properly substantiate key claims (as outline above). I have taken this into account in my decision to raise AF-UKHPR1000-0236 below.

4.3.9.2 Inherent Heterogeneous Boron Dilution Events

589. The RP has identified two faults scenarios that have the potential to lead to the generation of an unborated slug in the RCS which might subsequently be transferred to the reactor core (Ref. 118). The first scenario is a SB/IB LOCA where an unborated slug develops in a SG during the reflux condensation phase of the transient. The second scenario is an SGTR in which there is the potential for an unborated slug to form as a result of backflow from the secondary to primary side of an SG after RCPs are tripped. In either case, the slug may subsequently be transferred to the core during a transition to natural circulation. As these are design basis faults, the RP has assessed them on a conservative basis. I am content that this is appropriate.

590. The RP argues that the response to the SGTR fault (either automatic or manual) acts to maintain the primary pressure above its secondary pressure during cooldown thus avoiding the potential for heterogeneous boron dilution. The RP claims that in any event the consequences of boron dilution caused by the restart of natural circulation following SGTR are bounded by the analysis for SB/IB LOCA and so only the SB/IB LOCA scenario has been explicitly analysed.

591. The RP presents an analysis of the SB/IB LOCA scenario which models the change to core reactivity associated with transfer of an unborated slug to the reactor core. The maximum possible slug is conservatively taken to be [redacted] which corresponds to the total volume of the cross-over leg plus the volume of the SG outlet plenum.

592. The RP has analysed the mixing of the slug during transport using the CFD code FLUENT with initial and boundary conditions determined by an assessment of the SB/IB LOCA transient using the thermal hydraulics code LOCUST. The LOCUST analysis utilises assumptions that are claimed to favour the rate of formation of an unborated slug in the SG outlet plenum. The RP identifies a minimum boron concentration of [redacted] at the core inlet as the decoupling criterion to ensure that no return to criticality occurs for the transient. Based on its analysis, the RP concludes that the boron concentration at core inlet will remain above [redacted] during the passage of the slug through the core with a minimum margin of [redacted]. The RP therefore concludes that re-criticality will not occur for inherent heterogeneous boron dilution scenarios.

593. The assessed transient is a complex transient for which, in my opinion, there are significant challenges in predicting both (i) the flow conditions at which a dilute slug will be generated in a loop and subsequently transferred to the core and (ii) the degree of mixing that the slug experiences within the RPV downcomer and lower plenum during the period of its transit. This differs from the position for external boron dilution for which the application of LOCUST to predict flow conditions is, in my opinion, relatively straightforward and the primary challenges concern the application of CFD. Given this, I have focused my review of the use of LOCUST and FLUENT on their use by the RP to support the analysis of inherent boron dilution transients.

LOCUST Analysis

594. The RP recognises that inherent dilution can only occur over a limited range of break sizes. This arises because there will be insufficient loss of RCP [RCS] inventory at small break sizes to lose natural circulation, whereas at large break sizes the primary circuit pressure and temperature fall sufficiently to inhibit SG heat transfer, which is needed to generate a dilute condensate slug. The RP has therefore analysed SB/IB LOCA with the thermal hydraulics code LOCUST over a range of break sizes to

establish the conditions at which inherent boron dilution can occur. The RP has penalised calculations to favour the formation of a dilute slug by choosing bounding values for parameters that minimise RCP [RCS] inventory, maximise core steam generation and maximise condensation in the SGs. Following this philosophy, the RP has chosen to locate the break on the loop with the pressuriser located near the safety injection nozzle.

595. From my review of the RP's LOCUST analysis, I am content with its penalisation philosophy and assumptions which I consider to be logical. I am also generally content with the application of the single failure criterion in which only one of three safety injection trains and one or two out of three RBS [EBS] trains is assumed to operate. However, the RP's report (Ref. 118) does not include or reference validation evidence for LOCUST to support its use in analysing the transients in question (SAP AV.2). In the absence of validation evidence, it is not possible to know how reliably the flow conditions under which a dilute slug is transported to the core are captured by LOCUST.

596. For this reason, I raised a query on validation within RQ-UKHPR1000-1513 (Ref. 6). In response, the RP has cited the assessments reported in the verification and validation report for LOCUST (Ref. 17) as evidence underpinning its use for inherent boron dilution. I note that Ref. 17 presents a Phenomena Identification and Ranking Table (PIRT) analysis for IB-LOCA and reports on a wide range of SET and IET comparisons for identified phenomena. However, the PIRT is referenced to acceptance criteria on fuel integrity and the maintenance of core cooling which I do not consider to be relevant to the inherent boron dilution scenario being considered. I do not dismiss the potential relevance of much of the validation evidence presented in Ref. 17, which provides confidence in the capability of LOCUST. However, in my opinion, the validation case should be based on a PIRT referenced to an appropriate acceptance criterion (e.g. lower plenum boron concentration following a return to natural circulation) with phenomena ranked accordingly and test data identified with reference to these rankings.

597. I have taken this into account in my decision to raise AF-UKHPR1000-0236 below.

FLUENT Analysis

598. The RP has modelled the transport of a dilute slug through the RPV core on a computational domain which includes the RPV internals and three inlet cold legs. The slug is assumed to have 0 ppm boron concentration and to have a volume equal to the entire volume of the SG outlet plenum and cross-over leg ([redacted]). From a computational perspective, the slug is introduced into the flow domain by setting the boron concentration to 0 ppm at a cold leg inlet boundary over the period of time that [redacted] of water enters the flow domain. I expect that the actual slug size and concentration will depend on the rate of condensation in the relevant SG, the injection of borated water into the loops and any intermittent mixing that may occur. I therefore judge that the assumptions on slug size and concentration are conservative. The RP states that flow initial and boundary conditions (comprising hot leg flow rate and safety and RBS [EBS] injection histories) are otherwise derived from the LOCUST outputs. The computation tracks the transport of the slug as it enters the downcomer and interacts with the RPV inventory and flow from the other loops.

599. The RP has assessed the evolution of boron concentration at the core inlet for the three break sizes considered in the LOCUST assessment but reports little sensitivity of outputs to break size. The RP also reports an additional set of sensitivity tests on computational time step, mesh resolution and turbulence model choice to demonstrate that the solutions are robust. In my opinion, whilst an important summary of the validation, the RP's presentation and discussion of results in Ref.118 is too limited to

form a judgement of its analysis against ONR expectations (SAPs AV.1-9), particularly with regard to validation for the scenario.

600. I sought further information and in response to RQ-UKHPR1000-1513 (Ref. 6) the RP indicated that experimental tests have been conducted to underpin the use of CFD for this scenario. However, insufficient information on the test data has been provided to form a meaningful judgement against ONR expectations. Given that I am content that the RP has chosen a conservative slug size for analysis and noting the sensitivities summarised in Ref. 118, I am content not to progress this further during GDA.

4.3.9.3 Conclusions for heterogeneous boron dilution faults

601. From my assessment of external and internal heterogeneous boron dilution faults I am satisfied that the RP has provided an adequate safety case for me to judge that the generic UK HPR1000 design has sufficient safety measures to support the RP's claim that the faults can be considered as practically eliminated. However, I have identified a number of areas where a licensee needs to undertake additional work to strengthen the evidence that underpins this claim for the full range of operating conditions as the design and operating procedures are developed. I have therefore raised the following Assessment Finding which a licensee will need to resolve:

AF-UKHPR1000-0236 – The licensee should provide further evidence to underpin the use of LOCUST and computational fluid dynamics in heterogeneous boron dilution scenarios. This should include, but not be limited to:

- Appropriate Phenomena Identification and Ranking Table (PIRT) analysis referenced to relevant acceptance criteria.
- Justification of the validity of the models used.
- Validation against test data.
- Sensitivity studies of outputs to plant conditions and uncertainties in the prediction of residual slug sizes.

4.3.10 Primary Flow Asymmetry Effects

602. An asymmetric primary flow rate or asymmetric Steam Generator Tube Plugging (SGTP) may lead to asymmetric primary state points (setpoints) or change the initial states assumed in the safety analysis potentially reducing the margins to the relevant safety criteria. Asymmetry effects may also include (but is not limited to) asymmetries in primary flow rates, differences in loop flow resistance, as-built deviations, and possible degradation in reactor coolant pump performance through plant life.

603. During the life (or even commissioning) asymmetrical SG behaviour can occur due to different length of the secondary piping (e.g. steam lines), resistances, manufacturing tolerances, pressure drops, etc. It is not uncommon in PWR to observe that the power transferred in the SGs may differ and that 1 or 2 SGs transfer more power than the other SG(s). These conditions can be worsened (or compensated) during the full plant life by SGTP which is undertaken to isolate degraded SG tubes.

604. In the UK HPR1000 transient analysis, all three primary loops are considered symmetric with the same flow rate and consideration of SGTP (from 0% to 10%). The original UK HPR1000 safety case submissions did not account for or discuss asymmetry effects. To gain confidence that the generic UK HPR1000 design is not overly sensitive to asymmetry effects and that the analysis of DBCs has appropriate conservatisms to account for asymmetry effects (noting the expectations of ONR SAPs paragraphs 631 and 638), the RP has presented a new report to assess the influence of primary and secondary geometrical data and associated uncertainties to develop a bounding asymmetrical scenario (Ref. 19).

605. This scenario results in the following differences in heat transfer: SG1: [redacted] Nominal Power; SG2: [redacted] Nominal Power and SG3: [redacted]% Nominal Power, leading to approximately [redacted] Full Power difference. In my opinion this bounding asymmetrical case is very conservative and unlikely to be possible. The RP has also presented a list of design basis and DEC-A transients which would be most affected by the asymmetry and has provided reasoning as to why they are still bounded by the extant analysis. I am content that this approach is appropriate.

606. Ref. 119 concludes that, with the power difference between three loops of ~[redacted] Full Power, the results of the transient analysis conducted for DBCs and DEC-A events would not be challenged and notes that the factors that could cause asymmetry will be minimised during design and manufacture. I am content to support this judgement during GDA as the bounding case assumed in Ref. 119 is reasonable and will be confirmed during the commissioning tests and form part of the acceptance criteria for relevant tests (e.g. the individual power of each SGs and total power). This is normal business for a licensee as part of plant commissioning.

4.3.11 Containment Building Performance

607. To evaluate the performance of the containment during design basis faults and validate the containment design parameters the RP has undertaken analysis of bounding DBCs. In Refs 120 and 121 the RP has analysed the pressures and temperatures that will be experienced by the containment during a LB-LOCA (double ended guillotine break) and MSLB. Given that these faults lead to large steam releases into the containment I am content that these are an appropriate basis for this purpose, consistent with the expectation of SAPs FA.9 that DBA should provide an input into the engineering requirements for SSCs.

608. The analysis and discussion of the containment design is presented in Chapter 7 of the PCSR (Ref. 3). The analysis is conducted in two steps. First, a Mass Energy Release (MER) analysis has been conducted using system thermal hydraulics codes (LOCUST for LB-LOCA and GINKGO for MSLB) then the containment analysis code CATALPA uses this as input data to calculate the containment pressure and temperature response during the transient.

609. The analysis has been conducted against the internal containment design pressure and temperature of 0.52 MPa and 145°C.

610. Within Ref. 120 the RP has analysed a LB-LOCA in the hot leg, cold leg and crossover leg. Of these, the hot leg LB-LOCA is the most limiting with a peak pressure of [redacted] MPa and peak temperature of [redacted] °C.

611. For MSLB (Ref. 121) the RP has analysed a range of initial power levels and two different potential single failures. The first is a failure to close the MSIV on the affected SG and the second is failure of the ASG [EFWS] flowrate limitation on the affected SG. The most limiting case is at hot zero power with failure of ASG [EFWS] limitation to affected SG with a peak pressure of [redacted] Mpa and a peak temperature of [redacted] °C.

612. To gain confidence in the analysis I have briefly reviewed the key methods and assumptions against the general expectations of FA.6 and FA.7. I have also considered the capabilities and limitations of the CATALPA code (more detail on this code is presented in Appendix 1).

613. The detail of the main assumptions are presented in the containment analysis reports (Refs.122 and 123), Additional information on the containment models has been incorporated into Appendix A of the LB-LOCA containment analysis report (Ref. 122). From this I have been able to establish that the RP has developed a reasonably

detailed containment model (for this type of code) which includes all the major mass structures and the IRWST (which influences calculation and results). Some key assumptions of the RP's modelling are:

- The outer surface of the containment is considered to be adiabatic to minimize the heat removed to the outside (although heat transfer from the containment wall to the outer protective containment is credited).
- Primary containment leak rate is zero (i.e. perfect isolation for the mass).
- Containment spray is not credited/modelled.
- Only energy removal from containment is done through the Component Cooling Water System (RRI [CCWS]) / Essential Service Water System [ESWS]) system.

614. I am content that these assumptions are appropriately conservative, that CATALPA is an appropriate code for this analysis and that the results show sufficient margins to the design pressure. I am therefore satisfied that appropriate analysis has been conducted to inform the design of the containment.

615. Given that the RP are intending to modify the geometry of the MCL (Ref. 88) I have sought to understand the potential impact upon the containment analysis. The response to RQ-UKHPR1000-1613 (Ref. 6) shows that the impact is likely to be minor and will not invalidate the conclusions of Ref. 122. I am content that the RP has submitted adequate analysis for containment performance analysis during GDA and that the implications of the modification of the MCL geometry can be confirmed during detailed design.

4.3.12 Strengths

616. Following my assessment of the design basis reactor faults I have identified the following strengths:

- The RP has demonstrated that the analysis methods have been applied consistently and that the acceptance criteria are met for all DBCs.
- For those faults for which DNB is predicted the RP has considered means by which the consequences can be reduced.
- For frequent faults the RP has identified diverse means of delivering safety functions and provided analysis to justify their effectiveness.
- The RP has identified faults arising from failures within support systems or arising from spurious C&I actuation and demonstrated that they can be protected against by existing safety measures.
- All DBCs are presented within a fault schedule which summarises the safety measures required following a fault to bring the reactor or SFP to a stable, safe state.

4.3.13 Outcomes

617. As a result of my assessment of the design basis reactor faults I have identified eight Assessment Findings:

- to demonstrate that the high neutron flux (source range) trip setting is adequate to protect against homogeneous boron dilution faults from shutdown conditions at the start of cycle.
- to demonstrate that the source range, intermediate range and power range detectors can be considered as diverse and that the risks of a CCF are reduced ALARP.
- to consider whether it is reasonably practicable to provide automatic isolation of the boron dilution source via the REN [NSS] boron concentration signal to

prevent a return to criticality in the event of a homogeneous boron dilution fault at cold shutdown with a failure of RPS [PS].
- to demonstrate that the safety functions of the filtering system, EHR [CHRS], RIS [SIS] can be met, and that adequate heat removal from the core is achieved in the "zero fibre" approach.
- to assess the frequency of spurious C&I events, confirm the appropriate analysis methods and criteria and demonstrate that these criteria can be satisfied (either by analysis or comparison to other analysis).
- to provide an adequate safety case for the loss of RCPs during normal make-up at low boron concentration.
- to review the procedure to clear the RIS [SIS] pipeline of an unborated slug to ensure that it is consistent with the FC1 RCP start-up function.
- to provide further evidence to underpin the use of CFD in heterogeneous boron dilution scenarios.

618. In addition, Assessment Findings AF-UKHPR1000-0005, AF-UKHPR1000-0010 and AF-UKHPR1000-0165, raised in other Assessment Reports, will need to be addressed before it can be concluded that the risks from RCCA ejection accidents, SGTR and LB-LOCA are ALARP.

619. I have also identified a number of minor shortfalls during my assessment of this part of the safety case.

4.3.14 Conclusion

620. Based on the outcome of my assessment, considering ONR SAPs FA.6, FA.7 and TAG NS-TAST-GD-006, I have concluded that the analysis of generic UK HPR1000 design basis reactor faults adequately meets my expectations for GDA. The RP has demonstrated the capability of the safety measures to prevent damage to the containment barriers during these events. Subject to the licensee adequately resolving the Assessment Findings I have identified, I am satisfied that the consequences have been predicted conservatively and support a demonstration that the consequences are reduced ALARP.

4.4 Reactor Design Extension Conditions

621. It is considered good practice for new reactor plant to demonstrate that there is no escalation of consequences for faults just beyond the traditional design basis criteria. The expectation from IAEA SSR 2/1 and WENRA Objectives for new NPP (Refs. 8 and 9) is that the safety analysis will cover low frequency events and sequences of greater severity than those considered within the design basis and show that there is adequate protection against these faults. ONR's FA SAPs (Ref. 2) and NS-TAST-GD-006 (Ref. 4) set similar expectations.

622. As discussed in Section 4.2 above the RP has identified a number of sequences which they have identified as DEC-A events with the intention of demonstrating that the generic UK HPR1000 design can withstand events beyond the design basis, without core damage. Additional safety measures are provided in the design to provide protection against these sequences. Some of these sequences have been used by the RP to demonstrate diverse protection for frequent faults specifically for the UK HPR1000 safety case (my assessment of the general aspect of the use of DEC-A analysis for this purpose is reported in Section 4.2 of this report and for individual faults within the relevant parts of Section 4.3).

623. Chapter 13 of the PCSR contains the list of DEC-A faults (reproduced as Table 5 of this report) and provides a summary of the analysis of bounding cases that has been performed to demonstrate the effectiveness of the DEC-A safety measures. In this

section of my assessment report I consider the adequacy of this analysis and the associated safety measures.

624. The reactor DEC-A events primarily fall into 2 main groups: those relating to a loss of cooling and ATWS faults. I have focussed my assessment on these groups of faults below, along with SB-LOCA with loss of safety injection. I have discussed fuel route DEC-A events within Section 4.5. Given that the RP has applied its conservative DBC4 analysis rules and acceptance criteria to these faults I am satisfied that this adequately meets the graded expectations for DEC-A sequences as set out in NS-TAST-GD-006 (Ref. 4) and IIAE SSG-2 (Ref. 8).

4.4.1 Loss of Cooling Faults

625. The generic UK HPR1000 design has a number of additional, diverse systems which are provided to protect against faults involving a loss of cooling. In the short term (i.e. to the controlled state), decay heat can be removed via the VDA [ASDS] and ASG [EFWS]. A single train of ASG [EFWS] and VDA [ASDS] are designed to be capable of delivering this function. If this function is not available, the automatic ASP [SPHRS] function (F-SC3) or a manual bleed and feed function (FC2) can be used for decay heat removal. My assessment of these functions is described in sub-section 4.4.1.1 below.

626. The normal cooling chain for long term heat removal consists of the RRI [CCWS] and SEC [ESWS] which transfer heat from the RHR system to the ultimate heat sink. The RRI [CWCS] also provides cooling water for the LHSI pumps.

627. If there is a total loss of cooling chain and the primary circuit is intact the heat can be removed via the secondary circuit. The RP has analysed this as a Loss of Ultimate Heat Sink (LUHS) for 100 hours (POS A and B) and I discuss my assessment of this in Section 4.4.1.1 below.

628. However, in some plant states secondary side heat removal is not available. In these circumstances the EHR [CHRS], DEL [SCWS] and ECS [ECS] can provide alternative means of long-term heat removal:

- The EHR [CHRS] recirculates water from the IRWST by spraying via a spray ring around the containment structure.
- The ECS [ECS] is an additional cooling system for the removal of heat from the EHR [CHRS] or PTR [FPCTS] following a total loss of cooling chain or station black out. The system removes heat to dedicated cooling towers via an intermediate circuit.
- In the case of RRI [CCWS] and/or SEC [ESWS] failure, the DEL [SCWS] can offer a diverse cooling chain to cool the LHSI pump motors in Train A and B. During total loss of cooling chain accidents in state A or state D, the diverse cooling chain can be connected to LHSI pumps automatically by the RRI [CCES] high temperature or low flowrate signal.

629. The RP has analysed a number of transients to demonstrate that these systems can provide sufficient cooling to prevent core damage and ensure long term heat removal. In sub-section 4.4.1.2 below I have briefly considered these systems in turn along with the substantiation that has been submitted to demonstrate their effectiveness. I have then given an overall conclusion on the protection available against loss of cooling chain faults.

630. Finally in this section I have also considered the safety case for a Station Blackout (SBO) event which involves a LOOP together with a CCF of the EDGs (Section 4.4.1.3).

4.4.1.1 Loss of Secondary Side Cooling

Manual Feed and Bleed

631. The feed and bleed function is credited for beyond design basis faults and as a diverse means of protection for frequent faults, and is therefore identified as a DEC-A safety feature. The feed and bleed function employs MHSI/LHSI in combination with the PSVs and provides a means of heat removal when secondary cooldown is unavailable.

632. The RP has identified the following bounding cases for which the feed and bleed function is credited:

- SBO (POS G).
- TLOFW (i.e. failure of normal feed + failure of the ASG [EFWS]) (POS A).
- SB-LOCA with failure of MCD.

633. I have presented my assessment of SBO in sub-section 4.4.1.3 of this report. My assessment of feed and bleed has focussed on SB-LOCA and loss of normal feedwater which are frequent faults. Feed and bleed therefore provide the diverse means of protection for these faults.

634. The analyses for the TLOFW and SB-LOCA sequence is presented in Refs. 124 and 125 respectively. Both analyses have been performed using LOCUST. In the analysis of both accidents, the RP aims to demonstrate that the DBC-4 fuel integrity acceptance criteria are met. As the accidents are DEC-A, the single failure criterion has not been applied and unavailability of equipment due to maintenance has not been considered. Moreover, a consequential LOOP is not considered in these analyses. However, the RP has applied conservative assumptions for system performance and initial conditions.

635. In a loss of feedwater fault, the temperature of the secondary side rises and the SG level decreases. Reactor trip occurs when the SG low level 1 signal is generated. The ASG [EFWS] is normally actuated when the SG level low 2 signal is generated. However, in the TLOFW fault sequence, the ASG [EFWS] does not actuate and pressure and temperature in both the primary and secondary systems rises until the VDA [ASDS] opening setpoint is reached, which limits secondary pressure. At this point the VDA [ASDS] alone cannot remove sufficient heat from the RCP [RCS], and the PSVs cyclically open to limit pressure. When the core outlet temperature reaches 330 °C the operator begins to perform actions to depressurise the primary circuit and the RCP [RCS] pressure drops rapidly, leading to the collapsed level to drop below the top of the core and causing a relatively small spike in PCT (~ 355 °C). The safety injection signal is generated by pressuriser pressure low 3, and the MHSI begins to compensate for the loss in the RPV water level. Eventually, the entry criteria for RHR are met and heat removal is provided for the long term. Over the whole transient, low levels of oxidation and hydrogen generation are predicted by the analysis, however this is within the RP's acceptance criteria.

636. For the SB-LOCA, the normal protection is provided by reducing the RCP [RCS] pressure via the MCD automatic procedure until the safety injection pressure is reached. In the scenario analysed, reactor trip is actuated as the pressuriser pressure decreases to the pressuriser pressure low 2 setpoint, which results in turbine trip and closure of the ARE [MFFCS]. Once the safety injection signal is reached at the pressuriser pressure low 3 setpoint, the MHSI are started. However, since the VDA [ASDS] is assumed unavailable, the RCP [RCS] pressure remains high and MHSI is unable to be injected. Unlike the TLOFW fault in which the PSVs are opened when the core outlet temperature reaches 330 °C the SB-LOCA analysis simply applies a 30 minutes delay from the beginning of the fault. The depressurisation allows safety

injection and a very similar behaviour to the TLOFW fault observed. The RP's analysis shows that all acceptance criteria are met.

637. The origin of the 330 °C limit is not explained. Moreover, it is unclear why the RP uses the 330 °C as the prompt for operator action in the TLOFW fault in contrast to the assumption of 30 minutes delay in the SB- LOCA. From my examination of the analysis I note that the 330 °C limit is not reached during the SB-LOCA transient and 330 °C is reached after approximately 40 minutes in the TLOFW accident. As such I am satisfied that the RP has made conservative assumptions on operator actions. I am satisfied that the lack of explanation for this is a minor shortfall.

638. In my opinion the feed and bleed function is represented quite simplistically within the analysis, resulting in a fast depressurisation of the primary circuit and brief core uncovery. A more controlled depressurisation may be beneficial to reduce the thermal stresses on components and this should be considered by a future licensee during the development of operating instructions. However, I am content to judge that the approach used by the RP in the analysis is conservative and appropriate for GDA to demonstrate the capability of the feed and bleed function.

639. With the above in mind, I am satisfied that the RP has demonstrated feed and bleed as a viable diverse means of protection for frequent faults when secondary cooldown is unavailable.

Secondary Passive Heat Removal System (ASP [SPHRS])

640. The ASP [SPHRS] is an F-SC3 system for passive heat removal from the SGs. Unlike several of the other safety measures described within this section, the ASP [SPHRS] is a dedicated DEC-A safety feature and is not credited for demonstrating diverse protection for any design basis accidents. In this section I present my assessment of how the ASP [SPHRS] adds to the defence in depth of the generic UK HPR1000 design.

641. The ASP [SPHRS] consists of three trains, one per SG. In a fault in which the SG water level reduces, the normal protection is provided by the ASG [EFWS]. However, if ASG [EFW] fails, the ASP [SPHRS] setpoint will be reached; ASP [SPHRS] is actuated when the SG low level 3 signal is generated.

642. In a fault such as loss of secondary heat removal, the battery powered VDA [ASDS] initially removes heat until the setpoint for ASP [SPHRS] initiation is reached. At this point, the ASP [SPHRS] isolation valves are automatically opened by the KDS [DAS]. Steam from the SGs is transmitted to the ASP [SPHRS] heat exchanger, where it is condensed and transfers heat through heat exchangers to the large ASP [SPHRS] tank (3035 tonnes). The condensed water is then recirculated to the SG via natural circulation. The water from the ASP [SPHRS] tank evaporates and is then released to the atmosphere. Each SG is equipped with an ASP [SPHRS] heat exchanger capable of removing at least [redacted] MW decay heat (Ref.126).

643. The ASP [SPHRS] is capable of providing heat removal in the following beyond design basis events:

- Total loss of AC power (TLACP) (i.e. LOOP + CCF of EDG + CCF of SBO).
- Total loss of cooling chain with loss of the secondary cooldown.
- Total loss of feedwater (TLOFW) (i.e. loss of normal feedwater + CCF of ASG [EFWS]).

644. The first two sequences involve failure of the primary and diverse means of protection. For the TLOFW, whilst feed and bleed is identified as the diverse means of protection,

the ASP [SPHRS] would, in reality, act before feed and bleed was initiated. Feed and bleed is therefore identified as F-SC2, and the ASP [SPHRS] is therefore only credited for DEC-A sequences and is F-SC3. I am content that this classification is appropriate and that the ASP [SPHRS] provides additional defence in depth which, in my opinion, should be acknowledged as a strength to the generic UK HPR1000 design.

645. The RP has presented analysis to demonstrate the effectiveness of the ASP [SPHRS] in Ref. 127. Within this, the RP explains that the TLOFW fault sequence bounds the TLACP because the TLACP results in a faster reactor trip, a faster trip of RCPs and a trip of the pressuriser heaters (RCPs and pressuriser heaters are an important heat source). Similarly the RP argue that the TLOFW bounds the above total loss of cooling chain sequence, as the total loss of cooling chain results in a faster reactor trip and a faster trip of the RCPs, and the CCF of secondary cooldown occurs after reactor trip. Whilst the initiating events are very different, the transients are similar and the all depend on how much heat can be removed from the ASP [SPHRS]. With this in mind, I am convinced that the RP's approach to bound these accidents with the TLOFW sequence in the demonstration of the effectiveness of the ASP [SPHRS] is appropriate.

646. The analysis, presented in Ref. 127, has been performed using the LOCUST code. As the fault sequence involves two phase flow modelling, I consider this code to be appropriate. Similar to several loss of heat removal faults, the RP claim that if the core remains covered then no fuel damage will occur. This is covered in Section 4.3 and I am satisfied that it is also appropriate here. The aim of the analysis is therefore to demonstrate that the ASP [SPHRS] ensures that the core remains covered.

647. The analysis has been performed from the full power case, since this results in the highest heat load to be removed by the ASP [SPHRS]. Consistent with the RP's analysis rules for DEC-A events, the RP has not assumed a single failure or equipment unavailability for preventative maintenance. Therefore all three trains of ASP [SPHRS] are assumed available. A consequential LOOP is not considered, which is conservative for this type of fault. I judge that these assumptions are appropriate and meet my expectations for a DEC-A sequence, as informed by NS-TAST-006 and SSG-2 (Refs. 4 and 9).

648. Although the TLOFW is a DEC-A sequence, the RP has still applied a 30-minute delay to the operator actions following the first significant signal (which is shortly after the initiating event). This delays tripping the pressuriser heaters and RCPs, maximising the heat input for the ASP [SPHRS] to remove. The RP has also assumed that the CVCS let down line remains open, therefore reducing the RCP [RCS] inventory. The penalising failure/success of F-SC3 SSCs is normally expected to be applied in DBA, and I consider that it is conservative to apply this assumption in the DEC-A analyses. The RP has applied additional conservative assumptions such as maximum core power, minimum loop flow, maximum core bypass and others. These assumptions are similar to those applied in DBA and are conservative. With this in mind, I am satisfied that the RP has applied conservative assumptions, consistent with the expectations for DBA, therefore I am satisfied that they are adequate for analysis of this fault.

649. The analysis shows that following the TLOFW, the water level drops and the SG low level 1 signal is reached, actuating reactor trip and subsequently turbine trip. There is an initial heating of both the RCP [RCS] and secondary circuit and the VDA [ASDS] set-point is reached. The VDA [ASDS] limits the pressure on the secondary side and the SG level is reduced until the SG level low 3 signal is generated. The maximum power is predicted to be around [redacted] MW per SG. At this time, the heat input from the decay heat, pressuriser heaters and RCPs is greater than the capacity of the ASPs and the PSVs open and close cyclically until the operator trips the pressuriser heaters and RCPs. After this point the ASP [SPHRS] begins to remove more heat than is input and the pressure and temperature in the SG begins to decrease, reducing RCP [RCS]

pressure and temperature. The power of the ASP [SPHRS] gradually decreases as the heat input decreases, and water consumption slows. With the cyclic opening of the PSVs ended, the RCP [RCS] inventory becomes stable. As the RCP [RCS] cools in the long term the water level drops, but remains well above the inventory required to keep the core covered in the long term.

650. Since the ASP [SPHRS] is a notable feature of the UK HPR1000, I commissioned my TSC to perform confirmatory analysis on the effectiveness of the ASP [SPHRS] for the TLOFW fault. The TSC's analysis (Ref. 128) found that based on the design information provided by the RP, the ASP [SPHRS] is likely to be capable of significantly higher heat removal than reported by the RP. To make comparable analyses, my TSC needed to artificially reduced the heat transfer area of the ASP [SPHRS] by a factor of 0.64. The system response of the secondary side is very similar in the modified case.

651. The TSC analysis also revealed that the RP's analysis assumes that MHSI is unavailable as the operator manually actuates a permissive signal (P11, in accordance with operating procedures), which blocks the pressuriser pressure low 3 signal from triggering safety injection. The TSC analysis with safety injection available shows that the MHSI injects cyclically as the RCP [RCS] pressure decreases and the RPV level remains higher than that predicted by the RP. The TSC analysis therefore demonstrates that the RP's analysis is conservative, both in the performance of the ASP [SPHRS] and the availability of systems (MHSI) to maintain water level.

652. I am therefore satisfied that the RP has demonstrated that the core remains covered using conservative analyses, meeting my expectations for FA.7.

653. The RP has demonstrated in Appendix 4C of Ref. 127 that the ASP [SPHRS] can remove heat for 72 hours following actuation, before the ASP [SPHRS] tank needs to be refilled. The RP's calculation is based on conservative assumptions, such as a high decay heat, a high, constant heat transfer to the ASP [SPHRS] and no other environmental losses. Similar calculations were made by my TSC using the maximum power of the ASP [SPHRS] observed in its analysis (~26 MW). My TSC found that using conservative assumptions the ASP [SPHRS] tank inventory should provide heat removal for approximately 76 hours.

654. The three trains of ASP [SPHRS] isolation and control valves are powered by the battery backed LVP/LVQ[†] DC switch boards. Therefore, it should be noted that in the event of a TLACP the valves should be operable for at least 24 hours. To meet the 72 hours of operability, however, the EDGs, SBO DGs or mobile DGs must be available after 24 hours to supply the batteries. The site layout is site specific, and arguments have not been made regarding satisfying this requirement. The arrangements for delivering the required functions will therefore need to be confirmed by the licensee as part of the site specific design and safety case.

655. With the above in mind, I am satisfied that the RP has demonstrated that sufficient margin, in both time and water level, is provided by the ASP [SPHRS] to provide core cooling without core damage. This is aligned with my expectation for FA.7. In my opinion the ASP [SPHRS] is an important feature of the generic UK HPR1000 design which strengthens the defence in depth against a number of faults involving a loss of secondary cooling.

[†] *LVP supplies Division A. LVQ supplies Division B and C.*

Loss of Ultimate Heat Sink

656. A loss of ultimate heat sink fault involves a total loss of SEC [ESWS] or a complete failure of the pumping station. This system provides cooling water to the RRI [CCWS] which in turn cools the RCPs and RHR (when shutdown). The SEC [ESWS] consists of three independent trains; Train A and B each have redundant sets of pumps and filters while Train C has a single pump and filter. A loss of ultimate heat sink is an overheating event which may cause overpressure of the primary circuit or fuel and cladding damage. It may also induce a failure of the RCP seals. The loss of SEC [ESWS] will cause the RCPs to stop and means that RRI [CCWS] is not available to support RHR for long term cooling. Instead, following reactor trip on low RCP speed the decay heat can be removed via the secondary side using ASG [EFWS] and VDA [ASDS].

657. The RP has not undertaken a detailed assessment of all potential causes of a loss of ultimate heatsink during GDA and this will need to be done by a licensee. As such, the RP has not identified this fault based on initiating event frequency. Instead, the RP has analysed a LUHS for 100 hours Ref. 129 as a DEC-A sequence, following the guidance within IAEA SSG-2 (Ref. 8). In the UK, consistent with SAP EDR.3 and operating experience, it is my expectation that a CCF of the SEC [ESWS] (for example due to marine clogging of seawater inlets) leading to a loss of heat sink should be considered as a design basis fault, potentially as a frequent fault depending on the detailed design, location of the site and the resulting frequency of occurrence.

658. However, given that the SEC [ESWS] is a three-train system with redundancy within two of the trains, I am content to accept that the design should be tolerant to single failures and the risks of CCF can be reduced during detailed design. In addition, the protection against loss of heat sink is provided by the F-SC1 ASG [EFWS] and VDA [ASDS] (which are not cooled by the RRI [CCWS]), with additional defence in depth from feed and bleed and ASP [SPHRS] as discussed in the sub-sections above. Given the provision of defence in depth (as may be expected for a frequent fault) and the application of DBC-4 acceptance criteria, I am satisfied that informed judgements can be made on the adequacy of the generic UK HPR1000 design against loss of heat sink faults in GDA, even if the initiating event frequency was to change following detailed design.

659. The analysis of a loss of ultimate heat sink presented within Ref. 129 has been performed using LOCUST and the key assumptions are chosen to penalise the conditions for RCP seals and ASG [EFWS] water consumption. I am satisfied that the assumptions on initial plant conditions and system performance are conservative. The analysis concludes that the RCP pump seal tightness can be maintained to ensure primary circuit integrity and that there is sufficient feedwater available to ensure heat removal.

660. As noted in Section 4.3, the ASG [EFWS] is sized based on the FLB accident and [redacted] tonnes of feedwater is used to reach the safe state. In comparison, for the LUHS Ref. 129 predicts that [redacted] tonnes of feedwater are necessary for 100 hours. The RP notes that at least [redacted] tonnes are available in the ASG [EFWS] tanks ([redacted] tonnes per train). It is therefore necessary to refill the ASG [EFWS] tanks to maintain cooling and this is done using the ASP [SPHRS] tank which contains an additional 3035 tonnes. The refilling of the ASG [EFWS] tanks by ASP [SPHRS] starts approximately 29 hours after the start of the fault sequence.

661. Based on my review of Ref. 129 I am satisfied that there is sufficient water available to protect against the LUHS for 100 hours fault and that there is sufficient time for the operators to line up the ASP [SPHRS] to replenish the ASG [EFWS]. The frequency of a loss of ultimate heat sink fault will need to be confirmed by a licensee and the safety

case developed accordingly, but I am content that this can be progressed as normal business.

4.4.1.2 Loss of Cooling Chain (non-closed RCP [RCS])

Containment Heat Removal System (EHR [CHRS])

662. The mitigation against a loss of cooling described in the previous sub-section is only effective if secondary cooldown is available. In normal plant states and accident conditions where the RCP [RCS] is non-closed‡ or non-pressurisable§ the conditions for heat removal from the SGs are not achievable. Long-term heat removal is normally provided by RHR.

663. If RHR fails in these states the EHR [CHRS], which is a DEC-A system, provides the diverse means of long-term heat removal. The EHR [CHRS] is an F-SC3 system as it provides a backup to an FC2 function. I am content that this is appropriate and consistent with the RP's method for safety classification (Ref. 11) and ONR's guidance in NS-TAST-GD-094 (Ref. 4). The EHR [CHRS] system consists of two independent trains each with an intake line from the IRWST, a pump and a heat exchanger which is cooled by the RRI [CCWS] or the ECS [ECS]. Each train of EHR [CHRS] is completed by a spray ring around the inside of the upper containment. Each train is backed up by electrical supply from the EDGs and SBO diesels.

664. The RP has identified that a SB-LOCA with loss of LHSI (State A) is the most onerous case for the analysis of heat removal via the EHR [CHRS] and it can bound faults when the RCP [RCS] is not closed. On the basis that this fault occurs at the highest core power (and therefore has the greatest heat in the primary coolant), and the SB-LOCA is greater than other break sizes (e.g. RCP seal leakage), I am content that this is a reasonable approach. The analysis of SB-LOCA with loss of LHSI is reported in Ref. 78 where the analysis is undertaken using LOCUST (for analysis of the thermal hydraulics conditions within the reactor) and of ASTEC for the analysis of the containment thermal response.

665. In this sequence, an SB-LOCA occurs and is initially protected against by MCD and MHSI whilst the pressure and water level is large enough for secondary heat removal to be effective. However, LHSI fails and therefore long-term cooling via RHR is not available. The RP assumes that 30 minutes after reactor trip the operator starts two trains of RBS [EBS] pumps and opens three trains of VDA [ASDS] to cooldown the primary circuit. After the containment pressure reaches [redacted] MPa two trains of EHR [CHRS] are manually actuated to cool the IRWST. The decay heat is removed via the EHR [CHRS] and VDA [ASDS] and the primary coolant inventory is maintained by MHSI.

666. The ASTEC code was reviewed as part of the severe accident analysis assessment (Ref. 86). ONR's Severe Accident Analysis inspector has judged that ASTEC is suitable for use for modelling containment thermal hydraulics in the analysis of the effectiveness of the EHR [CHRS].

667. The analysis (Ref. 78) shows that the core remains covered, the containment pressure remains below the design pressure and the IRWST temperature is maintained at around 80°C, demonstrating that heat can be removed in the long term. The analysis has not considered any single failures affecting the safety systems and therefore there

‡ *The RCP [RCS] is non-closed when the pressuriser vent line is opened, the reactor vessel head vent line is opened, and/or the RCP [RCS] is not pressurisable.*
§ *The RCP [RCS] is pressurisable when both of the reactor vessel head venting line sleeve and the pressuriser vent blind flange are installed. The RCP [RCS] is not pressurisable when at least one of these is removed.*

are three trains of MHSI and ASG [EFWS] and two trains each of RBS [EBS] and EHR [CHRS] taken into account in the analysis. Given that the sequence already involves a total loss of LHSI for long term cooling (a FC-2 function) I am content that this is an acceptable approach and considering a further random single failure would be unnecessarily conservative. With this in mind, and that the RP has chosen the worst initial configuration I am content that my expectations for conservative analysis have been met. In addition, I note that minimum system performance has been assumed and that conservative initial conditions have been used. I am therefore satisfied that the analysis has been carried out in accordance with the expectations of FA.7.

668. Whilst the transient analysis report (Ref. 78) has assumed both trains of EHR [CHRS] are available, I note that the system design manual (Ref. 130) includes claims for a single train:

- activating one containment spray train of the EHR [CHRS] after 12h grace period can keep the pressure of the containment below the containment design pressure (0.52 MPa abs).
- during long-term operation of EHR [CHRS], one train of EHR [CHRS] can keep the pressure of the containment below [redacted] MPa abs.

669. The analysis that substantiates these claims has been performed against a more severe transient, the LB-LOCA with core melt, within the Severe Accident Analysis topic area and has been covered within the Severe Accident Analysis Step 4 Report (Ref.86). ONR's Severe Accident Analysis inspector has found that RP has adequately substantiated claims that the EHR [CHRS] is capable of removing sufficient heat such that the above criteria are met.

Extra Cooling System (ECS [ECS])

670. The ECS [ECS] is an F-SC3 system which can provide an alternative heat sink for the EHR [CHRS] or the PTR [FPCTS]. The system consists of two trains each with a pump, heat exchanger, cooling tower, makeup pool, filter and surge tank. These are located within the Extra Cooling System and Fire-fighting Water Production System building (BEJ).

671. The ECS [ECS] is claimed to support the EHR [CHRS] and PTR [FPCTS] in the following scenarios:

- Total loss of cooling chain with Reactor Coolant Sealing Leakage (POS A).
- Total loss of cooling chain (POS D).
- SBO (POS D).
- SBO (POS G).

672. The detailed design of the ECS [ECS] is not yet complete and further information will need to be produced to support an operational safety case. Nevertheless, the System Design Manual for ECS [ECS] (Ref. 131) contains the design requirements for the flow rates of the heat transfer circuits and the maximum water temperatures. Ref. 131 also notes that the sizing of the heat exchangers and mechanical draught cooling towers must ensure that the system can remove the heat load and provide cooling water within the limiting temperature for the most onerous case. It also specifies that the capacity of each makeup pool can supply the water required by one train of ECS [ECS] continually for 24 hours, and that after 24 hours the pools can be replenished (for example, by temporary mobile pumps).

673. As this is a simple system I am content that this is adequate information for GDA. I am satisfied that the design and analysis work needed to demonstrate that these requirements will be met is normal business and will be developed prior to operation. I

am however content to judge that this system provides additional diversity in the response to loss of cooling faults.

Safety Chilled Water System (DEL [SCWS])

674. The DEL[SCWS] normally provides chilled water to cooling coils or cooling circuits for a number of ventilation systems. In the case of RRI [CCWS] and/or SEC [ESWS] failure, the DEL [SCWS] provides a diverse cooling chain to cool the LHSI pumps of trains A and B instead. During a total loss of cooling chain fault with RCP seal leakage in state A or in state D, the diverse cooling chain is connected to LHSI pumps automatically by the high temperature or low flowrate signal of RRI [CCES]. During SBO in State D, the diverse cooling chain is connected to the LHSI pumps manually to ensure the cooling of LHSI pump motors. I have chosen not to assess these sequences in detail but I note the following points:

- The RP has concluded from transient analysis of the limiting cases (Refs 132 and 133) that all relevant acceptance criteria are met, applying the appropriate delays to the required operator actions.
- The automatic switching to DEL [SCWS] for LHSI cooling is a FC3 Function delivered by the F-SC2 SAS.
- The manual switching function is a FC3 function which can be delivered by SAS or KDS [DAS].
- The cooling requirements of the LHSI pumps is small in comparison to the requirements of the ventilation systems in normal operation (Ref. 134).

675. I am therefore content that the RP has demonstrated the effectiveness of DEL [SCWS] as a diverse cooling chain for the LHSI pump.

4.4.1.3 Station Blackout (SBO)

676. The RP defines a SBO as a LOOP with CCF of the EDGs. The RP has identified SBO as a DEC-A event. However, the RP has also identified that the SBO generators provide the diverse means of protection for frequent LOOPs with failure of the EDGs. The RP has assessed the consequences of an SBO in both the reactor and the SFP. My assessment of the RP's safety case for the SFP is presented in Section 4.5. This section presents my assessment of the RP's reactor SBO safety case.

677. To demonstrate the effectiveness of the safety measures for the reactor, the RP has analysed two accident types:

- SBO whilst the RCP [RCS] is closed (POS A – C3a) (Ref. 135).
- SBO whilst the RCP [RCS] is not closed (POS C3b /D) (Ref. 136).

678. For states where the RCP [RCS] is closed, the accident causes a coast down of the RCPs, a reactor trip (when at power) and a loss of heat removal. The temperature and pressure of the RCP [RCS] subsequently rise. The SBO generators are manually started. During this time cooling is initially provided via the SGs by the battery backed VDA [ASDS] alone, then subsequent along with ASG [EFWS] once the SBO generators have been started. It should be noted that in reality, the ASP [SPHRS] would initiate due to the low SG level prior to the start-up of the SBO generators. Whilst ASP [SPHRS] is not credited in Ref. 135, the RP has demonstrated the effectiveness of the ASP [SPHRS] against the most bounding case for heat removal in Ref. 127. My assessment of this safety measure is presented in Section 4.4.1.1.

679. For the non-closed configuration (i.e. in some shutdown states) the EHR [CHRS] and ECS [ECS] are required for heat removal. In the pressurisable configuration the operator must use the feed and bleed function in the long-term to manage RPV water

level and pressure, whereas for the non-pressurisable case only LHSI is used. Based on the similarity of the progression of these faults the RP has grouped them as one DEC-A event.

680. The RP has separated the two faults based on the accident progression into SBO during closed and non-closed configurations. My assessment of the RP's safety case for closed and non-closed configurations is provided in the following sub-sections.

SBO During Closed RCP [RCS] Configuration

681. Ref. 135 presents the RP's transient analysis of the SBO during the full power case using the LOCUST code. The SBO can lead to a decreasing RPV water level and requires two phase modelling, therefore the use of the LOCUST code is appropriate.

682. In Ref. 135 the RP claims that so long as the core remains covered no fuel damage will occur. No evidence is provided for this claim within Ref. 135. However, I note that the LOOP accident analysis is equivalent to the SBO analysis in the short term therefore I am satisfied with this claim. The RP states that the objective of the analysis is instead to demonstrate that the design limits of the thermal barrier of the RCPs are not exceeded. This is common practice for analysis of this sequence, and I judge it appropriate.

683. The VDA [ASDS] and ASG [EFWS] are F-SC1 as they provide the primary means of protection for several faults. The SBO DGs are F-SC2. The KDS [DAS] is used to perform the safety functions, which is also a F-SC2 system. As the KDS [DAS] and SBO DGs provide the diverse means of protection for a frequent fault (i.e. LOOP + CCF of the EDGs) I consider this classification appropriate and meets my expectations for ECS.2.

684. The RCPs incorporate a standstill seal system, which prevents leakage during SBO conditions. However, the RP has not included the values of these success criteria within Ref. 135, and instead cites the RCP [RCS] system design manual. Ref. 135 could benefit from including these figures, and I have identified this as a minor shortfall.

685. In Ref. 3, the RP has recognised the differing characteristics of the full range of plant configurations and has grouped them based on fault progression. For closed configurations, the RP states that accidents that occur in POS A are bounding in terms of pressure and temperature, as the decay heat is larger than that in POS B and C. Since the analysis is focused on meeting the design limits of the shaft seal, I judge that this is appropriate and meets my expectation for FA.6 in that the most onerous configuration is chosen.

686. The RP has not applied an additional single failure criterion in its analysis to demonstrate the effectiveness of the SBO DGs as a demand would only be placed on them following a CCF in the single failure tolerant EDGs. I am content that this is appropriate. The RP has assumed that no preventative maintenance (resulting in unavailability of the SBO generator or ASG [EFWS]) is being undertaken. The analysis therefore credits both trains of ASG [EFWS]. The SBO system design manual (Ref. 137) clearly states that one SBO DG is sufficient to provide electrical loads for dominant sequences, including the SBO at full power. Moreover, the EMIT strategy for electrical systems (Ref. 138) states that maintenance of one SBO DG is permissible in all operating states. In my opinion, there is an inconsistency between the safety analysis and the maintenance assumptions and the SDM, as the safety analysis does not demonstrate that one train of SBO/ASG [EFWS] is sufficient to remove heat during an SBO.

687. Informed by FA.6, it is my expectation that if maintenance is expected to be performed, then this should be taken into consideration in the DBA. Conversely, if the SBO DGs are assumed to be available the analysis of the SBO during full power operations, then the maintenance should be scheduled in such a way to ensure sufficient availability of the SBO DGs to deliver the required safety functions. The development of the maintenance schedule is for a licensee and this will need to ensure consistency with the safety analysis. I therefore have raised the following Assessment Finding:

AF-UKHPR1000-0237 – The Licensee shall, as part of detailed design, demonstrate that the maintenance schedule for the station black-out diesel generators is consistent with the safety analysis for relevant faults and resolves the shortfalls identified in GDA.

688. The RP's analysis shows that following reactor trip, the primary circuit pressure slowly increases as the VDA [ASDS] alone is not capable of removing all heat. The PSVs are predicted to open one time, which limits the pressure transient. However the temperature and pressure of the RCP [RCS] begins to rise again shortly after and only appears to stabilise after the initiation of the second train of ASG [EFWS], which appears to prevent further opening of the PSV. For this reason, the RPV water level is unaffected and the core remains covered throughout the transient. In my opinion if the second SBO DG was not available, the PSVs would cycle, releasing primary coolant and the resulting RPV level may be significantly lower.

689. I contracted my TSC to perform confirmatory analysis of the SBO sequence. My TSC concluded that there is close agreement between the predicted progression of the sequence between both sets of analysis and has advised that the inputs used by the RP have been conservatively applied (Ref. 139). In both the TSC's and the RP's analysis, the core remains covered and the pressure and temperatures remain below the design limits. I am therefore satisfied that the RP's analysis demonstrates that the consequences are acceptable and within the criteria set by FA.7.

690. Ref. 135 also claims that the SBO loads can be supplied for three days in this configuration. The RP claim that this sufficiently covers the requirement for diversity for frequent faults (i.e. short term and medium term LOOPs). However, as noted previously, the length of the frequent LOOPs requires site specific information, and this should be confirmed by the licensee.

691. I am therefore satisfied that if two trains of ASG [EFWS] are ensured to be available that the generic UK HPR1000 design should be capable of maintaining heat removal for three days after an SBO during plant states where the RCP [RCS] is closed.

SBO During Non-Closed RCP [RCS] Configuration

692. The SBO during non-closed RCP [RCS] configuration is classed as a DEC-A fault and involves a LOOP plus the additional failure of the EDG to start. The non-closed configuration is in place during periods of refuelling and maintenance operations. The worst time for a loss of cooling accident to occur is when the water level is at ¾ loop level. This occurs in POS C3a, POS C3b and parts of POS D. The RP has termed these conditions collectively as POS G. The RP has estimated that the frequency of an SBO coincident with being in one of the during POS G operating states is 1.77×10^{-8} pa.

693. Ref. 136 presents the RP's transient analysis of the SBO during some shutdown states (i.e. those in the non-closed configuration) using the LOCUST code. The analysis only covers the cooling for the reactor. It should be noted that an SBO could put concurrent demands on the ECS [ECS] to cool both the reactor and SFP. However, the most challenging states for the reactor and the SFP cannot occur simultaneously. This is because the most recently irradiated fuel has significantly higher decay heat and is either assumed to be all in the core or all in the SFP. The analysis requires modelling

of flow through the PSVs and LHSI injection therefore the use of the LOCUST code is appropriate.

694. The RP claim that if the core remains covered then fuel damage is avoided. The RP state, therefore, that the aim of the analysis is to demonstrate that the core remains covered. I judge that this is an appropriate success criterion.

695. The RP has performed analysis of two bounding cases, one in which the system is not pressurisable (and is at ¾ loop level, which is called POS C3b) and one in which the system is pressurisable (and is at ¾ loop operation, which is part of POS C3a). In both cases, the LHSI is initially used to restore the water level. However in the pressurisable case where steam is not evaporated into the large containment space, feed and bleed must be used to remove heat.

696. In both cases, the analysis applies conservative assumptions. For example, the worst possible decay heats based on shortest possible time to reach POS C3a and POS C3b are considered (and when all fuel is still present in the core). Moreover, the system performance is penalised.

697. For the non-pressurisable case, the RP presents the transient analysis and demonstrates that in the worst case 24.69 tonnes of water evaporates, leaving more than 55 tonnes of water available above the core.

698. For the pressurisable case, the RP's analysis shows that after LHSI is initiated the water level is restored. The LHSI flow decreases to zero as the system pressure builds. Following this, the pressure continues to rise until 32 bar is reached. At this point, the RP assumes that the operator opens the PSVs to allow injection of LHSI (the so called feed and bleed mode). After this point steam is transported to the containment and the EHR [CHRS] removes sufficient heat to cool the IRWST.

699. In both cases, once the heat removal is established the transients are stabilised and heat can be removed for as long as sufficient water (see Section 4.4.1.) and power are supplied.

700. I am satisfied that, if an SBO were to occur during shutdown conditions when the RCP [RCS] was not closed, if the SBO DGs, ECS [ECS] and EHR [CHRS] are available then the fuel would remain covered and no fuel damage would occur.

701. Similarly to the full power case, neither the single failure criterion or maintenance assumptions are applied. Unlike the full power case, however, the SBO DG system design manual (Ref. 137) states that two trains are required to remove heat from the core in the states covered in this analysis, which agrees with the assumptions made in the analysis (Ref. 136). However, both the analysis (Ref. 136) and system design manual (Ref. 137) are inconsistent with the assertion made in the EMIT strategy for Electrical Power Systems (Ref. 138), which states that maintenance of the SBO DGs can be performed in all states. For this reason AF-UKHPR1000-0237 (raised above) is also relevant to this analysis.

4.4.2 Anticipated Transient Without Scram (ATWS)

702. The RP has submitted a number of reports which consider potential scenarios where reactor trip is not actuated following a fault, either due to a failure of the protection system or a mechanical failure of the RCCAs to insert. A failure of the protection system can be protected against by the diverse reactor trip functions of KDS [DAS] but for scenarios where the RCCAs fail to insert, the RBS [EBS] system is required to insert negative reactivity to achieve reactor shutdown. The list of DEC-A events presented in Chapter 13 of the PCSR is supplemented by other ATWS analyses to

demonstrate the effectiveness of the RBS [EBS] system in providing a diverse means of reactivity control for frequent faults (these are presented in Chapter 12 of the PCSR). In total, the safety case includes analysis of 12 ATWS scenarios, the majority of which involve a mechanical failure of the RCCAs to insert (identified as ATWS Rods). These are:

Chapter 12

- ATWS Rods - Forced reduction in Reactor Coolant flow (3 pumps).
- ATWS Rods - Uncontrolled RCCA bank withdrawal at a subcritical or low power startup.
- RCCA Bank withdrawal with failure of primary protection sensor.
- ATWS Rods – RCCA Bank Withdrawal at Power.
- ATWS Rods - RCCA Misalignment up to Rod Drop.
- ATWS Rods - Uncontrolled single RCCA Withdrawal.

Chapter 13

- ATWS Rods – LOOP.
- ATWS Rods – SB-LOCA RPV water level remains above core.
- ATWS Rods – Loss of main feedwater.
- ATWS Rods – Excessive increase in secondary steam flow.
- ATWS Rods – ATWS Spurious pressuriser spraying.
- ATWS Rods – Steam line break downstream of MSIV.

703. In my opinion this is a comprehensive set of analysis and I am content that the RP has provided arguments to explain why these are bounding of other scenarios (although I have not examined all of these arguments). The protection against ATWS scenarios relies on the influence of the moderator and fuel temperature coefficients which act to limit reactivity until negative reactivity is provided by the injection of borated water by the RBS [EBS] system. RBS [EBS] is actuated on a reactor trip and RCCAs high rod position signal.

704. To gain confidence in the ATWS analysis I have chosen to sample the LOOP and loss of main feedwater faults (Refs. 140 and 141) and I commissioned my TSC to undertake confirmatory analysis of these sequences. The TSC analysis of both LOFW ATWS and LOOP ATWS is presented in Ref. 142. My TSC undertook the analysis using the ATHLET code and a coupled 3D neutron kinetics model. Within the analysis, the TSC used the same assumptions and boundary conditions for the plant conditions.

705. However, some core related assumptions could not be implemented, since the TSC used a physically realistic approach to analyse the core behaviour with 3D neutron kinetics, used with conservative assumptions and parameters. In this context, the TSC cannot consider any conservative value for integral reactivity feedback coefficient (as the RP has done). Instead, the equilibrium cycle at BOC burnup distribution was chosen in order to describe the state of the core from a neutronics point of view. This choice was made since the equilibrium cycle is the most representative of the burnup distribution during reactor operations. Furthermore, a realistic critical boron concentration has to be considered by the TSC ([redacted] ppm in this case) instead of the artificial initial null concentration that is considered by the RP.

4.4.2.1 LOFW ATWS

706. The LOFW leads to a decrease in the steam generator (SG) water inventory, triggering a reactor trip by the SG level (narrow range) low 1 signal. However, the rods fail to insert and the reactor trip does not occur. The triggering of the ATWS signal, which is followed by high-pressure boron injection, represents the additional independent way

to insert negative reactivity into the reactor and to mitigate the risks associated with ATWS. Emergency feedwater (ASG) is used to maintain secondary heat removal. Within Ref. 140 the RP concludes that the DNBR remains higher than the minimum value and all acceptance criteria are met.

707. My TSC's analysis of this fault is presented in Ref. 142 and this supports the RP's claim that the DNBR remains higher than the acceptance criteria. However, several discrepancies have been observed between my TSC's analysis and the RP's analysis. These discrepancies can be explained by the differences in modelling between the TSC and the RP. The main modelling difference affecting the scenario results is the one related to heat transfer in the SGs. The steam generators are finely nodalised in ATHLET code used by the TSC and allow heat transfer even if only one node is in contact with the water. This approach differs from GINKGO which has a single lumped node based on a correlation function of the water level. This difference and the minimisation of heat transfer in the SGs by the RP has the following effects:

- The RP predicts that less heat is removed from the primary side than my TSC, resulting in a reduction in SG water inventory and higher primary side pressure (when compared to the TSC analysis).
- The higher primary side temperature in the RP's analysis leads to stronger reactivity effects and a faster decrease in reactor power (than the TSC analysis).

708. Despite these differences, both the RP and TSC's analysis shows a return to criticality before the RBS [EBS] water enters the RPV later in the transient to increase the boron concentration and supress the reactivity. The TSC analysis predicts that the reactor remains close to criticality throughout the period modelled where the RP shows a much greater margin to criticality. This is mainly due to the boron concentration increase in the core which is almost twice as fast in the RP's simulation. This happens despite similar primary and RBS [EBS] mass flow rates. This can be explained by the different boron concentration in the RBS [EBS] system and/or differences in the boron transport model used.

709. In my opinion the TSC analysis provides confidence in the RP's claim that the acceptance criteria are met for a LOFW ATWS. While both the RP and TSC analysis predict a brief return to criticality before the RBS [EBS] injection is effective, I am satisfied that this transient does not result in any fuel damage. I am content that the analysis demonstrated that the protection provided by secondary side heat removal and injection of borated water through RBS [EBS] is adequate to return the reactor to a safe stable state.

4.4.2.2 ATWS LOOP

710. The LOOP leads to loss of electrical power for all auxiliary plant equipment, including the Reactor Coolant System (RCS) pumps, condensate and main feed water pumps. After LOOP, the electrical power is expected to be provided either by the plant generator or by the EDG. Together with the failure of reactor trip the LOOP results in an overheating of the core that is compensated in the short term by the negative moderator density and Doppler reactivity feedbacks. In the long term, the boron injected into the core by the RBS [EBS], activated by the ATWS signal and powered by an EDG, ensures the core subcriticality. The RP's analysis of this fault is presented in Ref. 141 and concludes that DNBR remains above the minimum value and acceptance criteria are met.

711. As with the LOFW ATWS, while the TSC analysis also predicts that DNBR remains higher than the minimum value, some differences in the progression of the sequence were observed:

- The minimal DNBR and the maximal primary pressure are less conservative in the TSC calculations because of the realistic approach using the 3D neutron kinetics model while the RP penalises the heat transfer from primary to secondary side and minimises moderator density feedback.
- In the RP's analysis, all three PSVs are opened during the first pressure peak and the pressure reaches almost [redacted] MPa. In the TSC analysis PSVs are activated three times during the transient, but only the first PSV opens. This behaviour indicates a larger amount of energy in the primary system in the RP's analysis.
- Later in the transient, the RP predicts a decrease in the core power that is not shown in the TSC's results. The decrease is caused by the higher energy level assumed in the primary system (i.e. lower moderator density) due to penalised heat removal through the SGs.

712. In both analyses, the core remains near criticality until the RBS [EBS] water enters the RPV. There are differences in the predictions of core power and reactivity during the transient with the RP predicting a short return to criticality just before RBS [EBS] injection is effective, where GRS predict a higher (but just sub-critical) reactivity throughout the transient. My TSC also made similar observations with regard to boron concentration to those described for the ATWS LOFW in paragraph 707 above. However I am content that these differences do not undermine the conclusions of Ref. 141 as they relate to differences in timings of events before RBS [EBS] injection but do not challenge the acceptance criteria.

713. In my opinion the TSC analysis provides confidence in the RP's claim that the acceptance criteria are met for ATWS LOOP and, as with the LOFW ATWS that the secondary side heat removal and injection of borated water through RBS [EBS] are adequate protection against this fault.

4.4.2.3 Common Findings

714. As a result of these discrepancies with the two cases discussed above, my TSC advised within Ref. 142 that ONR should seek additional ATWS analysis by the RP with a more realistic modelling of the neutron kinetics, together with a description of the boron injection modelling, to allow a better assessment of shutdown conditions. Whilst I agree that a less conservative and more realistic analysis would provide more confidence in the timings of the shutdown I have been content this has not been necessary for my judgements in GDA. The principal reason for this is that, whilst there are differences in the TSC and RP's analysis, both show margin to the DNB criteria and both predict shutdown within the 1000 seconds analysed. The differences highlight the contrasting approaches between the TSC and the RP; my TSC uses a best estimate code which is capable of realistic results whereas the RP's methods are more simplistic and are penalised for the specific criteria under consideration.

715. The confirmatory analysis also enabled me to gain further insights into the RP's methods and assumptions and I identified two aspects of the analysis which may be non-conservative. The first is the choice of Moderator Temperature Coefficient (MTC) and the second is the DNB criteria and use of radial power distributions (FdH) without uncertainties. I discuss each of these matters in the following paragraphs before coming to an overall conclusion on their significance.

716. During the development of the confirmatory analysis, my TSC noted that the RP used different values for moderator density feedback and Doppler feedback reactivity feedback in the two ATWS cases that it analysed. Specifically, for ATWS LOOP, the RP uses the reactivity coefficients from cycle C3 at BCX. For ATWS LOFW, the RP uses the reactivity coefficients from cycle C2 at BCX. In response to

RQ-UKHPR1000-1127 and RQ-UK HPR1000-1328 the RP explained (Ref. 6) that the ATWS analysis uses a bounding MTC in the following way:

- The bounding coefficient is identified by ranking the cycles by their absolute MTC value (here: C1 < C3 < C2 < Eq. at BCX).
- The core conditions of the most limiting case are then applied in the calculation.
- If the acceptance criteria can be met, this core condition is used for the analysis, otherwise the next case in the ranking is applied.
- This implies that the acceptance criteria are not met for either ATWS using the MTC of cycle 1 at BCX. For the LOFW ATWS, the criteria cannot be met either using the MTC of cycle 3 at BCX.

717. The choice of MTC has not been explicitly justified by the RP but it argues that the moderator temperature coefficient used envelops 99% of the operating time. ONR's Fuel and Core Inspector has considered this matter (Ref. 20) and concluded that, for the periods when the MTC will be non-conservative, other factors within the fuel data should partially compensate for the slightly non-conservative MTC assumption when determining the margin available to the DNBR limit in these faults. I am therefore content that the margins to DNB are not likely to be significantly affected by this matter, but this is not explained nor justified in the RP's safety case.

718. The second topic arose from my review of the assumptions within the analysis of RCCA misalignment ATWS (sub-section 4.3.4.3). From discussion with the RP and working with ONR's Fuel and Core inspector I have established that the RP has analysed this fault (and other ATWS faults) against the deterministic DNB method without consideration of uncertainties on FdH. This appears to be contrary to the general analysis rules within the DNBR design limit document (Ref 143) which is clear that where the deterministic method of DNB analysis is used it shall be used with uncertainties applied to the plant parameters.

719. I am content that other parameters have considered conservative assumptions and uncertainties and that the overall results are likely to be conservative, but I consider that there is a shortfall in the justification for using the deterministic DNB limit without consideration of uncertainties of radial power distribution for the analysis of ATWS faults. In my opinion this should be justified to demonstrate that the analysis is conservative as required by FA.7

720. I have therefore concluded that, while the RP has demonstrated acceptable margins to the acceptance criteria for the ATWS faults that I have sampled, the RP has not adequately justified the input assumptions used (the choice of reactivity coefficients, uncertainties for radial power distributions and the use of deterministic DNB limit). I am content to judge that this does not need to be addressed during GDA but I have raised the following Assessment Finding:

AF-UKHPR1000-0238 – The licensee shall justify the choice of reactivity coefficients, uncertainties for radial power distributions and criteria for departure from nucleate boiling used within the analysis of anticipated transient without scram events.

4.4.2.4 Conclusions for ATWS

721. Following my review of the ATWS faults, I am satisfied that PCSR Chapters 12 and 13 provide an adequate safety case to demonstrate the effectiveness of the protection against a range of ATWS events. Based on my assessment of a sample of the analysis I am content that, while there may be a return to criticality in the short term, the RP has demonstrated that the fuel acceptance criteria are met and that the RBS [EBS] system and secondary cooling can return the reactor to a safe stable state. The analysis shows that the PSVs are required to prevent overpressurisation of the primary circuit

and that they have sufficient capacity to do so. However, AF-UKHPR1000-0238 will need to be addressed by the licensee to justify some of the methods used.

4.4.3 SB-LOCA with Loss of Safety Injection

722. In the event of a SB-LOCA, the primary circuit needs to be depressurised to the MHSI injection pressure and this is achieved with the MCD function. If MHSI fails, the primary circuit needs to be further depressurised to the LHSI injection pressure. This further depressurisation is achieved manually using all three trains of VDA [ASDS] and is termed Low pressure full cooldown (LCD). Once the LHSI pressure is reached, the fault sequences progresses in the same way as other SB-LOCA faults, with long term cooling assured once RHR conditions are reached. The RP has analysed a SB-LOCA with total loss of MHSI in Ref. 144.

723. The RP has analysed two break sizes, a 2.5cm equivalent diameter break and a 5cm equivalent diameter break. For the larger break the RP has assumed that, following the automatic MCD the operator initiates LCD after 30 minutes. For the smaller break size, rather than using LCD the RP has chosen to assume a lower cooldown rate of [redacted] °C / hr as a more conservative assumption. Even with this slower cooldown the analysis shows that the core remains covered. The analysis concludes that the LOCA acceptance criteria for both break sizes with maximum PCT of [redacted] °C for the 5cm break.

724. The functions required to perform MCD and LCD are described within Ref. 145. The LCD function requires the operator to identify that MHSI has not initiated following MCD and perform a manual cooldown to reach LHSI pressure. The operator will have to choose whether to initiate LCD or a less demanding cooldown rate and the operator instructions for this will be developed at a later stage.

725. I am content that the assumption that the operator performs the necessary actions after 30 minutes is appropriate for GDA and that the approach to the analysis is consistent with the RP's deterministic rules and the expectations of FA.7 that such analysis should be performed on a conservative basis. Once the operating procedures have been developed the analysis should be reviewed to ensure that the assumptions on operator actions remain appropriate, however I am satisfied that this will be done as part of normal business as the safety case develops. I am content that the analysis presented in Ref. 144 demonstrates the effectiveness of the LCD function to allow LHSI injection in the event of a SB-LOCA with failure of MHSI.

4.4.4 Strengths

726. Following my assessment of the reactor DEC-A events I have identified the following strengths:

- The generic UK HPR1000 design contains a number of systems to protect against loss of cooling faults, providing levels of defence in depth independent of those claimed for design basis faults.
- The RP has identified a range of ATWS events and demonstrated the capability of the RBS [EBS] system to protect against these events without fuel damage.
- The RP has demonstrated that the reactor has sufficient protection against SBO in all operating states.
- The RP has demonstrated the effectiveness of the LCD function to allow LHSI injection in the event of a SB-LOCA with failure of MHSI.
- The analysis of DEC-A events has been carried out on a conservative basis and demonstrate that the consequences are acceptable, consistent with the expectations of SAPs FA.6 and FA.7.

4.4.5 Outcomes

727. As a result of my assessment of the reactor DEC-A events I have identified two Assessment Findings:

- to ensure the licensee defines maintenance requirements for the SBO DGs to ensure consistency between the maintenance schedule and the safety analysis.
- to ensure the licensee provides a justification for the choice of reactivity coefficients, uncertainties for radial power distributions and DNB criteria used within the analysis of ATWS events.

4.4.6 Conclusion

728. Based on the outcome of my assessment, considering ONR SAPs EKP.3, FA.7 and TAG NS-TAST-GD-006 (Ref. 4) and IAEA SSG-2 (Ref. 9), I have concluded that the analysis of UK HPR1000 reactor DEC-A events adequately meets my expectations for GDA. The RP has demonstrated the capability of the systems to prevent damage to the containment barriers during these DEC-A events. Subject to the licensee adequately resolving the Assessment Findings I have identified, I am satisfied that the consequences have been predicted conservatively and allow a demonstration that the consequences are ALARP.

4.5 Fuel Route Faults

729. The fuel route process for the UK HPR1000 consists of six main parts. These are: new fuel assemblies receipt and storage operations, core loading/unloading operations, reactor power operations, spent fuel assembly storage operations within the SFP, spent fuel assembly delivery to Spent Fuel Interim Storage (SFIS) and SFIS operations. As discussed in Section 2 above, transfer of casks between the spent fuel building and SFIS, repackaging of fuel assemblies and transfer of fuel off-site to a Geological Disposal Facility are out of scope of GDA.

730. The SFP is a steel lined reinforced concrete structure used for the temporary storage of irradiated and new fuel during refuelling, and the storage of spent fuel prior to interim storage. It is located in the fuel building, which is adjacent to the reactor building. The fuel pool contains neutron absorbing fuel racks, capable of storing spent fuel from roughly ten fuel cycles. The SFP is filled with boronated water, which both cools the fuel and ensures a large margin to criticality.

731. The SFP can also be hydraulically connected to a transfer pit and a loading pit within the fuel building. A fuel transfer tube connects the SFP to the area within the containment building which surrounds the RPV (the reactor cavity). During non-refuelling POS and conditions in which spent fuel is not being exported from the nuclear island, the SFP is isolated from the transfer tube, transfer pit and the loading pit via large sluice gates. During refuelling, the fuel transfer tube is opened, the SFP-transfer pit sluice gate is opened and a continuous pool is formed between the reactor pool (the filled reactor cavity), the transfer pit and the spent fuel pool. During fuel export (i.e. for interim storage) the sluice gate between the SFP and the loading pit is opened.

732. All fuel on-site will be in some part of the fuel route, and when full the SFP will contain multiple cores' worth of fuel. There is therefore the potential for faults arising within the fuel route to have significant radiological consequences should the fuel be exposed, damaged or lose cooling. In this section I have considered fuel route faults in two parts. In sub-section 4.5.1 I have considered the systems that are in place to ensure that there is adequate cooling and water inventory for the SFP (I have focussed my

assessment on the spent fuel pool as loss of cooling or inventory in the RPV or reactor pit is covered by the reactor faults described elsewhere in this report). In sub-section 4.5.2 I have considered potential faults which may occur during fuel movements in the reactor building or the spent fuel pool building and lead to a dropped fuel assembly.

733. The safety case for preventing unplanned criticality during fuel transport, handling and storage has been considered by ONR's criticality specialists within Ref. 146. I have therefore not considered these aspects within this report.

734. The detailed design of the SFIS facility (including the spent fuel transfer cask and storage canister) is outside the scope of GDA. The RP has therefore only submitted an outline of the major faults that could occur and a demonstration that future operations required for SFIS can be accommodated within the BFX. During GDA I have therefore supported ONR's Radioactive Waste assessment which is recorded within Ref. 147 and considers the RP's approach to the identification of the most significant potential faults and the measures that can be implemented to protect against these.

4.5.1 Spent Fuel Pool Cooling and Water Inventory Faults

735. It is my expectation that all faults relevant to cooling of fuel in the SFP are identified and that adequate protection is provided to protect against those faults. This section relates to the identification of the faults that affect cooling in the SFP (and the connected reactor pool, where appropriate), and the RP's demonstration that adequate protection is provided against these faults.

736. The SFP is cooled by the F-SC2 PTR [FPCTS] system. The PTR [FPCTS] consists of three trains, referred to as Trains A, B and C. During non-refuelling operating modes, one train of PTR [FPCTS], Train A, is in operation. During refuelling operating modes, two trains of PTR [FPCTS] are in operation, and a third train, Train C, is in standby.

737. All trains normally transfer their heat to the RRI [CCWS]. The parts of the RRI [CCWS] which deliver cooling to the SFP are F-SC2. In the event of loss of cooling chain (i.e. loss of RRI [CCWS]) a backup heat sink, the F-SC3 ECS [ECS], provides cooling to Trains A and B of PTR [FPCTS] (using the heat exchanger that is used for the RRI [CCWS]). If all three trains of the PTR [FPCTS] fail, the ASP [SPHRS] tank can be aligned to the SFP to compensate for water which would be lost through evaporation of the SFP. The parts of ASP [SPHRS] which deliver this function are F-SC2. Blow out panels and manually operated vents protect the fuel building from over pressurisation.

738. The RRI [CCWS] is electrically backed up by the F-SC1 EDGs. Both the PTR [FPCTS] and ECS [ECS] can be powered by the EDGs, F-SC2 SBO generators, and F-SC3 mobile generators. Automatic isolation of the reactor pool and SFP connecting lines is performed by F-SC1 RPS [PS] when their respective low level signals are reached. Further operations of the isolation valves and the control valves of the ASP [SPHRS] can be performed by the F-SC2 SAS. The SFP containment isolation valves, RPS [PS] and SAS are backed by the F-SC1 (2 hour) and F-SC2 (24 hour) Uninterruptible Power Supply (UPS).

739. The RP has performed analysis to demonstrate that the generic UK HPR1000 design is tolerant of potential SFP design basis accidents. The RP has identified the following DBCs associated with the spent fuel pool:

- Loss of one train of PTR [FPCTS] in POS A/B/C/D.
- Loss of one train of PTR [FPCTS] in POS E/F.
- Non isolable small break or isolable RIS [SIS] break affecting fuel pool cooling.
- Isolable piping failure to connecting pipe of the SPF.

740. In addition to the above, the RP has also identified the following as a DEC-A condition:

- Loss of three trains of PTR [FPCTS].
- SBO for the SFP.

741. In the derivation of these faults, the RP has considered faults in all plant operating states and failure modes. There are notable omissions from the above list of DBCs; namely, damage to the SFP liner or concrete structure resulting in catastrophic drain down and failure of gates to adjacent compartments (referred to as pits). The RP has identified both of these as PIEs but excluded them from the DBA on the grounds of low frequency. My assessment of the identification of the accidents is summarised in sub-sections 4.5.1.1 and 4.5.1.2.

742. The above faults range from DBC-2 to DBC-4 and DEC-A faults. These faults can be categorised into two broad categories, a loss of cooling to the SPF and loss of SFP water inventory.

743. When cooling by the PTR [FPCTS] is available, the RP claim that SFP water temperature can be controlled such that boiling is avoided. The RP's objective is to demonstrate that sufficient heat can be removed such that the heat removed is greater than the heat input (i.e. decay heat). The RP claims in response to RQ-UKHPR1000-0622 (Ref. 6) that one train of PTR [FPCTS] (with RRI [CCWS]) is capable of maintaining the SFP lower than 80 °C in the long term, and therefore uses 80 °C as an acceptance criterion for long term cooling. Although not specifically demonstrated in all cases by the RP, once the balance between heat removal and decay heat is reached, even if additional active cooling systems are not restored, the temperature will continue to reduce due to evaporative losses and reducing decay heat over time. I am therefore content with the RP's use of the 80 °C acceptance criterion. This criterion has been applied by the RP to all design basis faults identified.

744. If the capability to remove heat via PTR [FPCTS] is completely lost, the RP claim that make-up water (via the ASP [SPHRS]) and evaporative cooling maintains sufficient heat removal. In this scenario, therefore, boiling is considered acceptable by the RP; my assessment of the radiological consequences of this is presented in Section 4.7.

745. In a similar way to reactor faults, the RP defines controlled and safe states for the SFP. The safety functions are categorised depending on which state they are transitioning the SFP to. Accidents related to loss of cooling are significantly slower than those with loss of inventory, therefore the RP claims (in Chapter 12 of the PCSR, Ref. 3) that the SFP can be considered to be in the controlled state at the beginning of the fault sequence, and requires cooling to be restored to bring the SFP to a safe state. For loss of inventory faults, the RP considers that a controlled state is reached when the water level is controlled (i.e. through isolation, makeup, or self-limiting water level drop).

746. The SFP cooling systems are run continuously. For this reason, maintenance must be performed whilst the system is in operation. Therefore, unlike the reactor faults, which do not assume any reduction in availability due to maintenance, the fault analysis of the SFP takes into account that some trains of safety may be unavailable. The assumptions related to maintenance are described where appropriate in sub-sections 4.5.1.1 and 4.5.1.2.

747. In the following sub-sections 4.5.1.1 and 4.5.2.2, I have summarised my assessment of the RP's identification of SFP faults and the adequacy of the protection against these faults.

4.5.1.1 Loss of Cooling to the SFP

Identification of Postulated Initiating Events

748. The PIE list (Ref 26) identifies a loss of one or two PTR [FPCTS] as DBCs which lead to a loss of heat removal from the SFP.

749. As I have previously noted, in POS A/B/C/D only one PTR [FPCTS] train is in service; whilst in POS E/F, owing to the larger decay heat in the SFP during refuelling, two trains of PTR [FPCTS] are in service. Moreover, there are differences related to the configurations of the reactor pool, fuel transfer tunnel, transfer pit and sluice gates in POS E/F in comparison to POS A/B/C/D. The difference in progression during POS A/B/C/D and POS E/F has been recognised by the RP who has identified two separate DBCs (Ref. 27).

750. The RP has also argued that a loss of two trains of PTR [FPCTS] can only happen in POS E/F (where two trains are in service) and the consequences can be bounded by the loss of three trains of PTR [FPCTS] (Ref. 106). I am content that this is a reasonable approach.

751. The F-SC1 RRI [CCWS] provides cooling to the F-SC2 PTR [FPCTS]. In the event of failure of the RRI [CCWS], the ECS [ECS] provides cooling to trains A and B of the PTR [FPCTS]. Although mechanical failure in the PTR [FPCTS] and loss of RRI [CCWS] have very similar consequences, for all cases related to the loss of PTR [FPCTS] as the initiating event, the RP assumes that a mechanical failure occurs in the PTR [FPCTS] system (e.g. a pump) rather than the cooling chain. This is because loss of PTR [FPCTS] through mechanical failure is not recoverable, whereas loss of RRI [CCWS] is recoverable (via the ECS [ECS]). I am therefore content that the RP has not explicitly analysed a loss of RRI [CCWS] and that the consequences can be bounded by a loss of PTR [FPCTS].I am also content that adequate protection is provided for loss of RRI [CCWS] by the F-SC3 ECS [ECS] and that the classification of the ECS [ECS] to deliver this function is consistent with the RP's methodology for the classification of SSCs.

752. Separately, as part of the identification of DEC-A events, the RP has identified SBO for the spent fuel pool for POS A-F.

753. For the SFP, there is little difference between the analysis methodologies for DBCs and DEC-A events. I have therefore presented my assessment of the RP's analysis of loss of one and three trains of PTR [FPCTS] and SBO for the SFP in the following subsections.

Loss of One Train of PTR [FPCTS] in POS A/B/C/D

754. The loss of one train of PTR [FPCTS] in POS A/B/C/D is a DBC-2 fault. The RP's analysis of this is presented in Ref. 148. The RP claims that protection against loss of one train of PTR [FPCTS] is provided by the redundant trains, B and C, which are normally in standby. The PTR [FPCTS] is an F-SC2 system, and the heat is removed by the RRI [CCWS], which is a F-SC1 system.

755. In the event of the loss of one train of PTR [FPCTS], the operator is expected to start train B of the PTR [FPCTS], and to ready train C in case train B is out for maintenance or fails to start. Whilst not stated in Ref. 148, there are several alarms and measurements for detecting the failure of the PTR [FPCTS] train A or the success/failure of trains B and C (e.g. pressure drops, valve position signals, flow rate detection etc.). The safety functions associated with relevant measurements, actuations and alarms area are delivered by the SAS, which is a F-SC2 system.

756. The RP applies conservative assumptions to the decay heat, initial water level (the lowest level before a low level alarm is actuated) and performance of the RRI [CCWS]. The analysis is a simple heat balance equation, which is appropriate for the analysis and I am content that these assumptions are consistent with the expectations of SAPs FA.6.

757. The RP claim that, even when applying conservative assumptions, ~[redacted] hours are available until 80 °C is reached and ~[redacted] hours are available until [redacted] °C is reached. The RP claim that by starting up one of the standby trains of PTR [FPCTS], the SFP stabilises at [redacted] °C (therefore meeting the [redacted] °C acceptance criterion). The RP therefore claim that the PTR [FPCTS] is effective in bringing the SFP to a safe state in POS A/B/C/D, no boiling or fuel damage occurs, and therefore there are no radiological consequences of this accident.

758. A potential concern arises for application of the single failure criterion to the three train PTR [FPCTS] if a fault affects the operating train, another is unavailable due to maintenance then assuming a random failure prevents operation of the third would leave the SFP without active cooling. Ref. 148 addresses this by stating that if one train is out for maintenance, then the third train is started up preventatively. This means that if one train is lost, another train is already running and the single failure criterion does not apply to it. As a result, the RP does not consider coincident maintenance and a random single failure but assumes that one standby train of PTR [FPCTS] is available (this position is explained in Ref. 149). I am content with this explanation and that it is not necessary for the RP to assume a single failure affecting one train of PTR [FPCTS].

759. In my opinion, the RP's analysis clearly demonstrates that, in the event of a loss of one train of PTR [FPCTS] in POS A/B/C/D, there is sufficient time to start up a standby train of PTR [FPCTS] which is capable of stabilising the water temperature before the RP's 80 °C safety case limit is reached. This is consistent with the expectations of SAPs FA.7 and FA.8.In addition, as the PTR [FPCTS] provides the primary means to return the plant to safe state (as defined by the RP), I am satisfied that the classification F-SC2 is appropriate.

Loss of One Train of PTR [FPCTS] in POS E/F

760. During POS E or F (POS E and F refer to refuelling and when the core is fully unloaded, respectively), the reactor cavity is flooded and hydraulically connected to the SFP. The RP has categorised a loss of one train of PTR [FPCTS] in POS E/F as a DBC-3 fault and the RP's analysis of this is presented in Ref. 149. Within this, the RP has considered all failure types and plant configurations and determined that POS F presents the most limiting initial conditions and configurations. This is due to the higher decay heat within the SFP during POS F where the reactor core is totally unloaded into the SFP. I am content that this assumption is conservative and consistent with the expectations of SAPs FA.5 and FA.6.

761. In POS F, two trains of PTR [FPCTS] are in operation to accommodate the additional decay heat from the fully unloaded core. It should be noted that in POS F, no fuel remains in the core. The RP applies the same conservative assumptions to water level and performance of the RRI [CCWS] as the POS A/B/C/D fault, however, a significantly higher decay heat is applied owing to the recently unloaded core. Whilst not stated in Ref. 149, this decay heat corresponds to 720 fuel assemblies from previous cycles, 72 fuel assemblies from a recent refuelling, and 177 fuel assemblies due to an emergency unloading of the core (Ref. 182). In my opinion, this is a conservative assumption.

762. Unlike the corresponding analysis for POS A/B/C/D, Ref. 149 does not provide a time to restore a train of PTR [FPCTS] before the SFP would start to boil. This is because two trains are in operation before the fault and the RP demonstrates (using heat balance equations) that the remaining train is sufficient to stabilise the water temperature [redacted] °C. The RP consider that the safe state is reached and that the third train of PTR [FPCTS] can then be used to bring the temperature back to the normal operating temperature. The RP therefore concludes that no fuel failure occurs and that no boiling occurs, therefore there are no radiological consequences.

763. I am satisfied that the RP's analysis of this fault uses appropriate methods and is conservative, consistent with the expectations of SAP FA.6 (Ref. 2). I am content that this demonstrates that, in the event of a loss of one train of PTR [FPCTS] in POS E/F, one train of PTR [FPCTS] would be capable of bringing the SFP to a safe state. This meets my expectations for FA.7 and FA.8.

Loss of Three Trains of PTR [FPCTS] in all Plant Operating States

764. The RP considers that loss of the operating PTR [FPCTS] trains (either one or two depending on plant state) plus failure of the redundant trains to start is a DEC-A sequence, based on the guidance within IAEA SSG-2 paragraph 3.41 (Ref. 8). I acknowledge that the PTR [FPCTS] incorporates redundancy in its cooling chain and diversity in the cooling of the PTR [FPCTS] pumps and as such total failure of PTR [FPCTS] is unlikely. However, I note that the RP has estimated a frequency of a loss of three trains of PTR [FPCTS] to be 1.01 $x10^{-3}$ pa in Ref. 35 and this is in line with SAP EDR.3 which sets a limit on claims on the reliability of a safety system to one failure per 100,000 demands.

765. The main implication of this fault being assessed as a DEC-A rather than a DBC is that the RP has not sought to demonstrate that the SFP temperature can be controlled using active systems. Instead, in Ref. 150 the RP seeks to demonstrate that, while boiling will occur, the spent fuel remains adequately covered and as such there will be no fuel failures. (The RP has separately analysed the radiological consequences to show that they are acceptable. My assessment of this is presented in Section 4.7 below). Given that this objective is consistent with the expectations of FA.7, I am satisfied that informed judgements can be made on the adequacy of the generic UK HPR1000 design in GDA, even if the event frequency was to change later.

766. The RP claims the ASP [SPHRS] to provide protection against a loss of all three trains of PTR [FPCTS]. The alignment requires a local action from an operator. Importantly, Ref. 150 notes that if the fuel transfer tube is open, an operator must close it before ASP [SPHRS] is actuated in order to avoid boron dilution in the reactor pool. After alignment, water from the ASP [SPHRS] is gravity fed into the spent fuel pool and compensates for water losses from evaporation from the spent fuel pool.

767. During GDA, the RP upgraded the categorisation of the ASP [SPHRS] make up functionality to F-SC2 and incorporated this into DR 3.0 under modification M32 (Ref. 156). As a consequence of this increase in safety classification a second makeup line to the SFP has been added to the ASP [SPHRS]. This modification has been made to allow the RP to claim this function as a diverse means of protection against an isolatable piping failure on a system connected to the SFP (as discussed in sub-section 4.5.1.2 below) but also provides benefit in the event of a loss of three trains of PTR [FPCTS].

768. In Ref. 150, the RP has not applied a single failure to the ASP [SPHRS] since the fault is categorised as DEC-A. Given that the sequence already includes the CCF of the FSC-2 PTR [FPCTS] and that the most limiting remaining single failure would only

result in failure to open one line of ASP [SPHRS] I am content to judge that this is reasonable.

769. In Ref. 150, the RP has applied the same conservatisms as those used in the analysis of the failure of one train of PTR [FPCTS] in POS E/F. The RP states that the time to boiling in the SFP is [redacted] hours. In response to RQ-UKHPR1000-1080 (Ref. 6), the RP quote the time required for alignment of the ASP [SPHRS] as 100 minutes. Once the ASP [SPHRS] is aligned, the maximum flow rate is [redacted] kg/s. In Ref. 150, the RP states that the maximum evaporation rate is [redacted] kg/s. As the ASP [SPHRS] is around 3035 m^3, the RP conclude that heat removal can be maintained in this configuration for over three days.

770. From my review of Ref. 150, I am satisfied that the RP has analysed a loss of three trains of PTR [FPCTS] on a conservative basis and has demonstrated that the ASP [SPHRS] is effective in removing heat from the SFP. Given that the heat is successfully removed and water level is maintained, I am satisfied that there will be no fuel damage and that this supports the demonstration that the consequences are ALARP.

Station Black Out in the SFP in all Operating States

771. The RP identifies SBO for the SFP in all operating states as a DEC-A event and the analysis is used to demonstrate the effectiveness of the SBO diesel generators as diverse protection against CCF of the EDGs following a LOOP. In this scenario, electrical power is lost to the normal cooling chain (RRI [CCWS]) and the ECS [ECS] must be initiated to remove heat from the PTR [FPCTS] system. The RP's analysis (Ref. 151) aims to demonstrate that one train of ECS [ECS] powered by an SBO diesel generator can provide sufficient cooling to the SFP via the PTR [FPCTS] in all operating conditions.

772. The RP has applied similar assumptions to those for loss of all three trains of PTR [FPCTS]. Importantly, the RP has performed the analysis using POS F and a large SFP irradiated fuel inventory. The decay heat, therefore, is the maximum allowable decay heat and is a conservative assumption.

773. The RP's analysis shows that approximately [redacted] hours until boiling occurs. The RP's analysis demonstrates that if the ECS [ECS] is initiated at [redacted] hours, the maximum temperature reached is [redacted] °C, and one train of ECS [ECS] can stabilise the temperature at [redacted] °C.

774. I am satisfied that appropriate conservatisms have been applied and that the RP has demonstrated that there is sufficient time to align the ECS [ECS] to ensure that the water in the SFP water will not boil. As a result, I am satisfied that the water level will remain above the fuel in the SFP and none of the physical barriers to prevent relocation of a significant quantity of radioactive material will be breached, therefore meeting the expectations of FA.7.

4.5.1.2 Loss of SFP Water Inventory

775. A loss of SFP water inventory can have significant off-site radiological consequences if it is sufficient to uncover the fuel or impair the active cooling systems. Smaller losses of inventory will reduce the shielding available to operators within the spent fuel building. The design of the SFP and connecting pipework has incorporated a number of design features to reduce the risk of a loss of inventory.

776. The penetrations in the SFP for the suction pipes for Trains A and B of the PTR [FPCTS] are at a higher elevation of that of Train C of the PTR [FPCTS]. Trains A

and B are also equipped with siphon breakers, whereas Train C is not. The logic for this is as follows (from the response to RQ-UKHPR1000-1395 (Ref. 6)): a break in Train A and B will result in a drain down of water limited to the lowest point of the penetration and that a sufficient water level will remain for Train C to perform its safety functions. If Train C was equipped with a siphon breaker, it would have no benefit to Trains A and B in the event of a break in Train C. In fact, incorporating a siphon breaker in Train C would defeat the purpose of putting it at a lower level. The RP explain that the only benefit to incorporating a siphon breaker in Train C would be to slightly increase the water level to which the water would drain to if a break in Train C occurred. I consider the RP's reasoning sensible and that the design of the penetrations reduces associated risks ALARP.

777. The design of the gates and adjoining compartments is such that failure of a gate will not result in a worse reduction in water level than a break in PTR [FPCTS]. This means that even if the gate failed, the PTR [FPCTS] would still be able to perform its safety functions. Moreover, the lowest point of the gate is above the top of the fuel rack. This means that a break upstream of the SFP (e.g. non-isolable break of connecting pipe to RHR) could not result in a drain down of the SFP. These considerations are common practice in the design of SFPs.

778. The water level in the SFP and connecting areas is continuously monitored and several setpoints and alarms are incorporated into the design to prompt protective actions should the water level drop. The alarms are assigned to several I&C systems, including the F-SC1 RPS [PS], the SAS and the F-SC3 KDA [SA I&C]. The automatic actions to isolate the SFP are carried out by the RPS [PS], whilst manual operations (e.g. opening/closing valves and starting/stopping pumps) are carried out by the SAS. The adequacy of water level monitoring has been considered by the severe accident analysis inspector (Ref.86), who has found that the design meets RGP and is ALARP.

Identification of Postulated Initiating Events

779. In the PIE list (Ref. 26), the RP identifies seven PIEs that have the potential to lead to a loss of inventory in the SFP. These are as follows:

- SFP structure damage (including pool liner).
- SFP gate failure.
- Break in pipeline connected to the SFP.
- Reactor pool or RPV break.
- Pipeline connected to the reactor pool break.
- Fuel transfer tube (FTT) break.
- Spurious drainage of SFP.

780. The majority of these PIEs are not taken forward as DBCs by the RP either due to low frequency or because the RP considers that they are less onerous than other fault conditions that have been analysed. The only PIE taken forward for analysis as a DBC is the break in a pipeline connected to the SFP, and it is the only fault related to loss of SFP water inventory faults to appear in the Fault Schedule. As my focus has been on the protection available for the PIEs (i.e. DBCs), I have not assessed the safety case for the remaining PIEs in detail. However, given the significant amount of fuel that can be present in the SFP and the potential for large radiological releases, I have considered the RP's arguments for excluding these faults from the list of DBCs in turn in this sub-section.

781. In response to RQ-UKHPR1000-622 (Ref. 6), the RP argues that PIEs as a result of damage to the SFP structure or pool liner leading to drain down of the SFP are not carried forward as DBCs as they are capable of withstanding design basis earthquakes and dropped loads. These claims have been assessed by ONR's Civil Engineering

inspector, who has found that the methodologies are conservative and that the arguments provided by the RP are reasonable (Ref. 152).

782. In Ref. 26 failures of a gate seal, reactor pool or RPV, and a leak in pipework connected to the reactor pool are excluded from the list of DBCs by the RP on the basis that a leak would be limited by the design of these features relative to the SFP (as discussed in paragraph 777 above). As such the RP asserts that faults would be less onerous than the design basis SFP pipeline breaks considered in the DBC. I the RP's arguments to be reasonable.

783. The RP argues that a double ended guillotine failure of the FTT would only result in limited drain down due to the leak tightness provided by adjacent compartments. The extent of the fault is therefore limited by passive means. These claims have been assessed by ONR's Structural Integrity inspector, who has found the arguments reasonable (Ref. 32). In addition, the RP claims that the lost water can also be made up via the F-SC1 MHSI and the normal water level can be restored. Given that the water loss is limited, I consider the RP's claims to be reasonable.

784. Regarding spurious drain down of the SFP, the progression of this accident is similar to a break in any of the connecting pipelines. However, the RP notes that a spurious drain down can be easily rectified by isolation of the affected lines. Even if the operator failed to act, an automatic signal is generated to isolated penetrations of the reactor pool and SFP when the water level reaches a low setpoint. A spurious drain down would have the same consequences as a non-isolable break (i.e. drainage to the suction line level). As drainage faults are protected by an FC1 isolation function, I am satisfied that this fault can be bounded by breaks in the connecting pipes.

785. Having reviewed the arguments above I am satisfied that the RP has provided sufficient arguments for not analysing these PIEs as DBCs.

786. The only PIE group that remains is related to breaks in connecting pipes to the SFP and reactor pool. This includes small and large breaks to the connecting pipes to the RCP [RCS] when in POS E. Ref. 106 groups these accidents further. Whilst Ref. 106 identifies large isolable breaks to the PTR [FPCTS] and RIS [SIS], the RP has only considered a small non-isolable break. For the RIS [SIS], the large bore pipework which is non-isolable is within the reactor building, and most of the leaked water would be collected in the IRWST and I am content that the consequences are bounded by breaks outside of the containment. I am not therefore not concerned that non-isolable breaks of large bore pipework within the containment are not identified as a DBC. However, a non-isolable leak in Train C of the PTR [FPCTS] would lead an initial rapid drop in water level to the bottom of the suction pipe of Train C, followed by a period in which the SFP heats up and begins to boil, further reducing the water level. Importantly, the PTR [FPCTS] is unable to remove heat in this scenario, and the ASP [SPHRS] is credited to provide makeup water.

787. I note that the frequency of a non-isolable break in a connecting pipe to the SFP is quoted in Ref. 106 as [redacted] pa (which is based on OPEX of low pressure pipes and the short length of pipe), which is lower than the RP's design basis cut off frequency and the criteria given by SAP FA.5. I judge that the frequencies quoted may be overly optimistic, and I did not consider that the probabilistic arguments alone were sufficient to justify excluding these faults from the DBA. I therefore sought further justification for exclusion of non-isolable breaks in the SFP.

788. My assessment of the RP's safety case for exclusion of non-isolable breaks in a connecting pipe to the SFP can be summarised as follows:

- The RP states that a break in Train C of the PTR [FPCTS] would lead to a consequential loss of all three trains of PTR [FPCTS] (Train C has a lower elevation than Trains A and B and therefore a break in it would not only take Train C out of service but also lower the water level to below the intake levels of the other two trains). This results in a loss of all active SFP cooling similar to that considered in the existing DEC-A fault loss of three trains of PTR [FPCTS]. However, in Ref. 153 and in response to RQ-UKHPR1000-1395 (Ref. 6), the RP has recognised that a non-isolable leak in the PTR [FPCTS] connecting lines results in a lower water level than loss of all three trains of PTR [FPCTS].
- It is therefore my opinion that anon-isolable break in Train C of the PTR [FPCTS] has the potential to be more onerous than a loss of all three trains of PTR [FPCTS], as it could progress more quickly and therefore allow less time to initiate ASP [SPHRS] to recover the water level, particularly if the break was to occur during fuel movement (when a fuel assembly will be lifted from the storage racks). In response to that challenge, the RP argues that if a non-isolable break were to occur during a fuel movement and the water was to decrease to the lowest level, the handled fuel would still remain covered The RP also argues (RQ-UKHPR1000-1080) that since about [redacted] hours is available until the SFP starts boiling (assuming the lowest water level), sufficient time is available to implement ASP [SPHRS] makeup (which takes approximately [redacted] minutes).
- On this basis, I am content the analysis of ASP [SPHRS] during loss of all three trains of PTR [FPCTS] (described in sub-section 4.5.1.1 above) provides adequate confidence for GDA that the ASP [SPHRS] will also be effective for the similar fault caused by a non-isolable break in a connecting line of Train C of the PTR [FPCTS], and even if fuel was being moved above the racks at the time of the event there will be sufficient time to align it.

789. As a result of the fault identification work described above, the RP has taken forward the following two PIEs as DBCs relating to a loss of water inventory:

- Non isolable small break or isolable RIS [SIS] break affecting fuel pool cooling
- Isolable piping failure to connecting pipe of the SPF

790. Based on the above I am satisfied that these are appropriate DBCs for demonstrating that the SFP can be protected against loss of water inventory faults, consistent with the expectations of SAP FA.5. However, it should be noted that the RP's arguments for why it has selected the two DBCs and have excluded others are scattered across References 26, 27, 106 and various RQ responses. This is a specific example of my general conclusions about the RP's fault identification that I have discussed in paragraph 92 where I recorded a minor shortfall.

791. In the following sub-sections I present my assessment of the analysis of these two DBCs.

Non-Isolable Small Break or Isolable RIS [SIS] Break Affecting Fuel Pool Cooling

792. This postulated initiating event relates to both small non-isolable and large isolable breaks in the reactor building, and is classed as a DBC-4 accident. The RP's analysis of these faults is presented in Ref. 154. Only breaks which occur whilst the fuel transfer tube is open can affect the SFP. I have therefore targeted the analysis results for these configurations.

793. Water level measurements, isolation of major penetrations, human actions to start MHSI and to open the reactor pool overflow line, and the RPS [PS] are all required to

reach a controlled state for the non-isolable leak. All safety functions are therefore FC1 and provided by a F-SC1 SSC**. Since these SSCs and human actions provide the primary means of reaching the controlled state, I consider the assignment of F-SC1 to be appropriate and meet my expectations of ECS.1 and ECS.2.

794. The analysis of the non-isolable leak assumes a small pipe (< 50 mm) connected to a the RHR line. The accident is assumed to occur in POS E.

795. As part of the response to the EMIT RO (RO-UKHPR1000-0021, Ref. 7), the RP has determined that maintenance of the PTR [FPCTS] cannot be performed during POS E, therefore no loss of availability due to maintenance is assumed in the analysis. The RP has assumed a single failure of one train of the PTR [FPCTS]. Whilst the isolation valve could, in principle, represent a more onerous single failure, the generic UK HPR1000 design includes double isolation with diversity considered in the valves. I am therefore content to judge that the single failure assumed in the analysis is appropriate and that the other assumptions made by the RP are appropriate and consistent with my expectations for FA.6.

796. The leak causes the reactor pool level to decrease, and an alarm is raised when the water level drops below + [redacted] m. The water level continues to drop to + [redacted] m where a F-SC1 safety function to isolate RIS [SIS] suction pipe is actuated. At + [redacted] m, the PTR [FPCTS] connecting pipes are isolated.

797. However, the water level continues to drop until the FC1 operator action to manually initiate MHSI (and to open the overflow line of the reactor pool) is performed when the water level decreases to + [redacted] m. Once the MHSI is initiated, the controlled state (i.e. when the water level is controlled) is reached. Ref. 154 does not provide timescales for the occurrence of the events. However, ONR's Human Factors assessment has assessed human reliability claims to perform these actions and has found that the RP's claims to be appropriate (Ref. 55).

798. Once control of the water level is established, the RP claims that the operator will start up two trains of PTR [FPCTS]. At this point the reactor pool and SFP become stable at [redacted] °C. The final water level is not reported; however, the RP does state that the level must be above + [redacted] m in order to restart PTR [FPCTS]. I therefore infer that the water level will be established above + [redacted] m, which is above the maximum lift height of a fuel assembly in the SFP (+ [redacted] m).

799. For the large isolable break (< 250 mm), the transient is terminated after the isolation signal is sent to the RIS [SIS] and PTR [FPCTS], which is an FC-1 safety function. After the break is isolated and PTR [FPCTS] is reinstated, the water level stabilises at [redacted] m.

800. I consider that the RP has provided adequate demonstration that an unisolable break would be recovered by the initiation of the MHSI, and that long term heat removal can be provided by the PTR [FPCTS]. In addition as the MHSI brings the accident to a controlled state and the PTR [FPCTS] provides the transition to the safe state, I consider that the classification of F-SC1 and F-SC2, respectively, are appropriate. I am also satisfied that an isolatable leak can be detected early by the RPS [PS] and automatically isolated to bring the plant to a controlled state.

801. I am satisfied that adequate protection exists for large isolable and small non-isolable breaks in the reactor building, and I am satisfied that the expectations of FA.7 and FA.8 have been met.

** *The functionality of manual MHSI during POS E was upgraded to F-SC1 1 during GDA*

Isolable Piping Failure to Connecting Pipe in the SFP

802. This postulated initiating event relates to isolatable breaks in the PTR [FPCTS] system and is a DBC-3 accident. The RP's analysis of these faults is presented in Ref. 155.

803. The large break results in a drainage of the SFP. If the pool level falls to + [redacted] m, a F-SC1 signal is generated and the RPS [PS] isolates all three trains of PTR [FPCTS]. For this fault, the RP has assumed that one train is unavailable due to application of a single failure, one train is unavailable due to maintenance and one train is lost due to the break. Unlike the loss of one train of PTR [FPCTS] fault, in which the other train of PTR [FPCTS] is available to provide cooling, all trains of PTR [FPCTS] are isolated in response to the fault and therefore all cooling via PTR [FPCTS] becomes unavailable.

804. The F-SC1 isolation of the break brings the SFP to the controlled state, and the ASP [SPHRS] is credited to provide long term evaporative cooling to the safe state. For this reason, the ASP [SPHRS] has been upgraded to F-SC2 during GDA (see design modification M32 (Ref. 156)). As discussed previously (para 766) I am satisfied that the upgraded ASP [SPHRS] has an appropriate classification (F-SC2) to deliver this long term safety function following design modification M32. I am therefore satisfied that the expectations of ECS.1 and ECS.2 have been met.

805. The assumptions used in the analysis are similar to those explained in sub-section 4.5.1.1. The RP has applied conservative decay heats, initial water levels and system performance. I judge that the assumptions are reasonable, conservative and meet my expectations for FA.6.

806. After isolation, the accident progresses similarly to loss of three trains of PTR [FPCTS]. The RP demonstrates that the water level remains above the fuel rack and that the water consumed over three days (e.g. POS A – 612 tonnes, POS F – 1755 tonnes) is significantly less than the capacity of the ASP [SPHRS] (3035 tonnes).

807. I am satisfied that the RP has demonstrated that isolation of the break and alignment of the ASP [SPHRS] will effectively bring the plant to a safe state, and that the ASP [SPHRS] is appropriately sized to protect against an isolable break in a connecting pipe to the SFP. I am also satisfied that the isolation system and ASP [SPHRS] are appropriately classified to bring the SFP to a controlled state and safe state, respectively. I am therefore satisfied that the expectations of FA.7 and FA.8 have been met.

4.5.2 Dropped Loads

808. As part of the fuel import, loading, unloading, storage and export operations, the fuel will be lifted by a variety of lifting equipment and with this comes the inherent potential for a dropped load event. The fuel may be new fuel, fuel with a high decay heat recently unloaded from the reactor, or longer cooled fuel. During some of these lifting operations the fuel will be contained within a transport container which offers protection against a drop while other operations involve a lift of the fuel assemblies alone.

809. The RP has undertaken specific fault identification for the lifting operations within the fuel route following the PIE identification process used elsewhere in the safety case. From this the RP has defined Dropping of a Fuel Assembly as a single bounding DBC-4 fault within Chapter 12 of the PCSR (Ref. 3). The analysis of this event has been performed on a bounding basis but the protection available and the nature of the radioactive release will be influenced by the specific nature of where the event occurs. The RP has also developed separate safety schedules for lifting operations within the SFP, lifting of spent fuel casks and lifting operations within containment. I have sampled in detail the assessment of dropped fuel assemblies within the SFP then

widened my assessment to consider other potential events (such as a dropped load within containment during refuelling) in coming to my conclusions on this aspect of the safety case.

4.5.2.1 Dropped Loads within the SFP

810. While dropped loads can occur anywhere in the fuel route, my assessment has focussed on operations within the SFP building. This is because of the potential range of faults and the fact that the original design used an overhead travelling crane for fuel handling operations within the SFP, which ONR recognised is unusual for spent fuel handling operations within the UK. Potential concerns with this type of crane included:

- The crane control system was providing control and safety functions (protection).
- Significant safety claims were placed upon the crane control system, yet this was only specified as a F-SC3 system, which did not appear to be commensurate with the associated safety demands.
- The submitted crane design placed significant demands upon operator control actions, with the resultant potential for operator errors leading to significant fault conditions.
- There was the potential for the overhead crane to travel outside the extent of the SFP which placed great reliance on the control system or protection measures to prevent this.

811. As a result of these matters, ONR raised RO-UKHPR1000-056 (Ref. 7) which required the RP to provide a suitable and sufficient safety case for the handling of spent fuel and the spent fuel casks within the fuel building, to demonstrate that the relevant risks have been reduced to ALARP. As a result of work undertaken to address RO-UKHPR1000-0056 the RP has replaced the overhead travelling crane with a gantry crane for fuel handling within the SFP. This change has been integrated into the generic UK HPR1000 design and safety case through modification M94 (Ref. 183).

812. The RP has submitted a document which provides a summary of the safety case for lifting operations within the SFP building (Ref. 157) following this modification. As a result of the modification there are a number of benefits for the safety case, including:

- More crane controls can be automated, so demands upon the operator will be reduced during fuel movements. This will reduce the potential for operator errors initiating faults during fuel handling operations within the pool.
- The safety claims (demands) placed upon the crane control system in its role of preventing faults will be significantly reduced (noting that this is a F-SC3 system).
- The use of a rigid telescopic sleeve can protect the fuel, whilst removing the potential to drop the fuel handling tool with fuel attached. The sleeve design will be similar to that used in the reactor building.
- The rigid sleeve is fixed to the transfer trolley and will help prevent the crane from moving fuel outside of the pool after a collision.
- The fault of lifting fuel out of the pool can be virtually eliminated.
- The risk imposed by a gantry crane during a seismic event will be less.

813. Ref. 157 presents optioneering for the lifting arrangements and an overview of both the original and revised design. The detailed design of the gantry crane is out of scope of GDA and will need to be completed by a licensee. It also contains a description of potential faults and protection for the original arrangements and the modified design.

814. The RP has developed a specific approach to categorisation of safety functions for the lifting equipment (Ref. 164) which is generally consistent with the general methodology

presented for the reactor in Ref. 13. The main differences relate to a different interpretation of prevention and protection functions, noting that the majority of safety measures are provided to prevent a dropped load. It should be noted that both Refs. 157 and 164 use Cat 1, Cat 2 and Cat 3 for safety functions rather than FC1, FC2 and FC3 used elsewhere in the generic UK HPR1000 safety case. Whilst I have not undertaken a detailed review of the RP's approach, I am satisfied that it is consistent with the principles outlined in NS-TAST-GD-094 (Ref. 4).

815. Table T-5.4-1 of Ref 157 identifies the safety functions and safety function categories identified for the original crane design and states that these remain applicable for the gantry crane, but with improved confidence that they can be delivered. The identified safety functions are summarised below:

- Cat 1 functions for the crane and its load path, for all load cases (normal, seismic and fault) and Cat 2 functions for smaller items (the hoist and tooling) in their role of preventing collapse / impact.
- Cat 3 control functions to restrict crane travel, prevent over-raise, overload, and failure / collapse due to skew / crabbing.
- Cat 1 function for mechanical features to prevent failure due to skew / crabbing.
- Cat 1 function for hardwired interlocks to prevent collapse / impact due to snagged loads and excess travel (backed by mechanical buffer stops).
- Cat 2 function to prevent overload / snag protection by limiting the size of the crane hoist.
- Cat 2 function to provide over-raise protection provided by mechanical stops.

Safety Schedule for the Spent Fuel Pool Crane

816. All of the potential PIEs identified by the RP related to SFP lifting operations are contained within a safety schedule (Appendix C to Ref. 157) which also contains details of the required protection. I am content that the RP has chosen to develop specific fault schedules for the lifting operations as it provides the flexibility to reflect the range of potential initiators of a dropped load and the prevention or protection measures that are required.

817. The format of the safety schedule is very similar to that of the reactor fault schedule and those that I have seen in other UK safety cases. However, my principal finding from the review of the safety schedule is a lack of clarity on how the claimed safety measures will work together to provide the levels of defence in depth required. For example:

- Where control systems are a potential cause of PIEs, the control systems are also credited within the safety measures column. It is not clear whether this is for completeness of describing all of the levels of defence in depth or whether the RP are claiming a control system as an independent measure to terminate the fault.
- For overload faults the RP claims that the structure and load path can withstand the maximum loads whilst also separately claiming a torque limiter to limit the forces generated. It is not clear whether the claim is that the SSCs can withstand the maximum forces or those controlled by the torque limiter.

818. I recognise that the substantiation of the safety measures is incomplete and will need to be developed prior to operation, but it is not currently clear from the safety schedule what the principal safety claims or performance requirements are. Given these shortfalls with the SFP crane safety schedule, I have widened my assessment and examined the safety schedules for the fuel handling machine within the containment building and for the lifting of spent fuel casks for export from the spent fuel building (presented in Ref. 164). I have not assessed these safety schedules in Ref. 164 in

detail but in my opinion there are similar weaknesses to those that I have identified for the SFP crane safety schedule, with a lack of clarity on the claims made and justification of these claims. I have considered this finding in my decision to raise AF-UKHPR1000-0239 below.

Dropping of a fuel assembly

819. In Chapter 12 of the PCSR (Ref. 3), all the PIEs that could lead to a dropped fuel assembly are bounded by a single DBC-4 fault of dropped fuel element which has been analysed for comparison against radiological targets. I am satisfied that this approach is similar to that for other reactor safety cases and is consistent with the expectations of NS-TAST-GD-006 for the grouping of similar faults for DBA. However, I note that within the safety schedule (Ref. 157) some of the faults have an IEF greater than that of the bounding DBC-4 fault. ONR's guidance (NS-TAST-GD-006, Ref. 4) states that the fault frequency should be the sum of all the frequencies attributed to the different initiators of a particular fault, and not just the frequency of the most challenging version of the fault. I note however that the IEFs within Ref. 157 are estimates rather than calculated and that they will need to be confirmed following detailed design.

820. The RP's analysis of this fault is presented in Ref. 165 which considers the potential consequences of the fault. Rather than demonstrating the adequacy of protection measures (as the case relies on preventing dropped loads rather than protection measures) Ref. 165 evaluates the potential radiological consequences for a dropped fuel assembly for comparison against radiological targets. The maximum off-site dose predicted to an adult is 1.01 mSv and for an infant is 9.62 mSv (Ref. 165). These doses are below ONR's Target 4 BSL of 100 mSv for low frequency faults. However, if the IEFs of the individual PIEs have a higher frequency, a higher frequency BSL would be more appropriate. In this case the off-site radiological consequences may challenge this BSL.

821. The RP has identified some significant conservatisms in Ref. 165 which it has reviewed in its ALARP assessment (Ref. 61). The RP's ALARP assessment (Ref. 61) notes that the consequences in the latest version of Ref. 165 are based on a source term which assumes all fuel rods are damaged within one fuel assembly and claims that this is a very conservative assumption. The RP notes that for a similar fault, the EPR safety case assumes a source term based on a fraction of damaged fuel rods and, that as the UK HPR1000 fuel is shorter than the EPR fuel, any impact forces during a drop would be smaller. I am content to support this reasoning. The RP has not however substantiated this assumption for a lower level of fuel damage and so the base case assumes all fuel rods within the assembly are damaged.

822. A supporting document (Ref. 162) has calculated the off-site radiological consequences of 1 and 17 damaged fuel rods within an assembly. For 1 rod the limiting (infant) dose is 0.06 mSv and for 17 rods the limiting (infant) dose is 1.2 mSv. The off-site doses are therefore very sensitive to the level of damage assumed to the fuel rods and this needs to be underpinned to support the radiological consequences and I have considered this in my decision to raise AF-UKHPR1000-0239 below.

823. I recognise that the safety case for dropped loads within the fuel route will need to be improved prior to operation of the UK HPR1000 and I do not consider that the matters that I have identified represent any fundamental weaknesses in the design. I am also satisfied that the design of the fuel handling equipment for the UK HPR1000 is not novel and that I have not identified any reasons why adequate substantiation of claims cannot be provided. However, I have identified some specific shortcomings in the safety case:

- The event frequency of the dropping fuel element DBC should reflect the IEFs of the individual causes and not just be based on the most limiting case.
- The consequences of a dropped fuel element should be evaluated on a justified amount of fuel damage and compared against the most appropriate radiological targets.
- The safety schedules and wider safety case should be clear on the claims that are made and be supported by appropriate substantiation.
- The safety assessment is contained within a number of documents and it is difficult to trace key claims.

824. I am satisfied that sufficient information has been provided and that some elements of the safety case can only be developed once the design has progressed such that the frequency of events can be substantiated and claims on SSCs can be confirmed. On this basis I have raised the following Assessment Finding:

AF-UKHPR1000-0239 – The licensee shall, as part of detailed design, justify the frequency of dropped load faults within the fuel route, identify and classify the structures, systems and components which are claimed for these faults and present a comparison against appropriate radiological targets to demonstrate that the risks are reduced to ALARP. The radiological consequences should be evaluated based on a justified amount of fuel damage.

4.5.3 Strengths

825. Following my assessment of the fuel route faults I have identified the following strengths

- The RP's analysis demonstrates that, in the event of a loss of one train of PTR [FPCTS] cooling there is sufficient time to start up a standby train to bring the SFP to a safe stable state.
- The RP's analysis demonstrates that, in the event of a total loss of PTR [FPCTS] cooling the ASP [SHRS] is capable of removing decay heat from the SFP.
- The RP has demonstrated that there is sufficient time to initiate the ECS [ECS] as an alternative heat sink in the event of an SBO.
- The RP has identified potential leaks from the SFP and either demonstrated that the consequences will be limited or that they can be isolated and water level maintained.
- The RP has identified potential dropped loads and assessed the potential consequences, with an adequate system for classification of safety measures. During the course of GDA the RP has made a significant design change to the SFP crane. The full safety case implications of this change need to be developed but it is expected that this will result in further reductions in the likelihood and consequences of some of the identified dropped load faults.

4.5.4 Outcomes

826. As a result of my assessment of the fuel route faults I have identified the following outcomes:

- I have raised an Assessment Finding to ensure the licensee justifies the frequency of dropped load faults within the fuel route, identify and classify the SSCs and present a comparison against radiological targets to demonstrate that the risks are reduced to ALARP.

4.5.5 Conclusion

827. Based on the outcome of my assessment, considering ONR SAPs FA.6, FA.7 and TAG NS-TAST-GD-006, I have concluded that the analysis of fuel route faults is sufficient for GDA, however further development of the safety case will be required as the detailed design progresses to support operation.

4.6 Non-Reactor Faults (Waste route)

828. I have intentionally limited the scope of my assessment of non-reactor faults. The related systems and operations have been considered in other topic areas, principally the radioactive waste topic area (Ref. 147). The objectives of my assessment from a Fault Studies' perspective are to gain confidence in the RP's claim that there are no faults within the radioactive waste management systems which meet the criteria for treatment as design basis faults.

829. In support of this claim the RP has undertaken a series of activities to identify the initiating events postulated to occur within the radioactive waste management systems by following its own PIE and DBC identification method and process. It concluded that none of the identified PIEs is qualified to be a design basis fault. The radioactive waste management systems considered in the RP's PIE identification include:

- Coolant Storage and Treatment System (TEP [CSTS]).
- Nuclear Island Vent and Drain System (RPE [VDS]).
- Liquid Waste Treatment System (TEU [LWTS]).
- Nuclear Island Liquid Waste Discharge System (TER [NLWDS]).
- Sewage Recovery System (SRE [SRS]).
- Conventional Island Liquid Waste Discharge System (SEL [LWDS(CI)]).
- Gaseous Waste Treatment System (TEG [GWTS]).
- Solid Waste Treatment System (TES [SWTS]).
- Reactor Boron and Water Makeup System (REA [RBWMS]).
- Steam Generator Blowdown System (APG [SGBS]).
- Solid Waste Treatment System (TES [SWTS), including leakage of radioactive material from waste packages.

830. In line with the generic fault identification process, the RP has undertaken FMEAs and used Master Logic Diagrams to identify PIEs for all radioactive waste management systems (Ref. 184). The PIEs have been grouped and bounded into 9 PIE groups with a representative (bounding) PIE for each group (Ref. 181).

831. Given the predicted low frequency and potential consequences of these faults the RP do not consider that they qualify as DBCs. By comparison with ONR's expectations for identifying design basis faults (as set out in SAPs FA.5 and NS-TAST-GD-006) I am content to support this approach. However, to satisfy myself of this conclusion I examined the evidence supporting the frequency and consequence calculations.

832. I have chosen to sample the TEG [GWTS] system to inform my assessment of adequacy of the RP's fault identification, as failures in this system have the potential to result in more significant radiological consequences than those possible from the other systems. Two bounding PIEs relate to the TEG [GWTS]; leakage of the pipeline in the recirculated flush unit of TEG [GWTS] and leakage in delay beds of TEG [GWTS].

833. The RP's method to calculate the PIE frequency is to sum the frequency of each failure mode of the component in question, including consideration of potential CCFs. The failure rate data are taken from the PSA data analysis report, (Ref. 166). The RP also considered data from OPEX and made engineering judgements when necessary. In my opinion this method used to derive PIE frequency is reasonable and largely

consistent with ONR expectations, including Appendix 3 of ONR NS-TAST-GD-006 (Ref. 4).

834. The RP claims that the frequency of a leakage of the pipeline in the recirculated flush unit of TEG [GWTS] is [redacted] pa, and is less than 1 x10^{-3} pa for a leakage in delay beds of TEG [GWTS]. The RP's safety case approach limits claims on reliability for F-SC3 SSCs to a failure rate of 10^{-2} pa, which is consistent with the expectation of ONR NS-TAST-GD-094 (Ref. 4) that the failure frequency of F-SC3 systems is between 10^{-1} pa and 10^{-2}pa. Given that the frequency of [redacted] pa assigned to this fault group is two orders of magnitude better than the RP's own safety classification limitations I have sought further substantiation of this claim.

835. In response to RQ-UKHPR1000-1177 and RQ-UKHPR1000-1283 (Ref. 6), the RP explained that the frequency for fault group DBC-RW-08 has been derived by applying its frequency calculation methodology with component failure rate data taken from US NRC data (Ref. 167). To justify the suitability of this data for use in the PIE frequency calculation, the RP presents further evidence by comparing this with data from the UK HSE data base (Ref. 168). Whilst I am satisfied that the RP has provided sufficient evidence to justify that the component failure rate data can support the calculated PIE frequency, this will need to be substantiated during detailed design as the reliabilities will be determined by a range of factors including the build quality, frequency and type of inspections and the operating conditions.

836. I have therefore also considered the RP's assessment of the consequences of failures within the TEG [GWTS] (Refs 185 and 186). The RP has calculated the unmitigated doses using the same methodology and generic assumptions as used elsewhere in the DBA. The maximum on-site dose (Ref. 185) is 60 mSv (leakage of the pipeline in the recirculated flush unit of TEG [GWTS]) and the maximum off-site dose (Ref. 186) is 4 mSv (Leakage in delay beds of TEG [GWTS]. These are the limiting doses for any of the radioactive waste PIEs. Given that none of the identified radioactive waste management system faults lead to unmitigated consequences which exceed the RP's BSL for the respective initiating fault frequency in RPT-4, I am satisfied that none of the identified PIEs for radioactive waste management meets the criteria of a design basis fault, as defined by SAP FA.5 and Target 4. Given this and noting that ONR's Radioactive Waste Assessment (Ref. 147) has concluded that the design of the gaseous and liquid waste treatment systems is consistent with RGP, I have not examined these faults further.

837. Whilst I am content with the RP's PIE and DBC identification method, during my assessment I have noted that the RP use the term 'plant operating modes' defined for reactor faults within the non-reactor fault analysis. The main purpose of the use of 'plant operating modes' concept is to define plant initial conditions and plant configurations when the initial event is postulated to occur. In the fault studies technical area, the concept of plant operating modes is used to facilitate the bounding fault identification and fault sequence selection in a conservative manner to meet DBA requirements.

838. The six operating modes, defined in accordance with reactor core and the reactor primary circuit conditions and configurations at different stages of intended operation of the plant, are not applicable to those systems whose operation and configurations have no direct relationship with reactor core and primary circuit operation conditions and configurations. For example, the TEG [GWTS] system is a safety related system, operating in all plant operating modes. According to the design intent of the TEG [GWTS] system, the system has two distinct plant operation conditions and configurations, "steady-state operation mode" and "surge gas operation mode", neither of which has a direct relationship with reactor plant operating modes. The initial conditions in the surge gas operation mode are worse than those in steady-state

operating mode in terms of the radiological consequence. Similarly, I note that many radioactive waste management systems and some auxiliary systems have their own defined system operation conditions and configurations which are different from those of the reactor core and reactor primary circuit. I have therefore raised the following GDA assessment finding:

AF-UKHPR1000-0240 – The licensee shall define and use appropriate terms for the identification of postulated initiating events, design basis faults and fault analysis, which characterise the operating conditions and configurations for non-reactor plant (including, but not limited to the radioactive waste management systems and relevant plant auxiliary systems). This should include those systems whose operation, conditions and configurations have no direct relationship with those defined for the reactor.

839. I am content that this shortfall does not undermine the RP's safety case for non-reactor faults. I am also content that it is normal business for the safety case to develop as the design and operation of the waste route develops and is confirmed. Further work will be required to substantiate the claims made in due course.

4.6.1 Strengths

840. Following my assessment of the non-reactor faults I have identified the following strengths:

- The RP has adequately demonstrated that, based on the predicted frequency of component failures and consequences, there are no faults which require DBA.

4.6.2 Outcomes

841. As a result of my assessment of the non-reactor faults I have identified the following outcome:

- I have raised an Assessment Finding to ensure the licensee uses appropriate terms for the identification of faults where the systems have operating conditions and configurations distinct from those defined for the reactor.

4.6.3 Conclusion

842. Based on the outcome of my assessment, considering ONR SAPs FA.5 and NS-TAST-GD-006, I have concluded that the analysis of non-reactor faults is sufficient for GDA and that there are no faults which require DBA, however further development of the safety case will be required as the detailed design progresses to support operation.

4.7 Off-Site Radiological Consequences

843. A fundamental objective of DBA 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) following the successful operation of identified safety measures. Judgements on whether consequences are ALARP are informed by consideration of the radiological consequences of faults to people and a comparison of those consequences with targets that represent relevant good practice. For design basis faults, ONR's applicable targets are provided by Target 4 of the SAPs (Ref. 2).

844. Detailed radiological consequence analysis is not always necessary. The unmitigated consequences of many reactor faults are likely to be significantly higher than the BSL and detailed calculations would not add any value to the safety case. When considering fault sequences where the safety measures operate as intended, if there is

no fuel damage and containment barriers are maintained, there will be no additional radiological consequences above those expected in normal operation. In such cases I do not expect that radiological consequence calculations are performed.

845. For some reactor or SFP faults, even with the correct performance of safety measures there will be a loss of one physical barrier preventing the release of radioactive material. In these cases, a dose calculation is necessary, even if other acceptance criteria have been met.

846. I am content that the RP's approach to radiological consequences analysis is consistent with these broad expectations and integrated into the fault studies documentation:

- For many reactor faults analysed within Chapter 12 of the PCSR (Ref. 3) all acceptance criteria are met, so no explicit radiological consequences are presented.
- The RP has identified 11 DBC faults which are representative of all DBCs and the radiological consequences of these have been explicitly analysed in Ref. 58.

847. In my assessment I have applied the expectations of ONR's Target 4. As part of my assessment, I have sampled the validity of the methodologies that underpin the radiological consequence analyses. I have achieved this by a sampling approach (targeting reactor faults), and by drawing upon the assessment conclusions of colleagues in other topic areas. In the following sub-sections, I present my assessment of:

- 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 Target 4 of the SAPs.
- The RP's fuel route dose calculations.

848. The RP has also considered radiological consequences for DEC- A sequences and these are presented in Ref. 169. The RP has chosen to assess the DEC-A events against the radiological targets for DBC-4 faults and I note the RP's conclusions that the BSLs are met and that there is no significant increase in consequences for these faults. I have therefore chosen not to look in detail at the results or sample the underlying methods further in this section.

4.7.1 Reactor Source Terms

849. To assess the off-site consequences of faults the RP needs to calculate the amount of fission products that may be released from the fuel (during normal operations or as a result of the fault condition) and through the various containment barriers until they are dispersed in the environment. These can either be calculated using computer codes or determined from conservative assumptions. These source terms differ depending on the amount of fuel damage assumed and the details of the release paths. The assessment of these aspects has been led by ONR's Chemistry inspector (Ref. 37) who has concluded that the data are based on appropriate methodologies and can be considered conservative.

850. For the SGTR faults the RP has updated the analysis to use a less conservative source term methodology. ONR's Chemistry assessment has concluded that the

updated methodology is appropriate but notes that it relies on a lower limit on primary circuit activity being assumed. AF-UKHPR1000-0165 has been raised for a licensee to ensure that this primary circuit activity limit is captured as a safety limit by a licensee. This limit is a key control on limiting the consequences of all DBCs where the release is dominated by primary activity (i.e. where there is no fuel damage predicted) and so reducing this limit will have benefit to other fault sequences as well as SGTR faults.

851. I have therefore assumed that the source terms used by the RP in the radiological consequence analysis (Ref. 58) are appropriate for this use.

4.7.2 Radiological Consequences Methods and Assumptions

852. The RP's methodologies for calculation of radiological consequences (Ref. 170) has been assessed by an ONR specialist inspector (Ref. 171) who has found:

- The adopted weather stability conditions (type D3) used in the analysis are not as conservative as those that would normally be used for DBA for accidents in the UK. The National Radiological Protection Board's document (Ref. 172) cited by the RP's methodology document was written to support the normal operations assessment methodology and not design basis accident analysis, where the more pessimistic F2 conditions are considered good practice in the UK.
- The assumed weather conditions include light continuous rain at 0.1mm/hr for the duration of the releases, corresponding roughly to the UK average annual rainfall spread evenly over 24 hours, 365 days of the year. The rainfall assumption is likely to have a conservative impact on the ingestion and groundshine exposure pathways, but it is difficult to assess how much as results are not given for no rainfall or more realistic rainfall rates.
- The iodine release modelling is conservative, with no credit having been taken for removal of iodine in transit from the core to the environment. This is a robust, bounding assumption however this may be unduly conservative.
- Site specific analysis should be undertaken to refine the analysis and address conservatisms and uncertainties.
- It is likely that there is sufficient conservatism in the analysis that further refinement will show clearer compliance with the radiological targets, however this will need to be demonstrated.

853. The final conclusions of the ONR assessment in Ref. 171 is that the RP's methods and assumptions are appropriate for meaningful comparisons to be made against Target 4 of the SAPs. I have therefore assumed that the RP's dose predictions for design basis faults can be used for regulatory judgements on the adequacy of the generic UK HPR1000 design and safety case.

854. However, site specific analysis will be required to support some of the key assumptions made within Ref. 170 and, based on the conclusions of Ref. 171 I have therefore raised the following assessment finding.

AF-UKHPR1000-0241 – The licensee shall, as part of the site-specific radiological consequence analysis for design basis analysis, justify the underpinning assumptions used. This should include, but not be limited to, the shortfalls identified in GDA:

- Conservative weather conditions.
- Conservative deposition velocities.
- Age-specific groundshine and immersion dose conversion factors.
- Rainfall rates that are typical for UK weather as well as no rain at all.
- Use of conservatism in the source term, notably in relation to iodine radionuclides.

- The omissions of radionuclides from the source term.

4.7.3 Comparison of Design Basis Reactor Fault Doses with SAPs Numerical Target 4

855. Within the PCSR Chapter 12 and supporting references, the RP has presented radiological consequences for 10 representative reactor faults and compared these to radiological targets, consistent with the expectation of ONR NS-TAST-GD-005 (Ref. 4). The RP has also assessed two faults for dropped fuel element and dropped spent fuel flask. I have discussed these faults in Section 4.5 above on fuel route faults.

856. The bounding reactor faults are:

- Turbine trip
- SG Tube Rupture (One tube)
- Small Break LOCA
- Rupture of a Line Carrying Primary Coolant outside containment
- Volume Control Tank Break
- Spectrum of RCCA Ejection Accident
- Steam System Piping Large Break
- Large Break LOCA
- SGTR (two tubes in one SG)
- RHR system Piping break inside or outside containment
- RCP seizure (Locked Rotor) or RCP Shaft Break

857. I have discussed the off-site dose consequences for SGTR, RCCA ejection accidents, LB-LOCA and RCP seizure within the relevant parts of Section 4.3 above. In this section I have recorded my general observations and insights on the acceptability of the radiological consequences. As noted in Section 4.2 above, the RP's radiological dose targets for design basis faults are identical to ONR's Target 4. From a comparison of the predicted off-site doses (Ref. 58) against SAPs Target 4 I have the following observations:

- The majority of the 11 modelled design basis reactor faults are between the BSO and BSL for all age groups.
- A number of faults are close to the BSL and I have considered these in more detail in the relevant parts of Section 4.3.
- With the exception of turbine trip (adult) none of the faults are below the BSO, despite the relevant transient analysis showing that the acceptance criteria are met and no fuel damage is predicted. This suggests that the RP has made conservative assumptions within the calculation of off-site doses.
- There is no explicit consideration of the radiological consequences of the diverse means of protection for frequent faults.
- The use of bounding faults means that a comparison for less frequent version of the faults may challenge the relevant target.
- The radiological consequences in Ref. 58 do not include consideration of boiling of the spent fuel pool, which is now within the design basis as a diverse means of cooling (with ASP [SPHRS] makeup (as discussed in Section 4.5).

858. In the following paragraphs I consider each of these points in turn.

859. The majority of the faults sit between the relevant BSO and BSL of Target 4 of the SAPs (Ref. 2). It is ONR's policy (NS-TAST-GD-005, Ref. 4) that a new facility should at least meet the BSLs. The BSOs form benchmarks that reflect modern safety standards and expectations (SAPs paragraph 701). As such, taken at face value I have no concerns with the predicted consequences for the bounding reactor faults. I have discussed within Section 4.3 the SGTR fault which was challenging for the BSL and the most recent analysis shows that this fault too meets the BSL. I have however

used the radiological dose calculations to inform my assessment of the ALARP demonstration (presented in Section 4.8) where I have targeted my effort on those faults with the highest consequences, consistent with ONR guidance (Ref. 4).

860. Within Ref. 12 the RP has also considered the radiological consequences of the bounding transients for the demonstration of diverse protection for frequent faults. Table 2 of Ref. 12 presents, for each sequence, the fuel integrity, primary circuit integrity, the containment integrity and the release path. From this the RP considers that the consequences of the bounding sequences can be represented by four existing radiological analysis of a SB-LOCA, RCCA ejection accident, turbine trip or dropped fuel assembly. In my opinion this is a logical way to consider the potential consequences and the RP's logic is clear.

861. Feed and bleed of the primary circuit is claimed as the diverse line for faults involving a failure of the secondary side heat removal (from ASG [EFWS] or VDA [ASDS]). The RP claims within Ref. 12 that the radiological consequences of feed and bleed can be bounded by those of a SB-LOCA. This is on the basis that in both sequences while primary circuit integrity is lost, fuel integrity and containment integrity are maintained. In my opinion this argument needs developing further as the releases from these sequences are different in some important ways. However, I am content not to progress this during GDA because:

- In the SB-LOCA source term assessment the activity is released directly into the containment and the RP assumes that containment and the containment sweeping and blowdown ventilation system (EBA [CSBVS]) are isolated manually 30 minutes after the accident.
- During feed and bleed, primary coolant is discharged into the pressuriser relief tank rather than directly into the containment. This relief tank has a rupture disk which will relieve primary coolant into the containment when the rupture disk design pressure is reached. However, if containment is isolated before the feed and bleed is initiated there should be no release from the containment.

862. I am therefore content that the consequences of feed and bleed are likely to be acceptable. However, in my opinion a licensee should provide additional arguments on the acceptability of the radiological consequences of bleed and feed or else provide a calculation of these consequences, but I consider this to be a minor shortfall.

863. Notwithstanding this point on feed and bleed, given that the frequency of the sequences involving a failure of the primary line of protection will be lower than the four bounding sequences (which are all lower than the relevant BSL in Target 4) I am satisfied that the consequences of these faults are likely to be acceptable.

864. The bounding faults identified by the RP give confidence that the consequences of the most onerous reactor faults will be acceptable. However, the higher frequency faults which are bounded by these 11 faults should be compared against the more restrictive targets set by Target 4 for high frequency faults. I am content that for GDA this is not a significant concern as the RP has demonstrated through transient analysis that relevant acceptance criteria are met for frequent faults with no fuel damage predicted.

865. Although the radiological consequences of a boiling SFP are not included within Ref. 58, following discussions with the RP these have been included within Ref. 155. Within this document, the RP argues that there will be no fuel failures as a result of boiling and that the activity released is therefore based on the SFP water activity. The calculated off-site dose is 3.37 $x10^{-3}$ mSv (infant) and for workers is 1.02 $x10^{-5}$ mSv. These are both below the relevant BSOs set by the SAPs Target 4. I note that the assessment is based upon the normal operating activity limits and an operator exposure time of [redacted] minutes (consistent with the RP's worker dose methodology (Ref.

173). These assumptions will need to be confirmed prior to operation but I am content not to progress this further during GDA.

4.7.4 Strengths

866. The RP has presented off-site radiological consequences for representative design basis faults, taking into account UK specific expectations and good practice.

867. The calculated radiological consequences meet the RP's own criteria and fall below ONR's BSL for Target 4 of the SAPs.

4.7.5 Outcomes

868. Based on my assessment I have raised an Assessment Finding to refine the modelling of off-site radiological consequences for the design basis faults for comparison against relevant targets.

869. Assessment Finding AF-UKHPR1000-0165 (raised in ONR's Chemistry Assessment Report) on primary coolant activity levels needs to be addressed to ensure that the consequences of an SGTR will be below the relevant BSL of Target 4 of the SAPs.

4.7.6 Conclusion

870. From my assessment I have concluded that the RP's methods and assumptions for off-site radiological consequence assessments are appropriate for meaningful comparisons to be made against Target 4 of the SAPs. I have therefore assumed that the RP's dose predictions for design basis faults can be used for regulatory judgements on the adequacy of the generic UK HPR1000 design and safety case.

871. I am satisfied that the radiological consequences of the bounding design basis faults are between the relevant BSO and BSL of ONR's Target 4 for all age groups. I am also content that the successful operation of safety measures for the majority of the reactor faults on the fault schedule should result in no off-site consequences at all.

4.8 Demonstration that Relevant Risks Have Been Reduced to ALARP

4.8.1 Assessment

872. The RP has produced a specific document for the demonstration of ALARP for the fault studies area at Ref. 174. This document is supported by a number of other documents which together support safety case claim 3.4 'The safety assessment shows that the nuclear safety risks are ALARP.' The principal supporting documents include:

- Compliance Analysis of Codes and Standards in Fault Studies (Ref. 175).
- Supporting Report on No Fuel Failure for Frequent Faults (Ref. 176).
- Supporting report on ALARP Assessment for DNB analysis (Ref. 21).
- ALARP Assessment for DBC radiological consequence (Ref. 61).
- Optioneering on the Reduction of SGTR Radiological Consequence (Ref. 94).

873. Ref. 174 presents a holistic ALARP assessment and a specific ALARP assessment. The holistic assessment is an overview of the evolution of the reference design, a discussion of compliance against RGP, a review of OPEX and a risk assessment. The specific ALARP assessment presents arguments for two specific areas studied by the RP in GDA; boron dilution faults and inadvertent reactor pit flooding. In my opinion the scope of the report is appropriate and consistent with the general expectations of NS-TAST-GD-005. The choice of topics for specific studies in this document is unclear as there are other topics which have also been studied during GDA (such as the safety

classification of key SSCs) but as these are recorded in other documents, I am content that this is a minor shortfall.

874. The risk assessment part of Ref. 174 includes a discussion of the results of the transient analysis against the decoupled criteria and the radiological targets. This discussion is supported by documents to demonstrate no fuel failure for frequent faults (Ref. 176), ALARP assessment for DNB (Ref. 21) and an ALARP assessment for DBC radiological consequences (Ref. 61). These studies meet my expectation that the RP should seek to demonstrate that there are no reasonably practicable measures to further reduce consequences, rather than relying solely on meeting relevant criteria. The most significant consequences discussed in this section are associated with the locked rotor, RCCA ejection and SGTR faults and I have recorded my assessment of these in the relevant parts of Section 4.3. Of particular relevance to this assessment are Assessment Findings AF-UKHPR1000-0165 (raised in the Chemistry topic area) on primary coolant activity and AF-UKHPR1000-0010 on RCCA ejection (raised in the Fuel and Core topic area) which will need to be addressed to support the conclusions of Ref. 174.

875. The risk assessment also includes a discussion of functional diversity for frequent faults. The RP summarises the shortfalls that had originally been identified in this demonstration and the outcomes of the optioneering that has been conducted to address these. I have discussed each of the items presented in this section of Ref. 174 in the relevant parts of Section 4.3.

876. During GDA, the RP has incorporated a number of plant modifications into the generic UK HPR1000 design and the most important of these modifications (from a fault studies perspective) are summarised in Ref. 174. From the documents that I have sampled as part of my assessment I am content that these modifications have been appropriately integrated into the UK HPR1000 safety case and I have discussed these within the relevant parts of this assessment. The modifications with the most relevance to my assessment are:

- M32 The classification of the ASP function to deliver water to the SFP has been raised from F-SC3 to F-SC2.
- M35 The DEL [SCWS] has been modified to improve its reliability and introduce diversity to reduce the risks of a CCF.
- M61 Modification of safety injection signal in KDS [DAS].
- M68 Modification spurious dilution caused by the LHSI pump seal cooling heat exchanger break.
- M87 Modification of start-up procedure of RCPs for implementation of new FC1 interlocks.
- M88 Modification of Overpressure ΔT setpoint for resolution of PCI negative margin.
- M94 Modification of the BFX to adopt gantry crane for fuel handling.

877. The RP has also reviewed the radiological consequences assessment and identified some further options which could reduce consequences further. The options include:

- Upgrade the F-SC3 EHR [CHRS] to scrub aerosol iodine.
- Reducing the assumed time to reach a negative pressure in the safeguard/fuel building. The RP has stated that if the negative pressure is established within 20 minutes (rather than the 30 minutes currently assumed in the consequences assessment) the radiological consequences to a person off-site can be reduced by about 4%.

878. The RP has rejected these options on the basis that the detriments outweigh the potential benefits. I have considered the arguments presented in Ref. 174 and I am

content to support this view, although it should be noted that even as an F-SC3 function the EHR [CHRS] will provide a benefit to the consequences and it is not credited in the RP's analysis.

4.8.2 Strengths

879. The RP has provided a comprehensive summary of the work that has been done to demonstrate that, from a fault studies perspective, risks are reduced ALARP.

4.8.3 Outcomes

880. I have not identified any shortfalls from my assessment of ALARP in the fault studies topic area. However, I have discussed a number of Assessment Findings AF-UKHPR1000-0165 (raised in the Chemistry topic area) on primary coolant activity and AF-UKHPR1000-0010 on RCCA ejection (raised in the Fuel and Core topic area) which will need to be addressed to support the conclusions of Ref. 174.

4.8.4 Conclusion

881. From my review of Ref. 174 and supporting documents I am satisfied that the scope of the ALARP case in the fault studies area is consistent with the expectations of NS-TAST-GD-005.

882. I am satisfied that the RP has identified appropriate improvements that can be made to the generic UK HPR1000 design to reduce risk and that these have been integrated into the safety case.

883. I am therefore satisfied that the demonstration in the fault studies area that risks have been reduced ALARP is sufficient for GDA.

4.9 Consolidated Safety Case

4.9.1 Assessment

884. My assessment of the UK HPR1000 fault studies safety case for GDA has been based on:

- the set of safety case submissions provided by the RP and summarised in Section 3.
- responses provided by the RP to ROs and RQs that I raised during GDA.
- information provided to me during my technical interactions with the RP during GDA.

885. At the end of GDA, the RP is expected to capture relevant information from RQs, ROs and other interactions in final versions of the safety case documents. These final safety case submissions are captured in the Master Document Submission List (MDSL) (Ref. 177) and constitute the basis for future development of the safety case by a licensee. It is these documents, including version 2 of the PCSR (noting that Ref. 3 is version 1), against which a DAC or interim DAC will be awarded, if that is the outcome from GDA.

886. I have therefore undertaken a further sample to check that information I was previously provided relevant to my assessment has subsequently been consolidated sufficiently well into the safety case submissions captured in the MDSL.

887. The majority of additional submissions have been provided in response to ROs or RQs that I have raised during GDA. These submissions have either been new documents or

updates to existing submissions and I have discussed these within my assessments of the relevant parts of the safety case.

888. Additional information has also been provided in response to RQs that I have raised during my assessment (Ref. 6). In general, I am satisfied that the RP has updated documents as required throughout GDA and that the information from RQs has been appropriately incorporated. To confirm this I have sampled the following responses to RQs:

- RQ-UKHPR1000-0504 Passive single failures. The information submitted in response to this RQ is included within the Evaluation of Passive Single Failures Rev. C (Ref. 178).
- RQ-UKHPR1000-0686 Large Steam System Piping Breaks. The information submitted in response to this RQ is included within the Steam System Piping Break Rev D (Ref. 54).
- RQ-UKHPR1000-0746 Primary Overpressure Protection and Consequential LOCA. This information submitted in response to this RQ is included within the SB-LOCA (State A) analysis Rev C (Ref. 179).

889. On this basis, I am content that the information from RQs has been adequately incorporated in the generic UK HPR1000 safety case. In addition, I am satisfied that the work undertaken by the RP to evaluate fault conditions arising from support systems and spurious C&I actuation faults has been integrated into the rest of the safety case.

890. I have also sampled revision 2 of PCSR Chapter 12 and relevant parts of Chapter 13 (Ref. 180 and 181), submitted after the end of my formal assessment period, to check that they contain the information expected and is consistent with my assessment. My review of Refs. 180 and 181 did not focus on technical detail, which I have covered in previous subsections of this report. Rather I have reviewed it for completeness against SAP SC.4, for ease of readability and to check whether interfaces and references are captured with sufficient clarity that the safety case is coherent.

891. In my opinion, Refs. 179 and 180 provides adequate linkage between the top-level claims, sub-claims, supporting arguments and evidence in the Fault Studies safety case (as summarised in Section 3). It summarises the ALARP arguments that I have assessed in sub-section 4.8 of this report. The technical content is of sufficient detail for this document, with references provided for further detail. I am satisfied that the document covers all aspects of the safety case expected by SAP SC.4 with the exception that operating rules are covered separately in PCSR Chapter 31 and that information about commissioning and EMIT is relatively limited in GDA, as discussed previously in this report.

892. Overall, I judge that revision 2 of PCSR Chapter 12 and relevant parts of Chapter 13 (Refs. 180 and 181) are adequate to provide an overview of the consolidated Fault Studies safety case with references out to further information.

4.9.2 Strengths

893. Following my assessment of the UK HPR1000 consolidated safety case I have identified the following strengths:

- based on my sample of submissions late in GDA, sufficient information previously shared with me by the RP that was important to my assessment (with known exceptions for reasons referred to previously in this report) has now been consolidated within the UK HPR1000 safety case;

- PCSR Chapters 12 and 13 version 2 (Refs. 180 and 181) provide an adequate overview of the consolidated safety case with references out to supporting information and meets the expectations set by SAP SC.4 for the purpose of GDA.

4.9.3 Conclusion

894. Based on the outcome of my assessment, I have concluded that information provided to me by the RP that is relevant to my assessment has now been sufficiently well consolidated in submissions included in the MDSL.

4.10 Comparison with Standards, Guidance and Relevant Good Practice

895. As explained in sub-section 2.4, the key SAPs I have used in this assessment are FA.1 to FA.9, EKP.1 to EKP.4, ECS.1 and ECS.2, AV.1 to AV.3. I have referred to other SAPs on an occasional basis throughout this report and the full list is presented in Annex 1.

896. The most relevant ONR TAG for assessment of fault studies is NS-TAST-GD-006. NS-TAST-GD-005, NS-TAST-GD-051 and NS-TAST-GD-094 have also been particularly important to parts of my assessment.

The most relevant IAEA guidance for the deterministic safety analysis is SSG-2. SSR-2/1 also contains a number of relevant requirements. Other than where I have identified minor shortfalls or assessment findings in this report, I am satisfied that the expectations I derived from these sources of RGP have been met by the UK HPR1000 fault studies safety case in the areas I have sampled.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

897. This report presents the findings of my Fault Studies assessment of the generic UK HPR1000 design as part of the GDA process.

898. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- The RP has adequately identified design basis faults and design extension conditions for all reactor operating modes for a range of potential initiating events, including those arising from support systems or as a result of spurious control or instrumentation actuations. The RP has also given appropriate consideration to fuel route and non-reactor facilities with significant radiological hazards.
- The RP has produced an adequate fault schedule with contents consistent with my expectations.
- The RP has appropriately assessed faults with adequate tools and methods, with appropriate levels of conservatism.
- The RP 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. While a departure from nucleate boiling is predicted for two limiting reactor faults, the predicted doses have been shown to be acceptable against numerical targets established in the SAPs.
- The RP has demonstrated that the design is capable of protecting against a loss of spent fuel pool cooling and that the consequences of a loss of inventory from the spent fuel pool will be limited or that they can be isolated and water level maintained.
- The RP has demonstrated that the availability requirements of the design basis analysis can be satisfied by the scheduling of maintenance activities.
- The analysis of non-reactor faults is sufficient for GDA and there are no faults arising within the waste route which qualify for treatment as design basis faults, however further development of the safety case will be required as the detailed design progresses.
- Where faults lead to a loss of one or more containment barriers the predicted radiological doses have been shown through conservative analysis to be acceptable against numerical targets established in ONR SAPs.
- Fault studies has been used to support general ALARP claims on the adequacy of the generic UK HPR1000 design. This has been supplemented in a number of areas by detailed optioneering studies where further design changes have been considered and implemented by the RP.

899. A number of matters remain, which I judge are appropriate for a licensee to consider and take forward in its site-specific safety submissions. These matters do not undermine the generic UK HPR1000 design and safety submissions but are primarily concerned with the provision of site-specific safety case evidence which will become available as the project progresses through the detailed design, construction and commissioning stages. These matters have been captured in Assessment Findings.

900. Overall, based on my sample assessment of the safety case for the generic UK HPR1000 design undertaken in accordance with ONR's procedures, I am satisfied that the case presented within the PCSR and supporting documentation is adequate. On this basis, I am content that a DAC should be granted for the generic UK HPR1000 design from a Fault Studies perspective.

5.2 Recommendations

901. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From a Fault Studies perspective, ONR should grant a DAC for the generic UK HPR1000 design.

- **Recommendation 2**: The 17 Assessment Findings identified in this report should be resolved by the licensee for a site specific application of the generic UK HPR1000 design.

6 REFERENCES

1. *New nuclear reactors: Generic Design Assessment: Guidance to Requesting Parties for the UK HPR1000*. ONR-GDA-GD-001. Revision 4. October 2019. ONR. www.onr.org.uk/new-reactors/ngn03.pdf

   New Nuclear Power Plants: Generic Design Assessment Technical Guidance. ONR-GDA-GD-007. Revision 0. May 2019. ONR. http://www.onr.org.uk/new-reactors/reports/onr-gda-007.pdf

2. *Safety Assessment Principles for Nuclear Facilities*. 2014 Edition, Revision 1. January 2020. http://www.onr.org.uk/saps/saps2014.pdf

3. Pre-Construction Safety Report

   Chapter 4 General Safety and Design Principles. HPR/GDA/PCSR/0004. Rev 001. January 2020. GNSL. 2020/13628.

   Chapter 6 Reactor Coolant System. HPR/GDA/PCSR/0006. Rev 001. January 2020. GNSL. 2020/13625.

   Chapter 7 Safety Systems. HPR/GDA/PCSR/0007. Rev 001. January 2020. GNSL. 2020/13658.

   Chapter 12 Design Basis Condition Analysis. HPR/GDA/PCSR/0012. Rev 001. January 2020. GNSL 2020/13934. 2020/13934.

   Chapter 13 Design Extension Conditions and Severe Accident Analysis. HPR/GDA/PCSR/0013. Rev 001. January 2020. GNSL. 2020/13935.

4. Technical Assessment Guides

   Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). NS-TAST-GD-005. Revision 9. May 2013. ONR.

   Design Basis Analysis. NS-TAST-GD-006. Revision 5. October 2020. ONR.

   Limits and Conditions for Nuclear Safety (Operating Rules). NS-TAST-GD-035. Revision 6. March 2018. ONR.

   The Purpose, Scope and Content of Nuclear Safety Cases. NS-TAST-GD-051 Revision 7. December 2019. ONR.

   Categorisation of Safety Functions and Classification of Structures, Systems and Components. NS-TAST-GD-094. Revision 2. July 2019. ONR.

   Guidance on Mechanics of Assessment. NS-TAST-GD-096 Revision 0. April 2020. ONR.

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

5. *GDA Step 4 Assessment Plan of Fault Studies for the UK HPR1000 Reactor*. ONR-GDA-AP-19-015. Revision 0. ONR. 2020/35211.

6. *UK HPR1000 – Regulatory Query (RQ) Tracking Sheet*. ONR. CM9 Ref. 2017/407871.

7. *UK HPR1000 – Regulatory Observation (RO) Tracking Sheet*. ONR. CM9 Ref. 2019/465031.

8. International Atomic Energy Agency (IAEA) guidance –

Safety of Nuclear Power Plants: Design. Specific Safety Requirements No SSR-2/1. Rev. 1. February 2016. IAEA.

Deterministic Safety Analysis for Nuclear Power Plants. No. SSG-2 (Rev. 1). 2019. IAEA.

Safety of Nuclear Power Plants: Design. Safety Requirements. International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-R-1. 2000. IAEA.

Safety Classification of Structures, Systems and Components in Nuclear Power Plants. Specific Safety Guide. SSG-30. 2014. IAEA.

Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants. IAEA TecDoc 1791. 2016. IAEA.

Design of the Reactor Containment and Associated Structures for Nuclear Power Plants. Specific Safety Guide. SSG-53. 2019. IAEA

www.iaea.org.

9. Western European Nuclear Regulators' Association.

Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. WENRA. September 2014.

Western European Nuclear Regulators' Association. Reactor Harmonization Group. Safety of new NPP designs. WENRA. March 2013.

WENRA Statement on Safety Objectives for New Nuclear Power Plants. WENRA. November 2010.

www.wenra.eu

10. *UK HPR1000 Fault Schedule.* GHX00600276DRAF02GN. Rev D. January 2021. CGN. 2021/8482.

11. *The Design Condition List and Acceptance Criteria.* GHX00100029DOZJ04GN Rev. J. January 2021. CGN. 2021/2094.

12. *Transient Analysis Report for Diverse Protection Line Demonstration.* GHX00600141DRAF02GN. Rev C. September 2020. CGN. 2020/288677.

13. *Methodology of Safety Categorisation and Classification*. GDA-REC-CGN-001768-GHX00100062DOZJO3GN. Rev B. June 2018. CGN. 2018/199731.

14. *LOCUST - A Thermal Hydraulic System Analysis Code: Qualification Report.* CNPRIGNF1117REC010004. Rev A. March 2019. CGN. CM92019/94120.

15. *GINKGO – A Transient System Analysis Code: Qualification Report.* CNPRIGNF1117REC010009. Rev A. March 2019. CGN. 2019/94142.

16. *CATALPA – A Thermal Hydraulic Containment Analysis Code: Qualification Report.* CNPRGNF1117REC010011. Rev A. March 2019. Ref. 2019/94146.

17. *LOCUST – A thermal-hydraulic System Analysis Code: Verification and Validation Report.* GHX00600143DRAF02TR. Rev D. March 2021. CGN. 2021/28217.

18. *GINKGO – A Transient System Analysis Code: Verification and Validation Report.* GHX0060014DRAF02TR. Rev D. March 2021.

19. *CATALPA -A Thermal-hydraulic Containment Analysis Code: Verification and Validation Report.* GHX00600139DRAF02TR. Rev B. July 2020.

20. *Step 4 Assessment of Fuel and Core for the UK HPR1000 Reactor.* ONR-NR-AR-21-021. 2021/23724.

21. *Supporting report on ALARP Assessment for DNB analysis.* GHX00120001DRAF00GN. Rev D. March 2021. CGN. 2021/28197.

22. *Definition of Normal Operating Modes and Corresponding Parameters.* GHX71100001DOYX03GN. Rev B. Oct 2018. CGN. 2018/315841.

23. *Generic limits and conditions for normal operation.* GX37OTS001DOYX45GN. Rev. B. May 2021. CGN. 2021/37697.

24. *Step 4 Assessment of PSA for the UK HPR1000 Reactor.* ONR-NR-AR-21-020. 2021/49362.

25. *Comparison of DBC list.* GHX00100118DOZJO3GN. Rev D. August 2020. CGN. 2020/258617.

26. *PIE list of UK HPR1000 of internal event (except for loss of support system).* GHX00100110DOZJ03GN. Rev H. May 2021. CGN. 2021/43558.

27. *PIE Grouping and Bounding Analysis for the PIE of Internal Event (Except for Loss of Support System).* GHX00100007DRAF03GN. Rev. E. August 2020. CGN. 2020/257001.

28. *Step 4 Assessment of Internal Hazards for the UK HPR1000 Reactor.* ONR-NR-AR-21-012. 2021/55302.

29. *UK HPR100 Fuel Assembly Mechanical Design.* GHX42500029SFSL44GN – FS1-0049660. Rev 2. September 2020. 2020/259703.

30. *Impact on Reactor Core and Primary Circuit Analysis Under the Inadvertent Flooding of the Reactor Pit Condition.* GHX00600368DRAF02GN. Rev A. July 2020. 2020/214820

31. *The Thermal Shock Analysis of RPV While Inadvertent Flooding of Reactor Pit Condition.* GHX00100041DPLX44GN. Rev A. July 2020. 2020/214799.

32. *Step 4 Assessment of Structural Integrity for the UK HPR1000 Reactor.* ONR-NR-AR-21-016. 2021/52300.

33. *Optioneering on the EHR [CHRS] Related to the Inadvertent Reactor Pit Flooding.* GHX00100002DNHX45GN. Rev C. December 2020. 2020/320736.

34. *Bounding case Selection for Diverse Protection Line Demonstration.* GHX00600277DRAF02GN. Rev D. May 2020. CGN. 2020/130904.

35. *Identification of DEC-A Sequences.* GHX00600001DOZJ02GN. Rev C. September 2020. CGN. 2020/270202.

36. *Decomposition of Safety Functions.* GHX80001001DOZJ03GN. Rev E. November 2020. CGN. 2020/315882.

37. *Step 4 Assessment Report of Chemistry for the UK HPR1000 Reactor.* ONR-NR-AR-21-002. 2021/41488.

38. *Examination, Maintenance, Inspection and Testing (EMIT) Strategy.* GHX42EMT001DOYKX45GN. Rev C. July 2020. CGN. 2020/225864.

39. *Examination, Maintenance, Inspection and Testing (EMIT) Windows.* GHX42EMT002DOYX45GN. Rev D. January 2021. CGN. 2021/8441.

40. *Step 4 Cross Cutting Assessment Report.* ONR-NR-AR-21-007. 2021/47905.

41. *LOCUST Detailed Code Review for the UK HPR1000 Safety Case on behalf of ONR.* ONRTSF/4NT/0714087/000/01. Rev 1. December 2020. Tractebel. 2021/21726.

42. *GINKGO Detailed Code Review for the UK HPR1000 Safety Case on behalf of ONR.* ONRTSF/4NT/0713390/000/01. Rev 1. December 2020. Tractebel. 2021/21725.

43. *CATALPA Code Review for the UK HPR1000 Safety Case on behalf of ONR.* ONRTSF4NT068503200001. Rev 1. March 2020. Tractebel. 2020/97042.

44. *Inadvertent Closure of One or All Main Steam Isolation Valves.* GHX00600089DRAF02GN. Rev C. November 2019. 2019/355731.

45. *Primary Side Overpressure Analysis Category 3*. GHX00600042DRAF02GN. Rev C. November 2019. CGN. 2019/355840.

46. *Inadvertent Closure of All Main Steam Isolation Valves with PSVs Fail to Open.* GHX00600284DRAF02GN. Rev A. August 2019. CGN. 2019/239885.

47. *Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG.* GHX00600072DRAF02GN. Rev C. November 2019. CGN. 2019/355822.

48. *Primary Side Overpressure Analysis – Category 4.* GHX00600043DRAF02GN. Rev C. CGN. 2019/355838.

49. *Short Term LOOP of 2 Hours Duration.* GHX00600028DRAF02GN. Rev. D. November 2019. CGN. 2019/355847.

50. *Medium Term LOOP of 24 Hours Duration.* GHX00600030DRAF02GN. Rev. D. September 2020. CGN. 2020/288715.

51. *Japanese earthquake and tsunami: Implications for the UK nuclear industry, Final Report*. September 2011. ONR. 2017/11808.

52. *European Utility Requirements for LWR nuclear power plants.*

53. *Increase in Feedwater Flow due to Feedwater System Malfunctions*. GHX00600075DRAF02GN. Rev C. November 2019. CGN. 2019/352938.

54. *Steam System Piping Large Break.* GHX00600081DRAF02GN. Rev D. August 2021. CGN. 2021/63481.

55. *Step 4 Assessment of Human Factors for the UK HPR1000 Reactor.* ONR-NR-AR-21-013. 2021/54151.

56. *UK HPR1000 – ONR396 Fault Studies Confirmatory Analysis D2.2.07 Phase 2 Technical Report Main Steam Line Break Analyses.* Rev 1. March 2021. GRS. 2021/30131.

57. *UK HPR1000 – ONR396 Fault Studies Confirmatory Analysis D2.2.07 Phase 2 Technical Report Main Steam Line Break Analyses.* Rev 1. March 2021. GRS. 2021/30131.

58. *Off-site Radiological Consequences analysis for Representative DBC Accidents of UK HPR1000.* GHX00100011DOHB00GN. Rev C. March 2021. CGN. 2021/28192.

59. *Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break.* GDA-REC-CGN-003083. Rev B. November 2018. CGN. 2018/367819.

60. *ONR396 Fault Studies Confirmatory Analysis – D2.2.05 Phase 2 Technical Report Reactor Coolant Pump Seizure (Locked Rotor).* Rev 1. March 2021. GRS. 2021/30129.

61. *ALARP Assessment for DBC Radiological Consequence.* GHX00600375DRAF02GN. Rev B. April 2021. CGN. 2021/31456.

62. *Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump.* GHX00600051DRAF02GN. Rev C. November 2019. CGN. 2019/352924.

63. *Forced Reduction in Reactor Coolant Flow (3 pumps).* GHX00600050DRAF02GN. Rev C. November 2019. CGN. 2019/355829.

64. *Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition (State A).* GHX00600095DRAF02GN. Rev C. November 2019. CGN. 2019/352921.

65. *UK HPR1000 – ONR396 Fault Studies Confirmatory Analysis – D2.2.08 Phase 2 Technical Report Uncontrolled RCCA Bank Withdrawal at Low Power Startup Conditions.* Rev 1. March 2021. GRS. 2021/30133.

66. *ATWS by Rods Failure – RCCA Bank Withdrawal at Power (State A).* GHX006002900DRAF02GN. Rev C. August 2020. CGN. 2020/256980.

67. *Source Term Analysis of RCCA Ejection Accidents.* GHX00600013DRAF02GN. Rev E. June 2020. CGN. 2020/189937.

68. *Functional Requirements for Prevention and Protection against Boron Dilution.* GHX11000001DOZJ45GN. Rev D. April 2021. CGN. 2021/35433.

69. *Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS].* GHX00600002DRDG02GN. Rev F. April 2021. CGN. 2021/34065.

70. *Justification Report on Boron Dilution Isolation Valves for RCV [CVCS] Malfunction Mitigation.* GHX00600026DRDG03GN. Rev A. May 2020. CGN. 2020/161919.

71. *RCCA Misalignment up to Rod Drop Without Limitation.* GHX00600091DRAF02GN. Rev C. November 2019. CGN. 2019/352893.

72. *ONR396 Fault Studies Confirmatory Analysis – D2.2.09 Phase 2 Technical Report RCCA misalignment up to Rod Drop without Limitation.* Rev 1. March 2021. GRS. 2021/30135.

73. *Spectrum of RCCA Ejection Accident*. GHX00600092DRAF02GN. Rev C. November 2019. CGN. 2019/352936.

74. *Small Break - Loss of Coolant Accident (State A).* GHX00100043DRAF03GN. Rev B. November 2019. CGN. 2019/355870.

75. *ONR396 Fault studies Confirmatory Analysis* – D2.2.01 Phase 2 Technical Report Loss of Coolant Accidents. Rev 1. March 2021. GRS. 2021/30124.

76. *Small Break LOCA with Failure of Reactor Trip Sensor*. GHX00600283DRAF02GN. Rev B. August 2020. CGN. 2020/256999.

77. *Small Break – Loss of Coolant Accident (SB-LOCA) with Failure of Medium Pressure Rapid Cooldown (MCD) (State A).* GHX00600096DRAF02GN. Rev D. November 2019. CGN. 2019/355720.

78. *Small Break - loss of Coolant Accident (SB-LOCA) with Total Loss of Low Head Safety Injection (LHSI) (State A).* GHX00600098DRAF02GN. Rev C. November 2019. CGN. 2019/352806.

79. *SB-LOCA with Total Loss of Medium Head Safety Injection (MHSI) (State A).* GHX00600097DRAF02GN. Rev D. November 2019. CGN. 2019/355708.

80. *ATWS by Rods Failure – Small Break Loss of Coolant Accident (SB-LOCA) (State A).* GHX00600286DRAF02GN. Rev B. November 2019. CGN. 2019/352890.

81. *Optioneering Report on Safety Injection Signal in SBLOCA.* GHX00100058DRAF03GN. Rev A. April 2020. CGN. 2020/128289.

82. *Internal Events Level 1 PSA.* Rev. B. CGN. April 2020. CGN. 2020/112233.

83. *Intermediate Break and up to Surge Line Break - Loss of Coolant Accident.* GHX00100042DRAF03GN. Rev C. March 2021. CGN. 2021/28199.

84. *VDA Atmospheric Steam Dump System Design Manual – Chapter 4 System & Component Design.* GDA-REX-CGN-002517. Rev A. CGN. October 2018. 2018/318474.

85. *LB-LOCA safety case clarification and core assessment report.* GHX00600007DRRL02GN. Rev C. June 2021. 2021/46979.

86. *Step 4 Assessment of Severe Accident Analysis for the UK HPR1000 Reactor*. ONR-NR-AR-21-008. 2021/49781.

87. *Large Break – Loss of Coolant Accident (up to double-ended break).* GHX00600004DRAF02GN. Rev D. July 2021. 2021/58474.

88. *The Delivery of UK HPR1000 GDA Design Modification Cat 1 "Design Modification of HIC Welds Inspectibility Related to MCL and MSL".* HPR-GDA-Lett-0098. December 2020. GNSL. 2020/318910.

89. *SG Tube Rupture (One Tube).* GHX00600084DRAF02GN. Rev C. November 2019. CGN. 2019/355758.

90. *Human reliability Assessment Report for Isolating Impaired SGG Manually*. GHX06001046DIKX03GN. Rev b. November 2020. CGN. 2020/314647.

91. *Supplementary Analysis Report for SGTR Event Considering Operator Available Time.* GHX0060038DRAF02GN. Rev A. November 2020. CGN. 2020/314651.

92. *ONR396 Fault studies Confirmatory Analysis – D2.2.04 Phase 2 Technical Report SG Tube Rupture (One Tube).* Rev 1. March 2021. 2021/30128.

93. *Optioneering on VVP [MSS] related to the Loss of MSL Isolation induced by CCF under SGTR (one tube).* GH00100070DNHX03GN. July 2020. CGN. 2020/233049.

94. *Optioneering on the Reduction of SGTR Radiological Consequences.* GHX00600370DRAF02GN. Rev C. April 2021. CGN. 2021/31455.

95. *Multiple Steam generator (SG) Tubes Rupture (10 tubes) (State A).* GHX00600086DRAF02GN. Rev C. November 2019. CGN. 20199/355748.

96. *SGTR (1 tube) with Atmospheric Steam Dump System (VDA [ASDS]) stuck open in the SG affected (State A).* GHX00600087DRAF02GN. Rev C. November 2019. CGN. 2019/355737.

97. *The Investigation Report on the Debris Effect.* GHX22400001DNHX00TR. Rev A. May 2020. 2020/130999

98. *Assessment of Debris in IRWST Under Accident Conditions.* GHX00600350DRAF02GN. Rev A. May 2020. 2020/161958.

99. *Optioneering Report of the Upstream Material.* GHX9980001DNHX45GN. Rev B. August 2020. CGN. 2020/235211.

100. *ALARP Demonstration Report for Safety Systems*. GHX00100050KPGB03GN. Rev E. December 2020. CGN. 2020/322688.

101. *Upstream Material Change Impact Analysis Report*. GHX99980002DNHX45GN. Rev A. August 2020. 2020/233068.

102. *Strainer upstream Debris Source Term analysis report*. GHX99980003DNHX45GN. Rev B. January 2021. CGN. 2021/4839.

103. *Uncontrolled RCP [RCS] Level Drop*. GHX00600048DRAF02GN, Rev C, November 2019. CGN. 2019/352961.

104. *RHR System Piping Break inside or outside Containment*. GHX00600124DRAF02GN. Rev C. November 2019. CGN. 2019/355691.

105. *Safety Functional Requirements of RIS [SIS].* GHX00600351DRAF02GN. Rev E. May 2021. 2021/43560.

106. *Identification of DBC list from PIE Grouping Results*. GHX00100056DRAF03GN. Rev D. January 2021. 2021/2756.

107. *Analysis for Loss of Support System Events.* GHX00600349DRAF02GN, Rev A, October 2020, CM9 Ref 2020/300435.

108. *PIE list of Spurious Actuation for I&C Systems.* GHX00100003DIYK03GN. Rev F. July 2021. CGN. 2021/51808.

109. *Step 4 Assessment of Control & Instrumentation for the UK HPR1000 Reactor.* ONR-NR-AR-21-005. 2021/46296.

110. *PIE Bounding Process of Spurious I&C Actuation*. GHX00100009DRAF03GN. Rev C. October 2020. CGN. 2020/305445.

111. *Analysis for Spurious I&C Actuation Events.* GHX00600348DRAF02GN. Rev B. October 2020. CGN. 2020/305433.

112. *CFD Analysis of Critical Water Slug Size for External Heterogeneous Dilution Scenarios.* GHX00600141DRAF02GN. Rev A. September 2020. CGN. 2020/288681.

113. *Demonstration of the Elimination of External Heterogeneous Boron Dilution.* GHX00600001DOZJ45GN. Rev C. February 2021. 2021/17446.

114. *Frequency Analysis for the PIE of Internal Event.* GHX00100117DOZJ03GN. Rev C. January 2021. 2021/8498.

115. *ONR GDA Close-out - UK EPR - GI-UKEPR-FS-01 Revision 1.* ONR-GDA-AR-12-010 Revision 0 DRAFT 1. 2012/10.

116. *Functional Requirements for Prevention and Protection against Boron Dilution.* GHX11000001DOZJ45GN. Rev B. December 2020. 2020/322749.

117. *M87 Modification for Start-Ip Procedure of Reactor Coolant Pumps.* HPR-GDA-LETT-0108. April 2021. GNSL. 2021/30975.

118. *Inherent Heterogeneous Boron Dilution Analysis.* GHX00600363DRAF02GN, Rev A, August 2020. (CM9 2020/233823).

119. *Asymmetry impact on state points and safety margins.* GHX00600387DRAF02GN. Rev A. March 2021. CGN. 2021/28196.

120. *Mass and Energy Release in case of Loss of Coolant Accident.* GHX00600310DRAF02GN. Rev. A. November 2020. CGN. 2020/314652.

121. *Mass and Energy Release in case of Steam Line Break*. GHX00600311DRAF02GN. Rev A. November 2020. CGN. 2020/314654.

122. *Containment P&T Analysis in case of Loss of Coolant Accident*. GHX00600006DRAF02GN. Rev D. June 2021. CGN. 2021/43831.

123. *Containment P&T Analysis in Case of Steam Line Break*. GHX00600241DRAF02GN. Rev C. January 2021. CGN. 2021/8435.

124. *Total Loss of Feedwater (State A).* GHX00600074DRAF02GN. Rev D. November 2019. CGN. 2019/355803.

125. *Small Break – Loss of Coolant Accident (SB-LOCA) with Failure of Medium Pressure Rapid Cooldown (MCD) State A.* GHX00600096DRAF02GN. Rev D. November 2019. CGN. 2019/355720.

126. *ASP-Secondary Passive Heat Removal System Design Manual Chapter 4 System and Component Design.* GHX17ASP004DNHX45GN. Rev. E. June 2021. CGN. 2021/52570.

127. *Assessment of ASP [SPHRS] Effectiveness.* GHX00600381DRAF02GN. Rev B. July 2021. CGN. 2021/58475.

128. *UK HPR1000 – ONR396 Fault Studies Confirmatory Analysis – D2.2.02 Phase 2 Technical Report Total Loss of Feed Water.* Rev 1. March 2021. GRS. 2021/30126.

129. *Loss of Ultimate Heat Sink (LUHS) for 100 Hours (States A and B).* GHX00600251DRAF02GN. Rev C. December 2020. CGN. 2020/322718.

130. *EHR Containment Heat Removal System Design Manual Chapter 3 System Functions and Design Basis.* GDA-REC-CGN-002337. Rev A. October 2018. CGN. 2018/318484.

131. *ECS Extra Cooling System Design Manual Chapter 3 System Functions and Design Basis.* GHX17ECS003DNHX45GN. Rev D. September 2021. CGN. 2021/67208.

132. *Station Black Out (SBO) in Shutdown Condition.* GHX00600026DRAF02GN. Rev D. December 2020. CGN. 2020/322716.

133. *Total Loss of Cooling Chain (TLOCC) with Reactor Coolant Pump Sealing Leakage (State A).* GHX00600119DRAF02GN. Rev D. December 2020. CGN. 2020/322715.

134. *DEL Safety Chilled Water System Design Manual Chapter 4 System and Component Design*. GHX17DEL004DCNT45GN. Rev D. September 2021. 2021/67024.

135. *Station Black Out (SBO) (State A).* GHX00600025DRAF02GN. Rev D. December 2020. CGN. 2020/322720.

136. *Station Black Out (SBO) in Shutdown Condition.* GHX00600026DRAF02GN. Rev D. December 2020. CGN. 2020/322716.

137. *LJP/LJQ SBO Power Supply (SBO DG) System Design Manual Chapter 3 System Functions and Design Bases.* GHX17LJP003DEDQ45GN. Rev A. August 2020. CGN. 2020/257040.

138. *Strategy of Electrical Power System EMIT.* GHX05000027DEDQ45GN. Rev C. 15 March 2021. CGN. 2021/22361.

139. *UK HPR1000 – ONR396 Fault Studies Confirmatory Analysis – D2.2.03 Phase 2 Technical Report Station Black Out.* Rev 1. March 2021. GRS. 2021/30127.

140. ATWS by Rods Failure - Loss of Feedwater (State A*). GHX00600078DRAF02GN.* Rev C. November 2019. CGN. 2019/352850.

141. *ATWS by Rods Failure – Loss of Offsite Power (State A).* GHX00600031DRAF02GN. Rev C. November 2019. CGN. 2019/352694.

142. *UK HPR1000 – ONR396 Fault Studies Confirmatory Analysis – D2.2.06 Phase 2 Technical Report ATWS Analysis.* Rev 1. March 2021. 2021/30130.

143. *DNBR Design limit.* GHX00100001DRRG03GN. Rev H. August 2020. CGN. 2020/232820.

144. *SB-LOCA with Total Loss of Medium Head Safety Injection (MHSI) (State A).* GHX00600097DRAF02GN. Rev E. July 2021. CGN. 2021/58176.

145. *VDA Atmospheric Steam Dump System Design manual – Chapter 6 System Operation and Maintenance.* GDA-REC-CGN-002909. Rev B. October 2018. CGN. 2018/318471.

146. *Step 4 Assessment of Radiological Protection for the UK HPR1000 Reactor*. ONR-NR-AR-21-022. 2021/52054.

147. *Step 4 Assessment of Radioactive Waste Management for the UK HPR1000 Reactor.* ONR-NR-AR-21-023. 2021/60031.

148. *Loss of One PTR [FPCTS] Train (State A\B\C\D).* GHX00600116DRAF02GN. Rev E. January 2021. CGN. 2021/8874.

149. *Loss of One PTR [FPCTS] Train (State E\F).* GHX00600118DRAF02GN. Rev D. January 2021. CGN. 2021/8875.

150. *Loss of Three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) trains (State A to F).* GHX00600250DRAF02GN. Rev C. January 2021. CGN. 2021/8876.

151. *Station Black Out (SBO) for Spent Fuel Pool (States A to F).* GHX00600117DRAF02GN. Rev D. November 2019. CGN. 2019/355696.

152. *Step 4 Assessment of Civil Engineering for the UK HPR1000 Reactor.* ONR-NR-AR-21-018. 2021/57205.

153. *ONR-NR-CR-20-433 - UK HPR1000 - Generic Safety Assessment - Fault Studies Level 4 Updates to PIE identification documents*. 3 September 2020. 2020/272860.

154. *Non isolable Small Break or Isolable RIS [SIS] Break*. GHX00600125DRAF02GN. Rev C. November 2019. CGN. 2019/352817.

155. *Isolable piping failure on a system connected to the spent fuel pool.* GHX00600079DRAF02GN. Rev F. July 2021. CGN. 2021/52102.

156. *Modification on ASP [SPHRS] Makeup to the SFP*. HPR-GDA-LETT-0074. October 2020. 2020/304366.

157. *Summary of Fuel Route Safety Case in BFX.* GHX30000001DNBZ00GN. Rev B. May 2021. CGN. 2021/43562.

158. *PIE Grouping and Bounding Analysis for the PIE of Internal Event (Except for Loss of Support System).* GHX00100007DRAF03GN. Rev. F. January 2021. 2021/2758.

159. *On-site Radiological Consequence Evaluation for Fuel Route PIE.* GHX00530035DNFP02GN. Rev B. January 2021. CGN. 2021/2105.

160. *Worker dose assessment for representative Design Basis Accidents.* GHX00100036DNFP03N. Rev E. January 2021. CGN. 2021/28198.

161. *On-site (MCR) radiological consequences Analysis for Representative DBC Accidents of UK HPR1000*. GHX001000010DOHB00GN. Rev C. Mach 2021. CGN. 2021/28193.

162. *Off-site radiological consequence analysis for fuel route PIE.* GHX00530002DOHB00GN. Rev A. April 2021. CGN. 2021/37816.

163. *Hazards Identification and Consequence Assessment of Fuel Handling Operations.* GHX00100009DPFJ45GN. Revision D. November 2020. 2020/315907.

164. *Classification of the Typical Cranes*. GHX45600013DPZS45GN. Rev D. January 2021. CGN. 2021/8446.

165. *Dropping of a fuel assembly*. GHX00600131DRAF02GN. Rev F. March 2021. CGN. 2021/28195.

166. *PSA Data Analysis Report*. GHX0065001DOZJ02GN. Rev F. January 2020. CGN. 2020/1414.

167. *U.S.NRC, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*. NUREG/CR-6928, 2015.

168. *Failure Rate and Event Data for use within Risk Assessments*. HSE. June 2017.

169. *DEC-A Radiological Consequence Analysis.* GHX00100008DOHB00GN. Rev A. June 2020. CGN. 2020/195900.

170. *Off-site Radiological Consequences Analysis Methodology for DBC Accidents of UK HPR1000.* GHX00540004DOHB00GN. Rev A. July 2020. CGN. 2020/226067.

171. *UK HPR1000 Radiological Consequence Assessment Note.* 2021/71620.

172. *NRPB, A Methodology for Assessing Doses from Short-term Planned Discharges to the Atmosphere*. NRPB-W54, March 2004.

173. *Worker Dose Assessment methodology for Design basis Accidents.* GHX00100036DNFP03GN. Rev E. January 2021. CGN. 2020/7676.

174. *ALARP Demonstration Report of Fault Studies.* GHX00100055KPGB03GN. Rev E. August 2021. CGN. 2021/59190.

175. *Suitability Analysis of Codes and Standards in Fault Studies.* GHX00800008DRAF02GN. Rev B. December 2019. CGN. 2019/376583.

176. *Supporting Report on No Fuel Failure for Frequent Faults.* GHX00600274DRAF02GN. Rev D. March 2021. CGN. 2021/28191.

177. *UK HPR1000 Master Document Submission List*. 2021/79537.

178. *Evaluation of Passive Single Failures.* GHX00600267DRAF02GN. Rev C. March 2020. CGN. 2020/99039.

179. *Small Break – Loss of Coolant Accident (State A).* GHX00100043DRAF03GN. Rev C. August 2021. CGN. 2021/63479.

180. *Chapter 12 Design Basis Condition Analysis.* HPR/GDA/PCSR/0012@002. Draft1. June 2021. GNSL. 2021/48480.

181. *Chapter 13 Design Extension Conditions and Severe Accident Analysis.* HPR/GDA/PCSR/0013@002. Draft1. June 20201. GNSL. 2021/48479.

182. *Decay Heat Report.* GHX00100047DRAF03GN. Rev B. November 2019. CGN. 2019/355865.

183. *The Delivery of UK HPR1000 GDA Modification – Category 2 "Modifications of the BFX to Adopt Gantry Crane for Fuel Handling (M94-GHTCN00203-A).* June 2021. GNSL. 2021/44825.

184. *PIE Grouping and Bounding Analysis for the PIE of Internal Event (Radioactive Waste Management Related).* GHX00200001DNFF02GN. Rev E. 24 May 2021. CGN. CM9 Ref. 2021/39980

185. *On-site Radiological Consequence Evaluation for Waste Route PIE.* GHX00530036DNFP02GN. Rev D. 31 January 2021. CGN. CM9 Ref. 2021/8881

186. *Off-site Radiological Consequences Evaluation for Waste Route PIE*. GHX00530001DOHB00GN. Rev C. 22 January 2021. CGN. CM9 Ref. 2021/6756

Table 3: List of Design Basis Conditions

	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
DBC-2 Conditions			
1	Decrease in Boron Concentration in Reactor Coolant due to Malfunction of RCV [CVCS], REA [RBWMS] and TEP[CSTS]	A/B/C	FF
2	RCCA misalignment up to Rod Drop	A	FF
3	Uncontrolled RCCA Bank Withdrawal at Power	A	FF
4	Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition	A/B/C	FF
5	Spurious reactor Trip	A/B/C	FF
6	Turbine Trip	A/B	FF
7	Loss of Normal Feedwater Flow	A/B	FF
8	Excessive Increase in Secondary Steam Flow	A/B	FF
9	Inadvertent Opening of a Pressuriser Safety Valve	A	FF
10	Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction	A/B	FF
11	Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction	A/B/C/D/E	FF
12	Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump	A/B/C	FF
13	Spurious Pressuriser Heater Operation	A/B/C	FF
14	Spurious Pressuriser Spray Operation	A/B/C	FF
15	Loss of One PTR [FPCTS] train	A/B/C/D	FF
16	Increase in Feedwater Flow due to Feedwater System Malfunctions	A/B	FF

	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
17	Startup of One Inactive Reactor Coolant Pump at an Improper Temperature	C/D/E	FF
18	Short Term Loop of 2 Hours Duration	A/B/C/D/E	FF
19	Inadvertent Opening of One SG Relief train or of One Safety Valve	A/B	FF
20	Loss of One RIS [SIS] Train in RHR Mode	C/D/E	FF
21	Loss of RRI [CCWS] or SEC [ESWS] Train A	A/B	FF
DBC-3 Conditions			
1	Rupture of a Line Carrying Primary Coolant outside Containment	A/B/C/D/E	IFF
2	Inadvertent Core Loading of Fuel Assemblies	A/B/C/D/E	IFF
3	Uncontrolled Single RCCA Withdrawal	A/B/C	FF
4	Inadvertent Closure of One or All Main Steam Isolation Valves	A/B	FF
5	Feedwater System Piping Small Break Including Breaks in Connecting Lines to SG	A/B	FF
6	Reduction in Feedwater Temperature due to Feedwater System Malfunctions	A/B	IFF
7	Steam System Piping Small Break Including Breaks in Connecting Lines	A/B	FF
8	Uncontrolled RCP [RCS] Level Drop	C/D/E	FF
9	SG Tube Rupture (One Tube)	A/B/C	FF
10	Small Break - Loss of Coolant Accident	A	FF
11	Forced Reduction in Reactor Coolant Flow (3 Pumps)	A/B/C	FF
12	Loss of One PTR [FPCTS] Train	E/F	FF
13	Isolatable Piping Failure on a System Connected to Spent Fuel Pool	A/B/C/D/E/F	FF

	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
14	Medium Term LOOP of 24 Hours Duration	A/B/C/D/E/F	FF
15	LOOP (>2 hours) Affecting Fuel Pool Cooling	A/B/C/D/E/F	FF
16	Inadvertent Opening of One Pressuriser Safety Valve	B/C	IFF
17	Volume Control Tank Break	A/B/C/D/E/F	IF
18	Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinet Rooms of Safeguard Building Division B	A/B	FF
19	Loss of RRI [CCWS] or SEC [ESWS] Train A	C/D/E	FF
DBC-4 Conditions			
1	Dropping of Spent Fuel Cask	A/B/C/D/E/F	IFF
2	Spectrum of RCCA Ejection Accident	A/B	IFF
3	Steam System Piping Large Break	A/B	IFF
4	Intermediate Break and up to Surge Line Break - Loss of Coolant Accident	A/B	IFF
5	Small Break - Loss of Coolant Accident	B	IFF
6	Small Break - Loss of Coolant Accident	C/D/E	IFF
7	SG Tube Rupture (Two Tubes in One SG)	A/B/C	IFF
8	RHR System Piping Break inside or outside Containment	C/D/E	IFF
9	Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break	A/B/C	IFF
10	Long Term LOOP of 168 Hours Duration	A/B/C/D/E/F	IFF
11	Dropping of Fuel Assembly	A/B/C/D/E/F	IFF
12	Non-Isolable Small Break or Isolable RIS [SIS] Break Affecting Fuel Pool Cooling	E	IFF
13	Feedwater System Piping Large Break Including Breaks in	A/B	IFF

	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
	Connecting Lines to SG		
14	Inadvertent Opening of Severe Accident Dedicated Valves (One Train)	A/B/C	IFF
15	Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinet Rooms of safeguard Building Division B	C	IFF

Table 4: List of DEC-A events

	Event Description	Safety Analysis States
1	Total Loss of Feedwater (TLOFW)	A
2	Small Break - Loss of Coolant Accident (SB-LOCA) with Failure of Medium Pressure Rapid Cooldown (MCD)	A
3	SB-LOCA with Total Loss of Low Head Safety Injection (LHSI)	A
4	SB-LOCA with Total Loss of LHSI (Shutdown Condition)	C/D
5	Loss of Residual Heat Removal (RHR) or Failure of Recovery of RHR after Loss of Offsite Power (LOOP)	C/D
6	Station Black Out (SBO)	A/B/C/D/E/F
7	Anticipated Transient Without Scram (ATWS) Due to Protection System (RPS [PS]) Failure	A
8	Anticipated Transient Without Scram (ATWS) Due to Failure of RCCA to insert, including: • LOOP • SB-LOCA • Loss of Main Feedwater • Excessive Increase in Secondary Steam Flow • Spurious Pressuriser Spraying • Steam Line Break Downstream of MSIV	A
9	SB-LOCA with Total Loss of Medium Head Safety Injection (MHSI)	A
10	Total Loss of Cooling Chain (TLOCC) with Reactor Coolant Pump Sealing Leakage	A
11	TLOCC (Shutdown Condition)	C/D
12	Loss of Three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) Trains	A/B/C/D/E/F
13	Loss of Ultimate Heat Sink (LUHS) for 100 Hours	A/B
14	Uncontrolled Primary Water Level Drop without Safety Injection (SI) Signal from RPS [PS]	C/D

	Event Description	Safety Analysis States
15	Multiple Steam Generator Tubes Rupture (SGTR) (10 tubes)	A
16	Main Steam Line Break (MSLB) with SGTR (1 tube) in the Affected Steam Generator (SG)	A
17	SGTR (1 tube) with Atmospheric Steam Dump System (VDA [ASDS]) Stuck Open in the Affected SG	A
18	TLOCC with Loss of Secondary Cooldown (failure of Emergency Feedwater System (ASG [EFWS] or VDA [ASDS])	A

Table 5: List of Specific Studies

	Event Description	Safety Analysis States
Spurious C&I actuation with RPS [PS] and SAS unavailable		
1	Spurious actuation of one or more ASG [EFWS] trains	A/B
2	Spurious actuation of one or more ASP[SPHRS] trains	A/B/C/D/E/F
3	Spurious actuation of the GCT [TBS] MCD function and RIS [SIS] injection function with large miniflow line closed	A/B
4	Spurious opening of one or more VDA [ASDS] trains	A/B/C/D/E/F
5	Spurious isolation of all main feedwater	A/B
6	Spurious isolation of all RHR trains	C/D/E/F
7	Spurious isolation of one or more steam lines	A/B
8	Spurious shutdown of all the reactor coolant pumps	A/B/C
9	Spurious isolation of RCV [CVCS] letdown due to isolation of the containment at stage A	A/B/C/D/E/F
10	Spurious actuation of one or more MHSI trains with large miniflow line closed	B
11	Spurious actuation of one or more MHSI trains with large miniflow line open	C/D/E/F
12	Spurious opening of one PSV	C/D/E/F
13	Spurious opening of the letdown line or isolation of the charging line of RCV [CVCS]	A/B/C/D/E/F
14	Spurious start-up of all the pressuriser heaters	A/B/C/D/E/F
15	Spurious opening of the pressuriser auxiliary spray line	A/B/C/D/E/F
16	Spurious isolation of one or more PTR [FPCTS] cooling trains	A/B/C/D/E/F
17	Total loss of RRI [CCWS] due to a certain spurious actuation	A/B/C/D/E/F
Loss of support systems		
18	Loss of Two RRI [CCWS] or SEC [ESWS] Trains	A/B/C/D/E/F

	Event Description	Safety Analysis States
19	Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room	C
Other		
20	Double-ended Guillotine Failure of Largest RCS Pipe	A
21	Main Steam Line Large Break	A/B

Table 6: Definition of Safety Analysis Domain

Normal Operating Modes	Standard operating conditions	RCP [RCS] state	Reactor coolant inventory	RCP[RCS] pumps in operation	RCP [RCS] average temperature (°C)	RCP [RCS] pressure (bar abs)	RCP [RCS] boron concentration	Rods	Detailed Operating States for PIE identification	Safety Analysis states for DBC Analysis
Reactor in power (RP)	Reactor in power	Closed	Pressuriser level at setpoint	3	295≤T≤307	155	Critical boron concentration	Shutdown banks extracted Control banks auto or manual	1	A
	Hot standby	Closed	Pressuriser level at setpoint	3	295	155	Critical boron concentration	Shutdown banks extracted Control banks manual	2	
Normal shutdown with steam generators (NS/SG)	Hot shutdown	Closed	Pressuriser level at setpoint	3	295	155	≥ boron concentration of hot shutdown	Shutdown banks extracted Other rods inserted	3	
	Intermediate shutdown with NS/SG connection conditions	Closed	Pressuriser level at setpoint	3	≤295	130≤P<155	≥ boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	4	
	Intermediate shutdown with NS/SG connection conditions	Closed	Pressuriser level at setpoint	3	T>135 and 32≤P≤130 and T>140 and P≤32		≥ boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	5	B
	Intermediate shutdown with RIS-RHR conditions	Closed	Pressuriser level at setpoint	3	135≤T≤140	24≤P≤32	≥ boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	6	

Normal Operating Modes	Standard operating conditions	RCP [RCS] state	Reactor coolant inventory	RCP[RCS] pumps in operation	RCP [RCS] average temperature (°C)	RCP [RCS] pressure (bar abs)	RCP [RCS] boron concentration	Rods	Detailed Operating States for PIE identification	Safety Analysis states for DBC Analysis
Normal shutdown with RIS-RHR (NS/RIS-RHR)	Intermediate shutdown with RIS-RHR	Closed	PZR level at setpoint or full	≥1	100≤T≤140	24≤P≤32	≥ boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	7	C
		Closed		≥1	10≤T<100	24≤P≤32	≥ boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted P< 5bar abs All rods inserted	8	
		Closed		≥0	10≤T≤60	P≤32	≥ boron concentration of refuelling		9	
	Normal cold shutdown for maintenance (RCP [RCS] pressurisable)	Non-closed and pressurisable	≥ ¾ loop level	0	10≤T≤60	P≤32	≥ boron concentration of refuelling	All rods inserted	10	
Maintenance cold shutdown (MCS)	Normal cold shutdown for maintenance (RCP [RCS] not pressurisable)	Non-closed and not pressurisable, reactor cavity non fillable	≥ ¾ loop level	0	10≤T≤60	Atmospheric pressure	≥ boron concentration of refuelling	All rods inserted	11	
		Non-closed and not pressurisable, reactor cavity fillable							12	D
Refuelling cold shutdown (RCS)	Normal cold shutdown for refuelling		Reactor cavity flooded	0	10≤T≤60	Atmospheric pressure	≥ boron concentration of refuelling	All rods inserted	13	E
Reactor completely discharged (RCD)	Core totally unloaded	-	-	-	-	-	-	-	14	F

Annex 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No	SAP Title	Description
SC.3	Lifecycle aspects	For each lifecycle stage, control of the hazard should be demonstrated by a valid safety case that takes into account the implications from previous stages and for future stages.
SC.4	Safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
SC.5	Optimism, uncertainty and conservatism	Safety cases should identify areas of optimism and uncertainty, together with their significance, in addition to strengths and any claimed conservatism.
EKP.1	Inherent safety	The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.
EKP.2	Fault tolerance	The sensitivity of the facility to potential faults should be minimised.
EKP.3	Defence in depth	Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.
EKP.4	Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.
EKP.5	Safety measures	Safety measures should be identified to deliver the required safety function(s).
ECS.1	Safety Categorisation	The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regards to safety.
ECS.2	Safety classification of structures, systems and components	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety.
EDR.3	Common cause failure	Common cause failure (CCF) should be addressed explicitly where a

SAP No	SAP Title	Description
		structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.
EDR.4	Single failure criterion	During any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.
ESS.1	Provision of safety systems	All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined stable, safe state.
ESS.2	Safety system specification	The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and reliability requirements should be specified.
ESS.4	Adequacy of initiating variables	The variables used to initiate a safety system action should be identified and shown to be suitable and sufficient for the system to achieve its safety function(s).
ESS.8	Automatic initiation	For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).
ESS.11	Demonstration of adequacy	The adequacy of the system design to achieve its specified functions and reliabilities should be demonstrated for each safety system.
ESS.22	Avoidance of spurious actuation	Spurious actuation of safety systems should be avoided by means such as the provision of multiple independent divisions within the design architecture and majority voting.
ESS.23	Allowance for unavailability of equipment	In determining the safety systems to be provided, allowance should be made for the potential unavailability of equipment.
FA.1	Design basis analysis, PSA and severe accident analysis	Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP.
FA.2	Identification of initiating faults	Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.

SAP No	SAP Title	Description
FA.3	Fault sequences	Fault sequences should be developed from the initiating faults and their potential consequences analysed.
FA.5	Initiating faults	The safety case should list all initiating faults that are included within the design basis analysis of the facility.
FA.6	Fault sequences	For each initiating fault within the design basis, the relevant design basis fault sequences should be identified.
FA.7	Consequences	Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.
FA.8	Linking of initiating faults, fault sequences and safety measures	DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures.
FA.9	Further use of DBA	DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.
AV.1	Theoretical models	Theoretical models should adequately represent the facility and site.
AV.2	Calculation methods	Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place.
AV.3	Use of data	The data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.
AV.4	Computer models	Computer models and datasets used in support of the safety analysis should be developed, maintained and applied in accordance with quality management procedures.
AV.5	Documentation	Documentation should be provided to facilitate review of the adequacy of the analytical models and data.
AV.6	Sensitivity studies	Studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.

SAP No	SAP Title	Description
NT.1	Assessment against targets	Safety cases should be assessed against the SAPs numerical targets for normal operational, design basis fault and radiological accident risks to people on and off the site.

Annex 2

Assessment Findings

Note: These Assessment Findings must be read in the context of the sections of the report listed in this table, where further detail is provided regarding the matters that led to the findings being raised.

Number	Assessment Finding	Report Section
AF-UKHPR1000-0025	The licensee shall, as part of detailed design, incorporate the specific studies undertaken into the design basis conditions and design extension conditions, supported by appropriate analysis.	4.2.2
AF-UKHPR1000-0028	The licensee shall, as part of detailed design, identify and categorise the safety functions claimed to prevent turbine overspeed and classify the relevant structures, systems and components that deliver those functions.	4.2.2.1
AF-UKHPR1000-0032	The licensee shall, as part of detailed design demonstrate that the high neutron flux (source range) trip setting can protect against homogeneous boron dilution faults from shutdown conditions at the start of cycle.	4.3.4.2
AF-UKHPR1000-0039	The licensee shall, as part of detailed design, demonstrate that the source range, intermediate range and power range detectors can be considered as diverse and that the risks of common cause failures are reduced to as low as reasonably practicable.	4.3.4.2
AF-UKHPR1000-0050	The licensee shall, as part of detailed design, justify whether it is reasonably practicable to provide automatic isolation of the boron dilution source via the nuclear sampling system boron concentration signal to prevent a return to criticality in the event of a homogeneous boron dilution fault at cold shutdown with a failure of the reactor protection system.	4.3.4.2

Number	Assessment Finding	Report Section
AF-UKHPR1000-0083	The licensee shall, as part of detailed design, demonstrate that the safety functions of the filtering system, containment heat removal system, and safety injection system can be met, and that adequate heat removal from the core is achieved in the “zero fibre” approach. This should include, but not be limited to: ■ A calculation of a more realistic debris source term. ■ An optimisation of the in-containment water storage tank filtration system dependent on the potential debris. ■ A demonstration that all cable tray wrapping has been removed from the zone of influence for all high energy pipe failures. ■ Details of appropriate testing to verify that the design is optimised. ■ A demonstration against safety criteria that the safety functions of the safety systems can be met.	4.3.5.5
AF-UKHPR1000-0157	The licensee shall, as part of detailed design, justify the frequency of spurious control and instrumentation faults, justify the analysis methods and criteria, and demonstrate that these criteria can be satisfied. This should be either by analysis or comparison to other analysis.	4.3.8
AF-UKHPR1000-0158	The licensee shall justify the frequency of boron dilution events following a loss of reactor coolant pumps and ensure that these faults are addressed within the safety case irrespective of whether they are within the design basis or not.	4.3.9.1
AF-UKHPR1000-0213	The licensee shall, as part of the development of operational procedures, demonstrate that the procedure to clear the safety injection system pipeline of an unborated slug of water is adequate to support the FC1 reactor coolant pump start-up function.	4.3.9.1
AF-UKHPR1000-0236	The licensee shall justify the LOCUST and computational fluid dynamics analysis of heterogeneous boron dilution scenarios. This should include, but not be limited to: ■ Appropriate Phenomena Identification and Ranking Table (PIRT) analysis referenced to relevant acceptance criteria. ■ Justification of the validity of the models used. ■ Validation against test data. ■ Sensitivity studies of outputs to plant conditions and uncertainties in the prediction of residual slug sizes.	4.3.9.2

Number	Assessment Finding	Report Section
AF-UKHPR1000-0237	The licensee shall, as part of detailed design, demonstrate that the maintenance schedule for the station black-out diesel generators is consistent with the safety analysis for relevant faults and resolves the shortfalls identified in GDA.	4.4.1.3
AF-UKHPR1000-0238	The licensee shall justify the choice of reactivity coefficients, uncertainties for radial power distributions and criteria for departure from nucleate boiling used within the analysis of anticipated transient without scram events.	4.4.2
AF-UKHPR1000-0239	The licensee shall, as part of detailed design, justify the frequency of dropped load faults within the fuel route, identify and classify the structures, systems and components which are claimed for these faults and present a comparison against appropriate radiological targets to demonstrate that the risks are reduced to ALARP. The radiological consequences should be evaluated based on a justified amount of fuel damage.	4.5.2.1
AF-UKHPR1000-0240	The licensee shall define and use appropriate terms for the identification of postulated initiating events, design basis conditions and fault analysis, which characterise the operating conditions and configurations for non-reactor plant (including, but not limited to the radioactive waste management systems and relevant plant auxiliary systems). This should include those systems whose operation, conditions and configurations have no direct relationship with those defined for the reactor.	4.6
AF-UKHPR1000-0241	The licensee shall, as part of the site-specific radiological consequence analysis for design basis analysis, justify the underpinning assumptions used. This should include, but not be limited to, the shortfalls identified in GDA regarding: ■ Conservative weather conditions. ■ Conservative deposition velocities. ■ Age-specific groundshine and immersion dose conversion factors. ■ Rainfall rates that are typical for UK weather as well as no rain at all. ■ Use of conservatism in the source term, notably in relation to iodine radionuclides. ■ The omissions of radionuclides from the source term.	4.7.2

Number	Assessment Finding	Report Section
AF-UKHPR1000-0242	The licensee shall provide sufficient evidence to demonstrate that the uncertainties of the LOCUST code are understood and have been accounted for within the relevant transient analysis.	Appendix 1
AF-UKHPR1000-0243	The licensee shall provide sufficient evidence to demonstrate that the uncertainties of the GINKGO code are understood and have been accounted for within the relevant transient analysis.	Appendix 1

Appendix 1

Assessment of computer codes used for the transient analysis of DBCs and DEC-A events

INTRODUCTION

902. This Appendix provides additional detail of my assessment of the principal codes used within the safety analysis (LOCUST, GINKGO and CATALPA). These codes have not been used for the licensing activities for the Fangchenggang reference plant and have not previously been used outside of China. Gaining confidence in these codes through regulatory assessment has therefore been a crucial outcome of the Fault Studies assessment during GDA.

903. For each code the RP has submitted a Qualification Report and a Verification and Validation (V&V) Report. The Qualification Reports (Refs. A1 to A3) give a summary of the code and validation evidence and justify its applicability to the UK HPR1000. The V&V documents (Refs. A4 to A6) provide the majority of the validation evidence and were provided during Step 4 and these need to be read with an understanding of the methods described within the transient analysis reports (which I have discussed in Section 4.2 and 4.3 of this report).

904. The codes PINE, COCO, POPLAR, LINDEN, BIRCH and PALM are also used as part of the reactor transient analysis and the assessment of these is recorded in ONR's Fuel and Core Assessment Report (Ref. A7). The sub-compartment code CAMPHOR, used for pressure and temperature calculations within compartments following a high energy pipe break, is discussed within the Internal Hazards report (Ref. A8).

905. The codes used in the UK HPR1000 safety case are new codes and as such it would be unreasonable of me to expect the same amount of validation and verification evidence as is available for established codes with many years of use and a wider user base. I do however expect that the development of these codes and the underpinning validation evidence will continue after GDA in support of activities in China and potential UK safety cases.

906. During the course of GDA, I have therefore sought to understand the methods and models used in the transient analysis and gain confidence that they are likely to give conservative results for the transients being assessed. I have not undertaken a detailed examination of the evidence provided for verification and validation, instead my reviews have focused on the strategy for verification and validation, the scope and extent of the evidence, the justification of the limits of application of the codes and how the RP has accounted for the major uncertainties within the codes within the safety analysis.

907. The majority of the validation evidence was provided during Step 4. To aid my assessment of the adequacy of these codes code I commissioned a TSC to undertake a review of the Qualification Reports and the Validation and Verification Reports against the expectations of the AV SAPs (Ref. A9) and NS-TAST-GD-042 (Ref. A10).

908. The reviews undertaken by my TSC are reported in Refs A11 to A13. My assessment has also been informed by the insights provided by the independent confirmatory analysis undertaken by another TSC(and discussed in relevant parts of Section 4 of this report).

909. The principal expectations for assessment of codes are described in ONR's SAPs AV.1 to AV.8 (Ref. A9) for the assurance of validity of data and models.

- AV.1 to AV.3 are principles related to Theoretical models, calculation methods and the use of data and form the main principles that I have applied during my assessment.
- AV.4 relates to quality management procedures.
- AV.5 sets general expectations on the information that should be provided to facility review of the analytical models and data.
- AV.6 sets the expectation that studies should be carried out to determine the sensitivity of the analysis to the assumptions made, the data used and the methods of calculation.
- AV.7 and AV.8 relate to the collection of data through life and periodic update of the safety analysis and as such are not relevant to my assessment during GDA.

910. Further guidance on the expected content of a validation report is provided in NS-TAST-GD-042 on the validation of computer codes and calculation methods (Ref. A10). In particular, Section 5.2 of Ref. A10 outlines good practice for the content of a validation report and expands upon the broad expectations outlined in SAP AV.5.

911. NS-TAST-GD-042 (para 38) sets a general expectation for the validation report and the treatment of uncertainties:

- "The validation report should identify the shortcomings in the computer code method of solution, the uncertainties of the associated physics models and the inaccuracy of the experimental data used in the validation work. This information should be used to define the sensitivity analyses to be performed as part of the safety case. The object of such analyses is to confirm and demonstrate that "cliff-edge effects" do not exist. The sensitivity analyses should cover the uncertainties/approximations in the mathematical models, input data and boundary conditions of the analysis."

912. Similar guidance is given within IAEA SSG-2(Ref. A14)..

913. In the section below I give an overview of LOCUST, GINGKO and CATALPA in turn and my assessment of the details of the physical models, numerical methods and correlations used, and the RP's demonstration of the limits of applicability (following the structure of Section 5.2 of NS-TAST-GD-042, Ref. A10). Given the wide range of application of LOCUST and GINKGO in the safety analysis I have focussed the majority of my assessment attention on these two codes. I have then given a general view on user proficiency and quality assurance arrangements as these aspects are common to all codes.

ASSESSMENT

914. The RP's strategy for the verification and validation of the codes is given in Section 4 of Refs A4 to A6.

- Verification is to ensure that the code is built correctly by checking that it meets the design specifications, by comparing coding to algorithms and equations and by comparing calculations against analytical solutions and manufactured solutions. Verification of the model has been performed by using phenomenological problems. These types of problems are used to demonstrate that the equations have been correctly coded.
- The validation of based on a number of Separate Effects Tests (SETs), Integral Effects Tests (IETs) or plant transients. The validation of the code can be divided into the validation of a single code model and the validation of the whole code models/The individual code models are validated against SETs in full size or scale test facilities, while the overall assessment is based on IETs.

915. I am content that this is an appropriate strategy and consistent with standard practice for assessing the verification and validation of analytical codes.

916. In my opinion the discussion of the SETs and IETs within the validation reports (A4 to A6) is, in general, brief and without full discussion and explanation of the results. The conclusions are limited to whether the code can predict the main phenomena with reasonable agreement. There is little discussion of any observed discrepancies or biases. Furthermore, there is little explanation of the reasoning for the modelling choices (such nodalisation, time steps or correlation options) that have been made or what impact varying such choices might make to the calculation results. As such, it is not possible for a reader of the V&V report to understand *in detail* the validation base or how any uncertainties in the code affect the outputs.

917. I have discussed this with the RP and through these discussions I have established that there is a significant amount of additional evidence within CGN to support the findings of Refs A4 to A6. Tables have been added to the latest revisions of the validation reports which contain the titles of a significant number of calculation notes; these provide the supporting additional detail to that summarised in the V&V reports. It has not been possible to examine these supporting documents during GDA but I have gained confidence that the conclusions within Refs A4 to A6 are supported by a more detailed analysis of the results.

LOCUST

General Aspects

918. LOCUST is a thermal hydraulics system analysis code that is used in the UK HPR1000 safety case to analyse design basis and DEC-A events. The RP has developed this code since 2015 and a qualification report (Ref. A1) and a V&V report (Ref. A4) has been submitted as part of the UK HPR1000 safety case to demonstrate the capability of LOCUST to perform the transient analysis for UK HPR1000. Two versions of LOCUST have developed:

- one is LOCUST using realistic models for SGTR, FLB and DEC-A analysis;
- the other is LOCUST-K containing conservative models for LOCA analysis according to the requirements of US NRC 10 CFR 50 Appendix K.

919. The validation report (Ref. A4) presents the theoretical models and equations for LOCUST and has a separate section describing how these are modified for LOCUST-K. In discussion with the RP I established that LOCUST-K has two different options LOCUST-K-SB and LOCUST-K-LB (used for SB/IB-LOCA and LB-LOCA respectively). These options have slightly different sub-models activated, reflecting some different phenomena between SB/IB-LOCA and LB-LOCA.

920. The details of these options have been described in the response to RQ-UKHPR1000-1579 (Ref. A15). The validation report does not include this information nor any specific validation for these options. However, I am content that this is a Minor Shortfall as these options represent the choices that users have to make when using the codes rather than being variations to the LOCUST code.

921. The RP has considered the approaches described within IAEA SSG-2 (Ref. A14, Table 1) and describes the models as follows:

- LOCUST-K is used for design basis LOCAs and LB-LOCA and is a conservative code used with conservative assumptions on system availability and initial and boundary conditions (Option 1 from IAEA SSG-2)

- LOCUST is used for FLB and SGTR accidents and is a best estimate code used with conservative assumptions on system availability and initial and boundary conditions (Option 2 from Table 1 IAEA SSG-2).
- LOCUST is used for DEC-A events and is a best-estimate code used with best-estimate assumptions on system availability and initial and boundary conditions (Option 4 from Table 1 IAEA SSG-2).

922. I have used these descriptions to inform my expectations for the evaluation of uncertainties below.

923. The latest version of the validation report (Ref. A4) is based on LOCUST V1.1.0 and LOCUST-K V1.1.0. I have noted that some of the transient analysis has used LOCUST V1.0.2 and LOCUST-K V1.0.1 (Ref. A16). The discrepancy has arisen as the cladding deformation model for [redacted] has been added in LOCUST V1.1.0 and LOCUST-K V1.1.0 and this model is documented in Section 3.3.4 of the LOCUST V&V report along with the validation tests associated with fuel failure phenomena.

924. The RP has claimed (Ref. A17) that it has assessed the impact of the update of the updated code version on UK HPR1000 transient analysis and that the results show that the main parameters calculated using old versions are more penalizing for LOCA transients and are of little difference with the latest versions for other transients. Therefore, the code versions used in UK HPR1000 safety cases have not been updated. I am content not to progress this matter further during GDA but a future licensee will need to ensure that a fixed version of the code is used for validation and safety analysis. I consider this matter to be a minor shortfall.

Details of Physical Models, Numerical Methods and Correlations used

925. The physical models within LOCUST and LOCUST-K are described in Chapter 3 of the V&V report (Ref. 4). The main features can be summarised as follows:

- LOCUST and LOCUST-K are based on a six-equation two-phase flow model to simulate the system thermal hydraulic response. These equations represent conservation of mass, energy and momentum for separate liquid and vapour phases. Conservation equations solve six primary variables: pressure, void fraction, liquid/vapour phase specific internal energy and liquid/vapour phase velocity.
- When the calculation involves non-condensable gases and boron transport, additional mass conservation equation and boron transport equation are added to solve the non-condensable quality and boron density, and the relevant terms in six conservation equations.
- In addition to those equations, additional models are considered to predict the behaviour of reactor systems such as heat conduction (1D model), reactor coolant system, reactor kinetics, critical flow models ([redacted]), Counter-current flow limitation ([redacted]), water packing mitigation models, abrupt area change and control systems including trips.
- LOCUST-K, which is dedicated to LOCA analyses, introduces 9 models according to the requirements of Appendix K of 10 CFR 50. ONR understands that all models described for LOCUST are also applicable for LOCUST-K except if it is explicitly mentioned that this is not the case.

926. As part of the review of Ref. A4, my TSC has compared the models with those from other similar codes and advised (Ref. A11) that the code is based on well-known correlations or implemented in other system thermal-hydraulics codes. Based on the description of these models and similarity with other codes, my TSC advised that the codes should be capable of simulating the relevant system thermal-hydraulic

phenomena expected during design basis accidents and design extension conditions. Given this and from my own review I am content that the information provided in the V&V report is satisfactory and I am satisfied that LOCUST and LOCUST-K are suitable for typical steady-state or transient calculations for the generic UK HPR1000 safety case, consistent with the general expectations of SAPS AV.1 and AV.2.

Verification and validation

927. The validation report for LOCUST (Ref. A4) reports the results of 58 SETs and 44 IETs (from 9 test facilities). Validation matrices show the tests relevant to the main phenomena for each fault type. Examination of these tables show that there is in general good coverage but I note that there are some phenomena for which the validation relies on a single test. Whilst I am content that the range of validation evidence is sufficient for GDA, a future licensee should consider greater depth and range of validation evidence to support future operation and that this can be done as part of the ongoing development of these codes, which is normal business.

928. The RP's validation strategy (Section 4 of Refence A4) states that in the verification of the models, code-to-code comparisons would be used where no analytical solutions can be reached. However, no code-to-code comparisons were initially presented. In response to my queries on this, the RP has clarified that of the 11 verification cases, code to code comparisons have been used in 2 cases to verify LOCUST. This information is now included within Section 5 of Ref. A4. This is important verification evidence to demonstrate that the code has correctly implemented the mathematical models and I welcome the addition of this information.

Limits of Application

929. SAP AV.3 states that the data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. ONR's NS-TAST-GD-042 sets the expectation that the validation report should define the limits for application of the calculation method and indicate the dominant processes which are expected to occur in any situation to which it is applicable.

930. Within Ref. A4, the RP presents the results of a range of validation tests (both separate and integral tests) to demonstrate the validation of LOCUST/LOCUST-K for a range of conditions. Tables 4-2 to 4-5 of Ref. A4 present the validation matrix and a range of SETs and IETs have been used to evaluate the code.

931. The original submissions did not however discuss the limits of application nor confirm that they covered the range of application for the UK HPR1000 safety case. The latest version of the Validation report (Ref. A4) submitted mid-way through Step 4 of GDA now includes this discussion. Table 6-1 of Ref. A4 presents a comparison between the range of application of the code and the validation range. From examination of Table 6-1 it can be seen that for some parameters the application of LOCUST exceeds the validated range.

932. This is discussed within Section 6.1.2 (Evaluation of Verification and Validation results) of Ref. A4. Within this section, the RP claims that the application outside of the validation range is acceptable on the basis that:

- No new phenomena appear within the extended application range;
- There are no cliff edge effects within the extended application range.

933. The RP examines each transient for which LOCUST or LOCUST-K is used and considers the significance of the difference between the validated range and range of

application. In most cases, I am satisfied that the differences are small and unlikely to make a significant difference.

934. For SBO however the difference in power level between the validation cases and the application range is significant. The validation covers a range between [redacted] of full power but is used for analysis of up to 102% of full power. The RP presents the results of a limited sensitivity study to investigate the impact of core power on the main phenomena that will be relevant during an SBO. From this the RP concludes that the initial power levels have little influence on the SBO thermal-hydraulic responses and that higher power levels only impact whether the PSVs open or not. As the capability of LOCUST to simulate PSVs operation is demonstrated elsewhere in Ref. A4, the RP claims that the use of LOCUST outside of the validated power range is acceptable.

935. The addition of this sensitivity study is welcome but in my opinion is not conclusive evidence as it is not an independent means of testing the capability of the code at different power levels. In my opinion, the validation would be strengthened by either comparison against other plant or test data (if available) or by comparison against other validated codes. I do not however consider that this to be a significant shortfall and it is unlikely to affect the conclusions of the transient analysis presented in the generic UK HPR1000 safety case.

936. I am therefore satisfied that the RP has provided an adequate justification on the range of application of LOCUST and LOCUST-K and that they have been used within their limits of application.

Comparison with other calculation methods

937. The RP has also included within Ref. A4 Appendix B a short description of comparisons between the analysis of LB-LOCA, SGTR, FLB and SB-LOCA with total loss of MHSI with LOCUST and another [redacted]. Several plots are included to compare the predictions between these codes.

938. As with the discussion against test data, the comparison between LOCUST/LOCUST-K and the other code is brief and lacking in detail. I have taken confidence from these comparisons that LOCUST/LOCUST-K is able to predict the main phenomena, but a further, more comprehensive comparison against an established code would provide stronger support to the validation base.

Uncertainty of Best Estimate Calculations and Inherent calculations bias

939. The RP has previously stated that a quantification of key uncertainties is not necessary for LOCUST-K as it is a conservative code used with conservative boundary conditions. I am content to accept this position for GDA as it is line with international practice (IAEA SSG-2, Ref. A14) and have not sought further information on the uncertainties of LOCUST-K.

940. For LOCUST, which is a best-estimate code used with conservative boundary conditions, the RP has stated that conservative input parameters will generate conservative safety analysis results. Both NS-TAST-GD-006 and NS-TAST-GD-042 contain the expectation that where best-estimate codes are used with conservative initial and boundary conditions, uncertainties in key parameters and correlations need to be allowed for and substantiated in the safety case. During GDA I have therefore sought to understand the major uncertainties within LOCUST and the way in which the RP has accounted for these in the use of this code.

941. I have discussed the treatment of uncertainties with the RP and as a result additional information is included within a new Appendix A of Ref. A4. Appendix A contains three main parts. Firstly, a clear summary of the main limitations of the code. Secondly, a set

of sensitivity studies to study the effects of the code uncertainties on the transient results. Thirdly, it contains a list of supporting reports which include the code user manuals, calculation notes and methodology reports (which provide guidance for user to carry out analysis correctly and conservatively).

942. In my opinion, the summaries provided in Appendix A give confidence that the RP has undertaken a significant amount of work to underpin the claim that the analysis results used within the UK HPR1000 safety case are conservative. In particular, I note that the use of sensitivities is consistent with the expectations of SAP AV.6. However, discussion of these sensitivity studies is brief, the evidence is difficult to find within the validation report and requires knowledge of the content of the supporting documents.

943. In my opinion, there remains a shortfall against the expectation of NS-TAST-GD-042 for the analysis of uncertainties within the code. I consider that some quantification of the uncertainties may be necessary to demonstrate that the conservative assumptions are sufficient to address all of the uncertainties in the codes. A robust comparison of predictions against an established code would also strengthen the case.

944. However, I do not consider that this is necessary during GDA but I do consider that the site-specific safety case should provide more coherent arguments and visibility of evidence to evaluate the uncertainties within GINKGO and provide a robust demonstration that the assumptions made within the transient analysis are adequately bounding. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0242 – The licensee shall provide sufficient evidence to demonstrate that the uncertainties of the LOCUST code are understood and have been accounted for within the transient analysis.

Summary and conclusions for LOCUST

945. My assessment of LOCUST/LOCUST-K has concluded that they are suitable for use in the transient analysis of DBCs and DEC-A events for UK HPR1000. I have not identified any significant shortfalls that would undermine my confidence in the use of these codes for this purpose.

946. However I consider that a future licensee will need to ensure that there is a strong justification of the uncertainties to support future plant operation, consistent with the expectations of NS-TAST-GD-042 and IAEA SSG-2. I have therefore raised assessment finding AF-UKHPR1000-0424 for a future licensee to address.

GINKGO

General Aspects

947. GINKGO is a thermal hydraulics system analysis code that is used in the UK HPR1000 safety case to analyse intact circuit design basis and DEC-A events. The RP has developed this code since 2011. A qualification report (Ref. A2) and a verification and validation report (Ref. A5) has been submitted as part of the UK HPR1000 safety case to demonstrate the capability of GINKGO to perform the transient analysis. The RP describes GINKGO as having both realistic models and models with conservatism and as such is a realistic conservative code.

948. This description of GINKGO is unusual in that codes are commonly either considered as best-estimate or conservative (IAEA SSG-2, Ref. A14). ONR NS-TAST-GD-006 (Ref. A10) notes that it is increasingly relevant good practice to use computer codes which model the physical behaviour of facilities activities and transients as realistically as possible, but with conservative initial and boundary conditions. I have therefore sought confidence that either the code is inherently conservative or that the code in

combination with the initial and boundary conditions will produce conservative outcomes.

949. The validation report (Ref. A5) is based upon GINKGO V1.5.0. From a sample of the transient analysis I have noted that these have been conducted using GINKGO V1.3.6 or GINKGO V1.4.0. The RP has confirmed that these versions have been used in the transient analysis. The RP has claimed (Ref. A18) that it has assessed the impact of the updated code version on UK HPR1000 transient analysis and that the results show that the differences are insignificant. I am content not to progress this further during GDA but a licensee will need to ensure that a fixed version of the code is used for validation and safety analysis. I consider this matter to be a minor shortfall.

Details of Physical Models Used, Numerical Methods and Correlations used

950. The physical models within GINKGO are described in Chapter 3 of the V&V report. The principal assumptions of the fluid model in GINKGO are listed as follows:

- One dimensional fluid flow, assuming constant properties across the fluid channel junction.
- Single fluid flow for two-phase slip flow.
- Thermal equilibrium between vapor phase and liquid phase. Phase velocity is calculated using the [redacted] model.

951. The major code/model limitations are:

- One dimensional fluid flow.
- Two-phase thermal equilibrium hypothesis.
- Limited 2-phase conditions (e.g. low void fraction, absence of steam in combination with subcooled water).
- Flashing and condensation cannot be simulated in the fluid flow model, except in the pressuriser.
- Effect of non-condensable gasses on the fluid behaviour is not accounted for.
- Lumped models of Steam Generator and Pressuriser.

952. My TSC has compared the models with those from other similar codes and advised (Ref. A12) that the code is based on well-known correlations or implemented in other system thermal-hydraulics codes. However, compared to thermal-hydraulic system codes like MANTA[††], RELAP5[‡‡], ATHLET[§§] applied for similar purposes (i.e. safety case of non-LOCA transient) GINKGO adopts a more 'simplified' modelling approach at the level of the fluid model. In particular, GINKGO features:

- A 4-field equation model (conservation of mixture mass, mixture energy, mixture momentum and drift flux model). The slip velocity term in mixture energy and mixture momentum equations is taken into account considering a drift flux model [redacted]. The limitations of this modelling approach are that only problems where the temperature of the two phases are equal can be simulated. Given the range of application, i.e. non-LOCA transients without boiling expected in the primary circuit, my TSC has advised that this is considered acceptable.
- A [redacted] model [redacted] for the SG secondary side and Pressuriser. As a consequence, GINKGO does not allow to explicitly model the SG feedwater

[††] MANTA is a thermal-hydraulic system code developed by AREVA/FRAMATOME.

[‡‡] RELAP5 is a thermal-hydraulic system code developed by INEL, supported and owned by USNRC.

[§§] ATHLET is a thermal-hydraulic system code developed by GRS.

ring, downcomer, riser and dryers/separator, nor does it allow to model the thermal stratification or interfacial heat transfer in the pressuriser.

953. My TSC has advised (Ref. A12) that the correlations used within GINKGO are implemented in other system thermal-hydraulics codes or are based on well-known correlations. My TSC concluded that GINKGO uses models and calculation methods that are commonly used in existing system thermal-hydraulic codes and that there is reasonable confidence that the code will be fit for the analysis of DBC and DEC-A events within the UK HPR000 safety case. Given this and from my own review I am content that the information provided in the V&V report is satisfactory and I am satisfied that GINKGO are suitable for typical steady-state or transient calculations for the generic UK HPR1000 safety case, consistent with the general expectations of SAPS AV.1 and AV.2.

Verification and validation

954. The validation report for GINKGO (Ref. A5) contains 11 SETs and 11 IETs (from 9 test facilities). The Validation matrix (Table 4-2) show the tests relevant to the main phenomena for each fault type. Examination of these tables show that there is in general reasonable coverage but I note that there are some phenomena for which the validation relies on a single test. These include natural circulation, break critical flow and VDA, MSSV and MSIV behaviour. Whilst I am content that the range of validation evidence is sufficient for GDA, a licensee should consider greater depth and range of validation evidence to support future operation and that this can be done as part of the ongoing development of these codes, which is normal business.

Limits of Application

955. SAP AV.3 states that the data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. NS-TAST-GD-042 (Ref. A10) sets the expectation that the validation report should define the limits for application of the calculation method and indicate the dominant processes which are expected to occur in any situation to which it is applicable.

956. The original submission did not discuss the limits of application nor confirm that they covered the range of application for the UK HPR1000 safety case. An updated version of the Validation report (Ref. A5) submitted mid-way through Step 4 of GDA now includes this discussion. Table 6-2 of Ref. A5 presents a comparison between the range of application of the code and the validation range. From examination of Table 6-2 it can be seen that for some parameters the application of GINKGO exceeds the validated range.

957. Section 6.1.2 of Ref. A5 presents a discussion of the validation results. Within this, the RP argues that GINKGO can be applied out of the validated range if:

- the application range is within the range of parameters in the steam table, and
- there is no new phenomena, or any new phenomena are not significant to the transient under consideration.

958. The RP summarised the key phenomena in Table 6-3 and conclude that GINKGO is applicable to the transient analysis in the UK HPR1000 safety case. However, the discussion that supports this conclusion is limited and it is up to the reader of the document to consider each phenomena in turn and the transients that are of relevance to form a view. Furthermore, there is no discussion of the limits of the steam table for this use, noting that GINKGO is limited to regions where the steam and water phases have equal temperature.

959. Notwithstanding this, the RP argues that the methods and assumptions used in the generic UK HPR1000 safety case transient analysis are conservative and as such compensate for any shortcomings in the validation evidence. Taking into account my regulatory assessment of the transient analysis and the confirmatory analysis undertaken by my TSC (and described in Section 4.3 and 4.4 of this report), I am content to accept this position for GDA.

Comparison with other calculation methods

960. Appendix B has been added to the latest version of the report and this summarises [redacted] comparisons (with plots of key parameters) undertaken for a selection of transients between GINKGO [redacted] Comparisons are presented for:

- Inadvertent Closure of One or All Main Steam Isolation Valves
- Increase in RCP[RCS] Inventory due to RCV[CVCS] Malfunction
- RCCA Misalignment up to Rod Drop without Limitation
- Reactor Coolant Pump Seizure or Reactor Coolant Pump Shaft Break
- Steam System Piping Large Break

961. For each of these transients the RP concludes that the comparison shows that the transient trend calculated by GINKGO and the reference code matches well with each other. Whilst these comparisons are a welcome addition to the report and give me some additional confidence in the predictive capabilities of GINKGO as there is no discussion of the nodalisation, user defined parameters, initial conditions or key assumptions they do not add significantly to the understanding of the uncertainties of GINKGO. In my opinion a more comprehensive comparison against an established code would provide stronger support to the validation base. I have taken this into account in coming to my conclusions on uncertainties in the following sub-section.

Uncertainty of Best Estimate Calculations and Inherent calculations bias

962. I discussed the treatment of uncertainties with the RP and as a result additional information is included within a new Appendix A of Ref. A5 to address these points. Appendix A contains three main parts. Firstly an explanation of why the RP consider GINKGO a “realistic conservative” code. Secondly, a description of the conservatisms with the models and the approaches to ensure conservative results (with examples of sensitivity studies which have been conducted to inform these approaches). Thirdly, it contains a list of supporting reports which include the code user manuals, calculation notes and methodology reports (which provide guidance for user to carry out analysis correctly and conservatively).

963. I consider that Section A2 is particularly helpful in summarising the models within GINKGO. 17 out of 22 models are used with conservative model parameters set by the user (for example, the fuel to coolant HTC can be set at a maximum or minimum value (depending on the scenario being studied) to ensure that the core heat transfer model is conservative). This information is presented in the associated Table A-1 which includes the key models and simplifications, the key parameters for each model, the sources of biases and the user guidance to ensure conservative application of the code. The table also indicates the transients to which the various models are relevant.

964. To illustrate how the RP determines how these models are penalised, Section 6.2.3 of Ref. A5 gives an example of a study undertaken to determine the conservatism of the GINKGO model for Inadvertent Closure of One main Steam Isolation Valve. This study considers key parameters and compares a “worst-possible” calculation with NPP measurements with uncertainty bands. The use of sensitivity studies in this way is consistent with the expectations of AV.6. However, the discussion is again brief without

discussion of how the “best estimate” or “worst possible” parameters have been chosen. Nevertheless, this section does provide some confidence that the code can replicate experiments and provides some insight into what conservative choices should be made.

965. In my opinion, there remains a shortfall against the expectation of NS-TAST-GD-042 for the analysis of uncertainties within the code. I consider that some quantification of the uncertainties may be necessary to demonstrate that conservative assumptions applied in the safety analysis are sufficient to address all of the uncertainties in the codes. A robust comparison of predictions against an established code would also strengthen the case.

966. However, as with the LOCUST code I do not consider that this is necessary during GDA but I do consider that the safety case for operation should provide more coherent arguments and visibility of evidence to evaluate the uncertainties within GINKGO and provide a robust demonstration that the assumptions made within the transient analysis are adequately bounding. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0243 – The licensee shall provide sufficient evidence to demonstrate that the uncertainties of the GINKGO code are understood and have been accounted for within the transient analysis.

Summary and conclusions for GINKGO

967. My assessment of the validation evidence submitted for GINKGO has concluded that it is suitable for use in the transient analysis of DBCs and DEC-A events for UK HPR1000. I have not identified any major shortfalls that would undermine my confidence in the use of these codes for this purpose.

968. However I consider that a licensee will need to ensure that there is a strong justification of the validation range to support future plant operation, consistent with the expectations of NS-TAST-GD-042 and IAEA SSG-2. I have therefore raised assessment finding AF-UKHPR1000-0243 for a future licensee to address.

CATALPA

969. CATALPA is a single-volume containment thermal-hydraulic analysis code. It is used to simulate the thermal-hydraulic responses of a PWR containment under the accident conditions with mass and energy release, such as LOCA, SLB accident, etc. It is also applied to simulate transient conditions for verifying the design temperature and pressure of containment and to verify the safety systems directly associated with the maintenance of containment integrity and the design of protection setpoints (e.g. the signal for pump shutdown under high containment pressure).

970. As it is a much simpler code than LOCUST and GINKGO and it is used in a more limited way in the UK HPR1000 safety case I have not considered it necessary to conduct a detailed review of the validation evidence. Instead, my assessment of this has been limited to gaining confidence in the general methods and approaches used by this code to provide assurance in the margins shown in the containment performance criteria.

971. My TSC has advised (Ref. A13) that CATALPA is very similar in models and hypotheses to other single volume containment codes and that the models and hypotheses are well known. I am content that the CATALPA validation report meets the general expectation of NS-TAST-GD-042 for the details of physical models used, numerical methods and correlations used.

972. My TSC also advised that, whilst the RP has demonstrated within Ref. A13 the ability of CATALPA to provide an over-estimation (conservative prediction) of the pressure and temperature peaks it has not demonstrated the capability to:

- underestimate containment pressure, which is conservative for the Large break LOCA analysis (as the containment pressure influences the break flow rate)
- over-predict containment pressure and temperature evolution during the long-term phase of the accidents. This is penalising for the qualification of the equipment in the reactor building and the radiological release from the containment following a LOCA.

973. For the first of these points I have satisfied myself from Ref. A4 that the RP uses a constant conservative containment pressure for the analysis of LB-LOCA. For the second point from examination of the containment pressure and temperature analysis document the predicted results are well below the design parameters of the containment. Furthermore, the estimations of containment leakage used in the radiological consequences assessment are independent of the containment pressures. I am therefore content the matters identified by my TSC are not significant for GDA.

974. Compared to LOCUST and GINKGO, the validation and verification matrix presented in Ref. A6 for CATALPA is much less extensive, with only 4 verification cases, 2 SETs and 3 IETs. I am content that this is to be expected for this code which is simpler and has fewer complex models than the thermal hydraulic codes. The report does not however provide any justification for why the verification and validation matrix is sufficient. Whilst I consider this to be a shortfall against the expectations of international guidance (IAEA SSG-2 para 5.30) that the approach to validation should be justified, given the significant margin to the containment design pressures and temperatures I am content that this is a minor shortfall.

Users Proficiency and Quality Assurance

975. NS-TAST-GD-042 sets the expectation that the validation report should contain sufficient information to enable ONR to make a judgement on the proficiency of the code users. AV.4 sets the requirement that computer models should be developed, maintained and applied in accordance with quality management procedures. My assessment has instead been based on a review of the documents submitted by the RP (supported by my TSC) and discussions with the RP to understand the training of the users and the guidance that is used to inform modelling choices.

976. My TSC has reviewed (Ref. A19) the RP's quality assurance documentation, which they found to be in accordance with their expectations and with relevant good practice such as guidance in IAEA SSG-2. Interactions with the RP and ONR's Fuel and Core inspectors have also given me confidence that sensible procedures are in place for transferring and control of data between disciplines (use of COCO output data in fault analysis is a very important example of this.)

977. I have noted above that the validation reports do not provide any conclusions with regards to how users of the code should choose parameters to ensure conservative calculations. Sections 6 of each report describes the conservatism of the codes and provides general advice on which parameters should be pessimised for the analysis of the different faults. However, the reports do not provide any definitive advice or guidelines to allow users to ensure that the choices take account of the uncertainties or bias within the code. I anticipate that such information would be contained within guidance documents available to the users of the code. Table A-8 has been added to the latest revision of the validation documents to provide references to guidance documents which are available to codes users.

978. I have taken assurances from the RP that adequate processes are in place within CGN to ensure that the analysts are suitably qualified to perform the analysis and are supported by adequate quality management arrangements. I have not identified any concerns from my review of the proficiency of the code users that might call into question the validity of the analysis used in the generic UK HPR1000 safety case. These arrangements will however need to be reviewed and updated once the organisation of the licensee has been decided.

979. It will be for a future licensee to decide what computer codes it utilises to support its safety case and operations, and what arrangements it has to control their use and ensure their adequacy. I am confident these decisions and arrangements will be subject to appropriate ONR attention as part of routine regulatory interventions associated with licensing and permissioning.

Summary and Conclusions

980. Overall I am satisfied that the RP has demonstrated that LOCUST, GINKGO and CATALPA are appropriate for use for the analysis of DBCs and DEC-A events within the generic UK HPR1000 safety case for the purpose of GDA. I am also confident that the codes have been used in such a way to ensure conservative results have been obtained within the safety analysis, as expected by FA.7. However, I have raised two Assessment Findings for a licensee to strengthen the validation bases for these codes.

References

A1 *LOCUST - A Thermal Hydraulic System Analysis Code: Qualification Report*. CNPRIGNF1117REC010004. Rev A. March 2019. CGN. 2019/94120

A2 *GINKGO – A Transient System Analysis Code: Qualification Report.* CNPRIGNF1117REC010009. Rev A. March 2019. CGN. 2019/94142.

A3 *CATALPA – A Thermal Hydraulic Containment Analysis Code: Qualification Report.* CNPRGNF1117REC010011. Rev A. March 2019. CGN. 2019/94146

A4 *LOCUST – A thermal-hydraulic System Analysis Code: Verification and Validation Report*. GHX00600143DRAF02TR. Rev D. March 2021. CGN. 2021/28217.

A5 *GINKGO – A Transient System Analysis Code: Verification and Validation Report*. GHX0060014DRAF02TR. Rev D. March 2021. CGN. 2021/28216.

A6 *CATALPA -A Thermal-hydraulic Containment Analysis Code: Verification and Validation Report*. GHX00600139DRAF02TR. Rev B. July 2020. 2020/220293.

A7 *Step 4 Fuel and Core Assessment Report.* ONR-NR-AR-21-021. 2021/23724.

A8 *Step 4 Internal Hazards Assessment Report.* ONR-NR-AR-21-012. 2021/55302.

A9 *Safety Assessment Principles for Nuclear Facilities*. 2014 Edition, Revision 1. January 2020. http://www.onr.org.uk/saps/saps2014.pdf

A10 *Validation of Computer Codes and Calculation Methods.* NS-TAST-GD-042. Revision 5. March 2019. ONR.

A11 *LOCUST Detailed Code Review for the UK HPR1000 Safety Case on behalf of ONR*. ONRTSF/4NT/0714087/000/01. Rev 1. December 2020. Tractebel. 2021/21726.

A12 *GINKGO Detailed Code Review for the UK HPR1000 Safety Case on behalf of ONR*. ONRTSF/4NT/0713390/000/01. Rev 1. December 2020. Tractebel. 2021/21725.

A13 *CATALPA Code Review for the UK HPR1000 Safety Case on behalf of ONR*. ONRTSF4NT068503200001. Rev 1. March 2020. Tractebel. 2020/97042.

A14 *Deterministic Safety Analysis for Nuclear Power Plants.* No. SSG-2 (Rev. 1). 2019. IAEA.

A15 *UK HPR1000 – Regulatory Query (RQ) Tracking Sheet*. ONR. 2017/407871

A16 *Chapter 12 Design Basis Condition Analysis.* HPR/GDA/PCSR/0012. Rev 001. January 2020. GNSL 2020/13934. 2020/13934.

A17 – *Email GNSL to ONR. Fault Studies Level 4 Meeting on 19th April Response to supplementary code questions.* GNSL. 2021/51008.

A18 *Email GNSL to ONR. GINKGO and CATALPA code versions.* September 2021. GNSL. 2021/65476.

A19 *Code Review for the UK HPR1000 Safety Case on behalf of ONR – Software Quality Assurance.* ONRTSF/4NT/0685039/000/00. Rev 1. October 2019. Tractebel. 2019/307311.