Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Severe Accident Analysis for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-008
Revision 0
January 2022

Published 01/22

EXECUTIVE SUMMARY

This report presents the findings of my assessment of the Severe Accident Analysis 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 Severe Accident Analysis 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 GDA 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 Severe Accident Analysis information contained within the PCSR and supporting documentation.

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

- The relevant severe accident phenomena that have been identified by the RP to be considered in the severe accident analysis.
- The RP's identification of safety features which are used for severe accident management.
- The RP's methodology for identification of bounding severe accident scenarios and the final list of scenarios used in the severe accident analysis.
- The safety functions of the safety features used for severe accident management.
- The analyses which support the RP's safety claims that the severe accident safety features are effective.
- The verification and validation of the computer codes used in the severe accident analysis.
- The engineering requirements of the structures, systems and components used for severe accident management.
- The overall claims that the potential for early or large releases of radioactivity have been practically eliminated by the UK HPR1000 design.
- The RP's demonstration that relevant risks have been reduced to as low as reasonably practicable.

The conclusions from my assessment are:

- The RP has adequately identified severe accidents phenomena, severe accident scenarios and safety features used for severe accident management.
- The RP has demonstrated that the UK HPR1000 safety features for severe accident management are effective through deterministic analysis and has provided appropriate verification and validation evidence for the codes used.
- The RP has demonstrated that appropriate engineering requirements have been derived and assigned to structures, systems and components claimed for severe accident management.
- The RP has demonstrated that the UK HPR1000 supporting systems are adequate to support the safety features for severe accident management.

- The RP has demonstrated that early or large releases have been practically eliminated in the UK HPR1000 design.
- The RP's approach is aligned with both ONR and international expectations for severe accident analysis.
- For the purposes of GDA, the RP has demonstrated that the design of the UK HPR1000 has reduced the relevant risks to ALARP.

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 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 four 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 Severe Accident Analysis perspective a DAC may be granted.

LIST OF ABBREVIATIONS

AC	Alternating Current
AICC	Adiabatic Isochoric Complete Combustion
ALARP	As Low As Reasonably Practicable
ASP [SPHRS]	Secondary Passive Heat Removal System
ASTEC	Accident Source Term Evaluation Code
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
CDF	Core Damage Frequency
CFD	Computational Fluid Dynamics
CGN	China General Nuclear Power Corporation Ltd
CHF	Critical Heat Flux
COT	Core Outlet Temperature
DAC	Design Acceptance Confirmation
DC	Direct Current
DCH	Direct Containment Heating
DDT	Deflagration to Detonation Transition
DEC	Design Extension Condition
DEC-A	Design Extension Condition A
DEC-B	Design Extension Condition B
ECS	Extra Cooling System
EDE [AVS]	Annulus Ventilation System
EDG	Emergency Diesel Generator
EHR [CHRS]	Containment Heat Removal System
ERVC	External Reactor Vessel Cooling
EUF [CFES]	Containment Filtration and Exhaust System
EUH [CCGCS]	Containment Combustible Gas Control System
EUR(s)	European Utility Requirement(s)
FCG3	Fangchenggang Unit 3
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd.
GNSL	General Nuclear System Ltd.
HIC	High Integrity Component

HOW2	(ONR) Business Management System
HPME	High Pressure Melt Ejection
HRA	Human Reliability Assessment
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IB-LOCA	Intermediate Break Loss of Coolant Accident
iDAC	Interim Design Acceptance Confirmation
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
IRWST	In-containment Refuelling Water Storage Tank
IS-LOCA	Interfacing System Loss Of Coolant Accident
IVMR	In-Vessel Melt Retention
IVR	In-Vessel Retention
JAC [FWPS]	Firefighting Water Production System
KDA [SA I&C]	Severe Accident Instrumentation and Control
KDS [DAS]	Diverse Actuation System
KIT	Karlsruhe Institute of Technology
KRT [PRMS]	Plant Radiation Monitoring System
LB-LOCA	Large Break Loss Of Coolant Accident
LCD	Low-pressure Cool Down
LHSI	Low Head Safety Injection
LOCA	Loss Of Coolant Accident
LOMFW	Loss Of Main Feed Water
LOOP	Loss Of Off-site Power
LSP	Lower Support Plate
MCCI	Molten Corium-Concrete Interaction
MCR	Main Control Room
MCS	Maintenance Cold Shutdown
MDEP	Multinational Design Evaluation Programme (within OECD-NEA)
MHSI	Medium Head Safety Injection
MSTM	Multi-Stud Tensioning Machine
MW	Megawatts
NEA	Nuclear Energy Agency (within OECD)
NNL	National Nuclear Laboratory
NPP	Nuclear Power Plant
NT	Numerical Target
OECD	Organisation for Economic Cooperation and Development
ONR	Office for Nuclear Regulation
PAR	Passive Autocatalytic Recombiners

PCSR	Pre-construction Safety Report
PDF	Probability Distribution Function
POS	Plant Operating State
PRT	Pressuriser Relief Tank
PSA	Probabilistic Safety Assessment
PTR [FPCTS]	Fuel Pool Cooling and Treatment System
PWR	Pressurised Water Reactor
QA	Quality Assurance
RCCA	Rod Cluster Control Assembly
RCD	Refuelling Complete Discharge
RCP [RCS]	Reactor Coolant System
RCS	Refuelling Cold Shutdown
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RHWG	Rector Harmonization Working Group (of WENRA)
RIS [SIS]	Safety Injection System
RO	Regulatory Observation
ROAAM	Risk Orientated Accident Analysis Methodology
RP	Requesting Party
RPS [PS]	Reactor Protection System
RPV	Reactor Pressure Vessel
RQ	Regulatory Query
SADV	Severe Accident Dedicated Valve
SAMG	Severe Accident Management Guidelines
SAS	Safety Actuation system
SAP(s)	Safety Assessment Principle(s)
SB-LOCA	Small Break Loss Of Coolant Accident
SBO	Station Black Out
SDM	System Design Manual
SER [DWDS (CI)]	Convention Island Demineralised Water Distribution System
SED [DWDS (NI)]	Nuclear Island Demineralised Water Distribution System
SEP [PWS (NI)]	Nuclear Island Potable Water System
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SLB	Steam Line Break
SoDA	(Environment Agency's) Statement of Design Acceptability
SQEP	Suitably Qualified and Experienced Personnel

SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
TSC	Technical Support Contractor
UPS	Uninterrupted Power Supply
VDU	Visual Display Unit
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Table(s)

Annex(es)

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 Severe Accident Analysis.

2. The UK HPR1000 is a pressurised water reactor (PWR) design proposed for deployment in the UK. General Nuclear System Ltd (GNSL) 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 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 Severe Accident Analysis 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 a Regulatory Observation (RO) I raised. Any 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 Severe Accident Analysis 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) and international standards and guidance, 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 GDA Guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

10. The strategy for my assessment of the Severe Accident Analysis aspects of the 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 my assessment plan, ONR-GDA-UKHPR1000-AP-19-09. 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 scope 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 RO I raised as a result of my on-going assessment, and the resolution thereof.

2.2 Sampling Strategy

13. 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 relevant severe accident phenomena that have been identified by the RP to be considered in the severe accident analysis.
- The RP's identification of safety features which are used for severe accident management.
- The RP's methodology for identification of bounding severe accident scenarios and the final list of scenarios used in the severe accident analysis.
- The safety functions of the safety features used for severe accident management.
- The analyses which support the RP's safety claims that the severe accident safety features are effective.
- The verification and validation of the computer codes used in the severe accident analysis.
- The engineering requirements of the structures, systems and components (SSCs) used for severe accident management.
- The overall claims that the potential for early or large releases of radioactivity have been 'practically eliminated' by the UK HPR1000 design, as per the International Atomic Energy Agency (IAEA) standard SSR-2/1 (Ref. 6).
- The RP's demonstration that relevant risks have been reduced so far as reasonably practicable

14. The Severe Accident Analysis topic area is concerned with very unlikely, high consequence events involving scenarios in which the robust design basis safety measures fail to prevent the escalation of accidents to a core melt scenario. For new reactors, generic strategies for severe accident mitigation are considered during the design process. My assessment is focussed on the generic UK HPR1000 design, the safety features (as per IAEA's definition (Ref. 6)) which enable severe accident mitigation and the deterministic analysis which demonstrates the effectiveness of the severe accident safety features.

15. I have based my sampling strategy on the novelty of the design and complexity of the substantiation of the claims related to the effectiveness of the safety features. My assessment conclusions are informed by the application of this sampling strategy

across a broad range of the demonstration of the effectiveness of the severe accident safety features submitted by the RP in its safety case documentation. However, I have targeted for particular attention the approach taken to demonstrate the effectiveness of the safety features to provide safety functions for in-vessel retention (IVR) and hydrogen management because of their significance to the HPR1000 design, their importance to maintaining confinement barriers and the associated novelty and uncertainty.

16. During Step 3, I identified that the RP had not submitted analysis results of ex-vessel steam explosions. The RP has since submitted the analysis results to support claims that it understands the progression of severe accidents following failure of the RPV. This meets my expectation, however, I have chosen not to target this analysis as the RP claims that ex-vessel steam explosions are practically eliminated.

2.3 Out of Scope Items

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

- Source term analysis – the amount and isotopic composition of radioactive material postulated to be released from the UK HPR1000 in a severe accident is relevant to this assessment. The RP has used the ASTEC code (as part of its wider severe accident analysis) to estimate the source term for a range of severe accidents. In this assessment, I have considered the verification and validation of the ASTEC code to simulate severe accident phenomena. However, in a change to the approach set out in my Step 4 assessment plan (Ref. 5), the ONR review of underlying chemistry models and in-containment radionuclide behaviour has been captured in the ONR Chemistry assessment (Ref. 7).
- Containment performance – for many severe accident scenarios, the UK HPR1000 containment building is the final barrier protecting people and the environment from the resulting radiological hazard, and demonstrating its continuing ability to deliver its confinement function is a vital aspect of the RP's severe accident analysis. However, the containment performance and supporting capacity analysis is demonstrated in the Civil Engineering sections of the UK HPR1000 safety case, and they are also of interest to the Level 2 and 3 Probabilistic Safety Analysis (PSA). As a result the regulatory assessment of the adequacy of containment performance to the high pressures and temperatures (and the associated fragility curves) has been reported in ONR's Civil Engineering and PSA assessments (Refs 8 and 9). However, I have assessed how the output of the deterministic analysis has been used as an input to these calculations.
- Fuel route beyond the nuclear island – the fuel route beyond the storage in the Spent Fuel Pool (SFP) is not within the scope of GDA.
- Severe Accident Management Guidelines (SAMGs) - A detailed assessment of technical specifications, operating /emergency procedures and accident management arrangements is out of scope for GDA. However, in my assessment I have considered potential severe accident management strategies and the compatibility of these with the UK HPR1000 design.
- Site layout – anything that is site layout dependent is generally outside of the scope of GDA (e.g. storage of mobile equipment).

2.4 Standards and Criteria

18. The relevant standards and criteria adopted within this assessment are principally the SAPs (Ref. 2), Technical Assessment Guides (TAGs) (Ref. 4), 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, 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

19. ONR's SAPs have been benchmarked against international expectations. The SAPs (Ref. 2) constitute the regulatory principles against which ONR judge the adequacy of safety cases. The full list of SAPs applicable to Severe Accident Analysis are included within Annex 1 of this report.

20. The key SAPs applied within my assessment are as follows:

- Engineering key principles: EKP.3, EKP.4 and EKP.5
- Severe accidents: FA.1, FA.15, FA.16, FA.25
- Computer codes and calculation methods: AV.1, AV.2, AV.3, AV.5 and AV.6
- Accident management and emergency preparedness: AM.1
- Numerical Targets: NT.1

21. The engineering key principles set the expectation that the UK HPR1000 incorporates a defence in depth approach, that safety functions are derived to deliver the fundamental safety functions, and that SSCs are identified to perform those safety functions. My assessment has targeted Level 4 defence in depth (as established by SAP EKP.4). However, as part of my assessment of the RP's safety case for practical elimination of early or large releases, I have considered ONR's wider assessment of the safety case which includes other levels of defence in depth.

22. The fault analysis SAPs set the expectation that severe accidents should be analysed and that measures to prevent accident progression and to mitigate consequences are provided. ONR therefore expects that the severe accident analysis should be used to identify severe accident safety features that provide this mitigation, form a suitable basis for accident management, inform emergency arrangements and are used as an input to PSA. In addition, the SAPs set out expectations for how the severe accident analysis is performed.

23. The assurance of validity of models and data (AV) series of SAPs set the expectation that adequate evidence of the verification and validation of codes is provided for codes that are used in the safety case. This has been an important consideration for my assessment of the UK HPR1000 severe accident analysis. It should be noted that to form a view of the adequacy of the RP's generic processes to ensure the quality assurance of its computer codes (AV.4), I have looked to the regulatory conclusions reached in the Step 4 Fault Studies assessment report (Ref. 10). SAPs AV.7 and AV.8 are associated with the ensuring operating data is collected to benchmark code performance and that codes and methods are reviewed over time. As a result, they have limited significance for GDA and should be matters for a future licensee to demonstrate over a period of time.

24. SAP AM.1 relates to emergency planning and preparedness. The majority of the expectations set out within AM.1 are both site specific and for a future licensee to determine. I have therefore not applied these expectations during GDA. However, the expectations in paragraphs 778 and 780 of the SAPs are related to equipment used to carry out emergency response and inform decision making. These set high-level expectations for how SSCs used in emergency response should be designed and are therefore part of GDA.

25. The Numerical Targets 7, 8 and 9 are relevant to regulatory judgements on severe accident safety cases. They set expectations related to risks to the public for individual sequences, total frequency of accidents and societal risk. However, my assessment

has mainly focused of the effectiveness of severe accident mitigation strategies to maintain the final confinement safety function. Therefore, many of my conclusions are informed by deterministic demonstrations of meeting technical criteria which ensure the confinement function is successfully maintained. The risks for severe accidents and the relevant numerical targets are explicitly considered in ONR's PSA report (Ref. 9) but they do provide a context for the judgements in my report for judging whether risks have been reduced ALARP. I have also considered the numerical targets in my assessment of RP's claims that early or large releases of radioactivity have been practically eliminated.

26. The Fukushima Daiichi accident which occurred in 2011 was a severe accident caused by an earthquake near Japan. Many important lessons have been learnt from the accident and some, particularly relating to the systems designed to cope with accidents, have direct relevance to my assessment. Following the accident, ONR's Chief Nuclear Inspector carried out a review of the implications of the Fukushima Daiichi accident on the UK nuclear industry (Ref. 11). The 2014 revision of the SAPs was prompted by publication of this report. In addition, the 2014 revision of the SAPs also takes into account the revised Western European Nuclear Regulators Association (WENRA) reference levels (Ref. 12), which also incorporate learning from Fukushima Daiichi. By assessing the RP's safety case against the expectations of the SAPS, therefore, I have already taken into account the lessons learnt from the Fukushima Daiichi accident. For this reason, I have not explicitly assessed the RP's safety case against these lessons.

2.4.2 Technical Assessment Guides

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

- NS-TAST-GD-007: Severe Accident Analysis
- NS-TAST-GD-042: Validation of Computer Codes and Calculation Methods
- NS-TAST-GD-094: Categorisation of Safety Functions and Classification of Structures and Components
- NS-TAST-GD-051: The Purpose, Scope and Content of Nuclear Safety Cases
- NS-TAST-GD-005: ONR Guidance on the Demonstration of ALARP

28. ONR's Severe Accident Analysis Technical Assessment Guide (NS-TAST-GD-007) was in the process of being updated during my assessment. The intention of the update is to better align the guidance with international standards and guidance. Whilst my assessment is cognisant of the expectations that will be set out in the update, my assessment is based on the expectations set out in Revision 4, supplemented by international guidance, particularly SSG-2 (2019) (Ref. 6) and WENRA guidance on Practical Elimination Applied to New NPP Designs (Ref. 12).

29. It is important to note that the above TAGs have also incorporated relevant lessons learned from the Fukushima Daiichi accident.

2.4.3 National and International Standards and Guidance

30. Beyond ONR's SAPs and TAGs, no other national standards have been used in my assessment. The following main international standards and guidance were used as part of this assessment (Refs 6 and 12):

- IAEA SSR-2/1 - Safety of Nuclear Power Plants: Design.
- IAEA SSG-2 - Deterministic Safety Analysis for Nuclear Power Plants.
- WENRA - Statement on Safety Objectives for New Nuclear Power Plants.
- WENRA - Safety of New NPP Designs.

- WENRA - Practical Elimination Applied to New NPP Designs – Key Elements and Expectations.

31. These international standards and guidance have also incorporated relevant lessons learnt from the Fukushima Daiichi accident. In addition to these, WENRA Reference Levels for Existing Reactors (Ref. 12) establish a number of expectations relevant to reactor severe accident analysis. Of particular note, Issue F introduces the concept of Design Extension Conditions (DECs). However, the key considerations for the design of a new nuclear power plant by a RP in GDA (as opposed to the operation of a nuclear power plant by a licensee) are all covered by the IAEA and WENRA specifically identified above.

2.5 Use of Technical Support Contractors

32. 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.

33. Table 1 below sets out the areas in which I used TSCs to support my assessment. I required this support to provide independent technical support and to perform independent analysis techniques not available within ONR.

Table 1: Work Packages Undertaken by the TSC

Number	Description
1	An introductory course to the ASTEC code to ONR inspectors
2	A review of the RP's severe accident verification and validation documentation
3	An independent analysis of the IVR strategy

34. Work Packages 1 and 2 were carried out by Tractebel, and Work Package 3 was carried out by GRS. Whilst the TSCs undertook detailed technical reviews and analysis, 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.

35. The main outputs of the TSCs that I have used in my assessment can be found at Refs 13 to 21.

2.6 Integration with Other Assessment Topics

36. 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:

- Probabilistic Safety Analysis – I have worked closely with ONR's PSA inspector in the following aspects:
  - The Level 1 PSA has been used as an input to determine accident sequences that result in core damage. These form the starting point for severe accident analysis. I have worked with PSA to ensure that the

Level 1 PSA is adequate for used as an input to the Severe Accident Analysis topic area.

- The PSA assessment has not looked in detail at the deterministic analysis, or the verification and validation of the codes used for severe accident analysis. ONR's PSA inspector has taken assurance from my assessment that the codes are suitable for use and that the deterministic analysis is adequate for use in the PSA.
- The RP has used the PSA to quantify risks in support claims that early or large releases are practically eliminated. I have worked closely with ONR's PSA inspector to ensure that the RP's PSA is adequate for use in this area.

- Fault Studies – I worked closely with the Fault Studies inspector to:

  - Ensure that adequate independence between the levels of defence in depth have been incorporated into the design.
  - Gain assurance that the RP has provided adequate substantiation of arguments that support the RP's claim that early or large releases have been practically eliminated.

- Structural Integrity – I worked closely with the Structural Integrity inspector to gain confidence that:

  - the Reactor Pressure Vessel (RPV) will maintain its structural integrity during the IVR condition;
  - thermal shock to the RPV during initiation of IVR will not result in fast fracture and therefore failure of the RPV;
  - failure of primary circuit components during severe accidents (i.e. creep rupture of Steam Generator (SG) tubes) are unlikely to occur; and
  - appropriate arguments related to practical elimination have been provided.

- Control and Instrumentation (C&I) - I worked closely with ONR's C&I inspector to ensure that:

  - the safety functions that are claimed for severe accident mitigation are appropriately assigned to C&I platforms; and
  - adequate independence of the levels of defence in depth have been incorporated into the design.

- Mechanical Engineering – I worked closely with the Mechanical Engineering inspector to ensure that requirements for equipment qualification have used the appropriate environmental conditions for accident situations.
- Electrical Engineering – I worked with ONR's Electrical Engineering inspector to ensure that the equipment electrical loads for severe accidents have been appropriately assigned to the supporting power supplies and that adequate power can be provided during the severe accident scenarios considered in the safety case.
- Human Factors – I worked with ONR's Human Factors inspector to ensure that the appropriate severe accidents human based safety claims have been identified, and that human actions identified are achievable.
- Radiological Protection – I worked with ONR's Radiological Protection inspector to consider whether the Main Control Room (MCR) remains habitable during a severe accident, and that doses received whilst carrying out local human actions are acceptable.

- Chemistry – I worked with ONR's Chemistry inspector to:
  - gain assurance that the ASTEC code includes the relevant physiochemical interactions and that adequate verification and validation has been submitted to ONR; and
  - gain assurance that the source term analysis has been performed adequately.
- Civil Engineering – I worked closely with ONR's Civil Engineering inspector to ensure that the technical success criteria related to the containment, which are used in the severe accident analysis, are appropriate.

2.7 Overseas Regulatory Interface

37. ONR has formal information exchange agreements with a number of international nuclear safety regulators. This includes collaboration through the work of the IAEA and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). This enables ONR to utilise overseas regulatory assessments of reactor technologies, where they are relevant to the UK; this helps to expedite assessment and promote consistency.

38. As part of my assessment I have engaged in the OECD-NEA's HPR1000 Multinational Design Evaluation Programme (MDEP) Working Group. Within this, a Severe Accidents Technical Expert Sub-Group was established with the following members: the Nuclear Regulatory Authority of Argentina, National Nuclear Regulator of South Africa and the National Nuclear Safety Administration of the People's Republic of China. The sub-group has produced the following Technical Reports and Common Positions relevant to my assessment (Ref. 22):

- Technical Report on Severe Accidents Hydrogen Management – The regulatory expectations for management of hydrogen during severe accidents and the analyses that demonstrated the effectiveness of combustible gas management systems was summarised and common expectations were identified.
- Technical Report on Regulatory Expectations for Severe Accident Analysis – Regulatory expectations for new reactors on severe accident safety features and their safety functions, engineering requirements related to those safety features (e.g. safety classification), and severe accidents deterministic analyses were collated and summarised. Common expectations were identified.
- Common Position on Lessons Learnt from Fukushima – Common expectations for lessons learnt were identified, and a common position on how the design of the HPR1000 meets these expectations was summarised.

39. These international engagements, the reports and positions produced by the sub-group have provided useful insights which have informed my own assessment for GDA. In particular, I have taken useful insights related to acceptance criteria for hydrogen management, the methodologies applied to demonstrate the effectiveness of IVR, and other nation's views on how practical elimination is demonstrated.

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the Generic UK HPR1000 Design

40. 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 UK HPR1000 design. The generic UK HPR1000 design is claimed to have a lifetime of at least 60 years and has a nominal electric output of 1,180 MW.

41. 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 with a steel RPV which is connected to the key primary circuit components, including the Reactor Coolant Pumps (RCP), 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.

42. 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 MCR. The fuel building is also adjacent to the reactor building and contains the fuel handling and short term storage facilities, such as the SFP. Finally, the nuclear auxiliary building contains a number of systems that support operation of the reactor. In combination with the diesel generator, personnel access and equipment access buildings, these constitute the nuclear island for the generic UK HPR1000 design.

43. The SFP contains storage racks for storing both new and irradiated fuel assemblies in boronated water. Criticality safety is ensured by the geometric spacing between fuel assemblies, neutron absorbing storage racks and the boronated water. The racks have sufficient capacity to store up to 10 operating-years-worth of irradiated fuel and a full core offload. During refuelling, the reactor cavity is filled and the fuel transfer tube is opened, forming a continuous pool from the reactor to the SFP. The pool formed in the reactor building is referred to as the reactor pool within this report.

44. The UK HPR1000 includes multiple Level 2 and Level 3 defence in depth safety measures. These are designed to control the plant in normal operation and prevent design basis faults (referred to by the RP as Design Basis Conditions (DBCs) 2, 3 or 4 based on frequency) identified in the safety case escalating to severe accident states. ONR's assessment of the adequacy of the design basis safety measures is presented in the Fault Studies report (Ref. 10). For ease of referencing, the main design basis safety measures are the Safety Injection System (RIS [SIS]), which comprises the accumulators, Medium Head Safety Injection (MHSI) and Low Head Safety Injection (LHSI), the Emergency Feed Water System (ASG [EFWS]), the Atmospheric Steam Dump (VDA [ASDS]), reactor scram and the Emergency Diesel Generators (EDGs). In addition to the design basis safety measures described, the UK HPR1000 design includes the Secondary Passive Decay Heat Removal System (ASP [SPHRS]) as an additional safety feature to prevent some extreme fault sequences involving multiple failures escalating to a severe accident.

45. The reactor building forms the last barrier to release of radioactivity to the environment. Both walls of the double walled containment are built from reinforced concrete. The

inner concrete containment wall is lined with an internal steel membrane provided for leak tightness. The external containment wall is designed to withstand external hazards and prevent any challenge to the internal containment wall. Between the internal and external containment walls the Annulus Ventilation System (EDE [AVS]) extracts and filters gases which may have leaked from the internal containment in both design basis faults and severe accidents. Demonstrating the integrity of the internal concrete containment wall and its steel liner is an important consideration for severe accident analysis, as the potential failure of these may result in a step change in any off-site release of radioactivity. I refer to both the steel liner and the concrete wall as simply 'the containment' within this report.

46. In the unlikely scenario where the safety systems cannot prevent escalation of a design basis fault to a core melt scenario, the UK HPR1000 employs Level 4 defence in depth. The main safety features that provide severe accident mitigation are the IVR system, the Containment Combustible Gas Control System (EUH [CCGCS]), the Severe Accident Depressurisation Valves (SADVs), the Containment Heat Removal System (EHR [CHRS]) and the Containment Filtration and Exhaust System (EUF [CFES]). My assessment is mainly focused on Level 4 defence in depth.

47. In the following subsections I summarise the main severe accident safety features and safety case claims related to severe accident mitigation. My description below is a summary of the RP's safety case provided in Ref. 3.

3.1.1 The In-Vessel Retention System

48. During a severe accident in the UK HPR1000, the melted core and reactor internals mixture (known as 'corium') travels downwards with gravity. Without adequate severe accident mitigation, the corium can melt through the bottom of the RPV. The corium has the potential to cause an ex-vessel steam explosion in water that may be located below the RPV which can be highly energetic and challenge the containment and the internal containment structures, such as those that support the RPV.

49. In addition, if the corium comes in contact with the thick concrete basemat which is below the RPV, there is potential for the corium to melt through the basemat and leak to the environment. During the ablation of the concrete, chemical reactions can occur between the concrete and the corium which generate non-condensable and combustible gases. These interactions are collectively referred to as the Molten Corium Concrete Interaction (MCCI) and can challenge the containment function.

50. MCCI and ex-vessel steam explosions have the potential to lead to early or large releases of radioactivity from breach of the containment.

51. To prevent conditions arising in which these phenomena could occur, the UK HPR1000 employs an IVR strategy to retain corium within the RPV throughout a severe accident. The IVR system is a subsystem of the EHR [CHRS]. The objective is to provide sufficient cooling to the exterior of the RPV such that a melted core is retained within the RPV. The IVR strategy consists of both short-term passive and long-term active External Reactor Vessel Cooling (ERVC), without the requirement for in-vessel water injection.

52. Following relocation of corium from the core region to the RPV lower head, the corium is at a high temperature and continues to generate decay heat from fission products. In order to retain corium within the RPV, sufficient thickness must remain within the RPV wall so that it does not melt through or fail under the internal pressure of the RPV and the weight of the contents of the RPV.

53. IVR is designed to prevent excessive melting of the RPV wall and to maintain the strength of the RPV.

54. In addition, good heat transfer should be maintained between the RPV wall and the water. If the heat flux is too high, a film of steam can blanket the external surface of the RPV wall and the efficiency of heat transfer from the RPV wall to the ERVC decreases significantly. This phenomenon is commonly referred to as film boiling and occurs when the heat flux increases beyond the so called Critical Heat Flux (CHF). When film boiling occurs, the RPV wall temperature increases rapidly and is assumed to fail; therefore the RP aims to demonstrate that the heat flux remains below the CHF throughout the severe accident progression analysed.

55. A simplified diagram of the EHR [CHRS] is shown below in Figure 1. As stated, the IVR system is a subsystem of EHR [CHRS], and is depicted in the blue, red and green lines. It consists of a dedicated in-containment 'reactor pit flooding tank' (730 te capacity), one fast passive flooding line (green), one slower passive flooding line (also in green), two active flooding lines (depicted in blue and red), the reactor pit, an optimised ex-vessel reactor cooling channel with inlet and outlet doors, and six recirculation pipes (which are not depicted in Figure 1). Four valves isolate the IVR tank from the reactor pit.

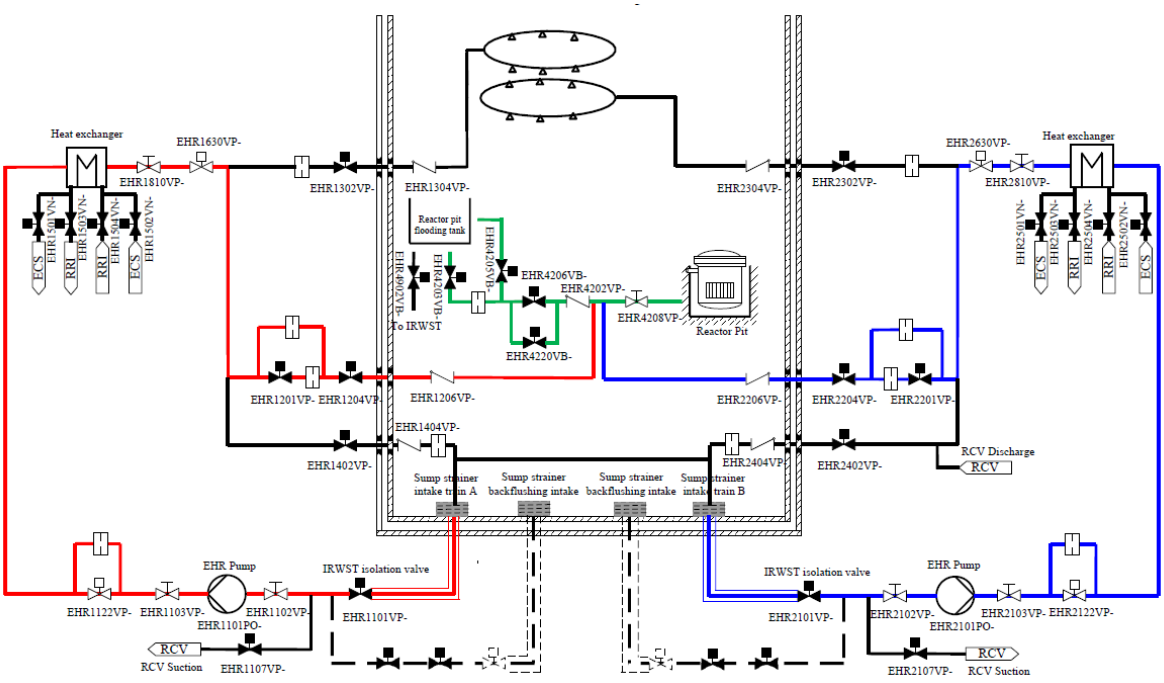

Figure 1: Simplified drawing of the EHR [CHRS]

56. The decision whether to implement severe accident mitigation is based upon a high temperature signal at the core outlet, set at 650 °C. Upon receiving the 650 °C core outlet temperature (COT) indication the operator is required to manually depressurise the primary circuit and begin flooding the reactor pit by manually opening four valves. All actions are carried out remotely from the MCR. Water is then gravity fed to the reactor pit via the lines (depicted in green in Figure 1) and begins to fill the reactor pit and the recirculation channels.

57. The ERVC channel surrounds the RPV and resides within the reactor pit. It is made up of Reflective Metallic Insulation (RMI) and is normally closed at the bottom to prevent unnecessary heat losses from the RPV in normal operation. Once the water level reaches the bottom of the ERVC channel, the doors, which are also made of RMI, open due to buoyancy forces, allowing the ERVC channel to fill with water. The IVR

tank drains until the water level in the tank falls below the elevation of the fast flow outlet pipe penetration. At this point, the reactor pit is filled and water is only needed to replace evaporative losses. As the water level is below the fast flow outlet penetration, the water can only be drained from the IVR tank to the reactor pit via the slow filling line (depicted by the green line from the bottom of the IVR tank in Figure 1), which has a penetration at a lower elevation to the fast flow line. The operator is required to switch to active injection before the IVR tank is depleted. The active injection lines are supplied by the In-Containment Refuelling Water Storage Tank (IRWST), which collects condensates from the containment and recirculates the water in the long term, without the need for an external water source.

58. As heat is removed from the RPV outer wall, the water temperature in the reactor cooling channel increases and steam is generated. The majority of water/steam loses heat to the surrounding structures and is recirculated to the bottom of the reactor pit via the six recirculation pipes. Any steam not recirculated discharges through a set of 12 exit doors located at the hot and cold legs of the RPV and is transported to the large containment space, where it condenses and is eventually transported to the IRWST.

59. The IVR subsystem is designed in such a way that the reactor pit can be quickly filled in approximately 30 minutes from initiation (i.e. fast passive filling). After this point, the water level is maintained passively via a slow passive injection line thereafter. After 10 hours the passive injection depletes and the operator is required to switch to active injection.

3.1.2 The Containment Combustible Gas Control System

60. During some PWR accident conditions there is potential for the generation of combustible gases. These gases can be generated by radiolysis of water (hydrogen), oxidation of metallic structures and fuel (hydrogen) and MCCI (hydrogen and carbon monoxide). The combustible gases generated in these processes can undergo combustion and result in failure of the containment. Accidents which do not lead to core melt, such design basis accidents, also lead to hydrogen generation primarily through oxidation of metals and radiolysis. The EUH [CCGCS] is designed to remove combustible gases from the containment that are generated by these processes.

61. Of these processes, the hydrogen generated by oxidation of the zirconium fuel cladding by steam presents the largest challenge to the hydrogen management during severe accidents in the UK HPR1000. This is because this reaction is exothermic, and the reaction rate is temperature dependent, providing a positive feedback loop. This feedback loop results in large quantities of hydrogen generated at a potentially high rate.

62. For GDA, as the UK HPR1000 is designed to prevent MCCI, the RP has only aimed to demonstrate that hydrogen can be managed sufficiently so that high energy combustion modes do not pose a challenge to the containment. High energy hydrogen combustion modes have the potential to result in a large or early radioactive release due to containment failure. By removing hydrogen from the containment, the EUH [CCGCS] limits concentrations such that the conditions in which a high energy combustion could occur are avoided.

63. The EUH [CCGCS] comprises passive autocatalytic recombiners (PARs) and in-containment hydrogen monitoring. The PARs recombine oxygen (in the containment atmosphere) and hydrogen to produce steam. There are 29 PARs within the containment of the UK HPR1000 of two different sizes. Two of these PARs are used for hydrogen management during some design basis accidents, such as Loss Of Coolant Accidents (LOCAs). The PARs are passive and do not require initiation. They are deliberately located to promote mixing of steam, air and hydrogen in the

containment and take advantage of natural circulation with the goal of avoiding dangerous concentrations of hydrogen.

64. The layout of the containment plays an important role in enabling the EUH [CCGCS] to remove hydrogen and to allow for good mixing of the hydrogen with other gases. In addition to enabling natural circulation, the containment design allows free flow between adjacent compartments and between compartments and the larger containment space.

65. The hydrogen monitors are used to inform decision making during severe accidents. There are two divisions of five monitors, located in various places around the containment to provide a good overall picture of local and average hydrogen concentrations. The monitors are started manually in severe accident scenarios and sample continuously thereafter. Information from the hydrogen monitors is displayed on a Visual Display Unit (VDU) within the MCR.

3.1.3 Severe Accident Depressurisation Valves

66. The pressure inside an RPV can potentially be very high during a severe accident. For severe accidents in the UK HPR1000 if the RPV is not depressurised then the internal pressure can result in failure of the RPV. This is because the RPV wall can be weakened as it is partially melted by the corium and has less strength at higher temperatures. Moreover, if the RPV failure occurs when the internal pressure is high, the corium can be ejected out of the RPV in a jet-like stream. High Pressure Melt Ejection (HPME) can result in a large pressurisation and potential failure of the containment.

67. During a HPME, the corium is ejected at high velocity and fragments, significantly enhancing heat transfer to the containment atmosphere and increasing the surface area of corium that can be oxidised which also generates heat (and hydrogen). The corium also has the potential to come into contact with the containment structures. The heating and over-pressurisation caused by these phenomena is commonly referred to as Direct Containment Heating (DCH) and have the potential to result in containment failure.

68. The UK HPR1000 includes three Primary Safety Valves (PSVs), which are designed to avoid overpressure of the primary circuit during faults where core melt does not occur. Whilst these too can be used to depressurise the primary circuit, the UK HPR1000 includes a set of valves dedicated to Level 4 defence in depth, SADVs, which are independent of the PSVs. The SADVs are fast acting for primary circuit depressurisation during a severe accident and are designed to be opened remotely from the MCR when the 650 °C COT is reached.

69. Whist they are mainly designed to prevent HPME and DCH, the depressurisation is also beneficial for enabling IVR, and for maintaining the structural integrity of the RPV and RCP [RCS] components during severe accident conditions; specifically, the RP claims that it interrupts high-pressure natural circulation of superheated steam which can fail components of the RCP [RCS] as it reduces the risk of creep rupture of the RPV after corium relocation.

70. Two trains of the SADV are connected to the upper dome of the pressuriser via a single common connection. Each train consists of both a gate valve (upstream) and globe valve (downstream) in series. The valves discharge to the Pressuriser Relief Tank (PRT) which is situated downstream of the SADVs.

71. The SADVs are designed to be used when the reactor pressure is not already equal to the containment pressure. When the 650 °C COT signal is received all four valves of

the SADV are designed to be opened and the primary coolant is discharged to the PRT. The PRT is designed with bursting discs which rupture as the pressure increases. The steam, water, non-condensable gases and fission products are then transported to the compartment in which the PRT resides and then to the larger containment space.

3.1.4 Containment Heat Removal System

72. During a severe accident in a PWR, water which is normally pressurised within the RPV evaporates and fills the containment with steam. Chemical and physical processes also generate non-condensable gases which are transported to the containment. Without mitigation, the pressure can continue to rise until containment failure occurs.

73. The UK HPR1000 includes the EHR [CHRS], which removes heat via spraying water from the inside of the upper dome of the containment. When the 650 °C COT signal is reached, the operator is able to actuate the EHR [CHRS] remotely from the MCR. The sprayed water droplets condense steam and the water is passively transported back to the IRWST (which sits at in the basement of the containment) via gravity. The water is cooled via a dedicated heat exchanger, which can be cooled by the Component Cooling Water System (RRI [CCWS]) (which is used in normal operation and rejects heat to sea water) or the Extra Cooling System (ECS) (which is only used in accident conditions and rejects heat to cooling towers), and is recirculated back to the spray rings. During a severe accident, the EHR [CHRS] is designed to remove sufficient heat to prevent containment overpressure without the need to vent the containment.

74. The EHR [CHRS] consists of two independent trains, each with a dedicated suction from the IRWST, heat exchanger, pump and spray ring. In addition, each heat exchanger of each train is cooled by an independent train of the ECS (or RRI [CCWS] if available).

3.1.5 Containment Filtration and Exhaust System

75. As stated above, during a severe accident in a PWR the containment fills with steam and non-condensable gases. Whilst for the UK HPR1000, the EHR [CHRS] is designed to cope with this phenomenon, the EUF [CFES] provides a back-up to the EHR [CHRS]. The RP claims (Ref. 3) that the EUF [CFES] is only required if the EHR [CHRS] fails upon demand and its functionality cannot be restored prior to the containment design limit being reached. The EUF [CFES], therefore, is only required in the extremely low probability sequence that a severe accident occurs and that the EHR [CHRS] fails.

76. The EUF [CFES] consists of a single penetration to the containment, two containment isolation valves, a combined filter unit, a downstream isolation valve, a rupture disc, a stack and a sub-system for replenishment of the filter bed.

77. In scenarios where the EHR [CHRS] has failed and pressure increases above the containment design pressure (0.52 MPa), the EUF [CFES] is opened, the rupture disc then opens and pressure inside the containment reduces.

78. The main purpose of the EUF [CFES] is to avoid catastrophic and irreversible damage to containment which results in unfiltered radioactive release to the environment. Discharges via the EUF [CFES] are filtered, significantly reducing the radioactivity of any gases vented from the containment. Moreover, the EUF [CFES] can be opened and closed multiple times in order to control the pressure of the containment whilst minimising the radioactive releases that are associated with its operation.

3.2 The UK HPR1000 Safety Case

79. In this section I provide an overview of the Severe Accident Analysis 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.

80. Requirement 20 of IAEA SSR-2/1 (Ref. 6) and the proceeding paragraphs to that requirement set the expectation that analysis of DECs is performed. To support meeting this expectation the RP has performed deterministic analysis of accidents without significant core damage and accidents with core melt. The RP refers to these as DEC-A events or sequences and DEC-B sequences, respectively. The RP only refers to DEC-B analysis in the context of deterministic analysis of the reactor (and not, for example, for severe accident analysis of spent fuel pool faults) and DEC-B scenarios as ones considered in the design of severe accident safety features. I have therefore adopted this terminology within my assessment report.

81. The RP has designed the safety features to support the 'severe accident mitigation strategies' (which is a term used by the RP, which is equivalent to 'high level candidate actions' defined in SSG-54 (Ref. 6)) based on the deterministic analysis of DEC-B sequences presented in the safety case.

82. The RP's DEC-B analysis forms a major part of its Severe Accident Analysis safety case. The main objective of the RP's Severe Accident Analysis safety case, therefore, is to identify all potential severe accident phenomena that have the potential to lead to an early or large release, to identify all sequences in which these phenomena can occur, to identify severe accident management strategies to prevent conditions arising in which those phenomena could occur, and to analyse the effectiveness of those strategies.

83. The RP's Severe Accident Analysis safety case also:

- addresses scenarios where the focus is on prevention rather than mitigation of severe accidents (e.g. the SFP);
- serves as a basis for the future development of SAMGs;
- provides an input of severe accident analysis for derivation of engineering requirements (e.g. classification of equipment, qualification of equipment, redundancy etc.);
- provides a link between the deterministic analysis and safety functions (including human actions);
- provides a holistic demonstration that the UK HPR1000 is designed to practically eliminate the potential for early or large releases of reactivity; and
- summarises the ALARP considerations from a severe accident analysis point of view.

84. The above aspects are discussed in further detail in sub-sections 3.2.1 and 3.2.2.

3.2.1 PCSR Structure

85. The RP has taken a tiered approach in constructing its safety case. The PCSR is the top-level tier 1 safety report, which is supported by tiers 2, 3 and 4. The most relevant chapter of the PCSR for this assessment is 'Chapter 13 Design Extension Conditions and Severe Accident Analysis' (Ref. 3).

86. Chapter 13 of the PCSR includes both DEC-A and Severe Accident Analysis, which encompasses DEC-B analysis. My assessment only covers Severe Accident Analysis

aspects of Chapter 13 of the PCSR. The assessment of DEC-A aspects have been assessed by ONR's Fault Studies inspector (Ref. 10).

87. The PCSR summarises the arguments and evidence which support the Severe Accident Analysis claims. Documents in tiers 2 and 3 include the more detailed supporting arguments and evidence. The majority of my assessment has been performed on tier 2 and 3 documents.

3.2.2 The RP's Claims, Arguments and Evidence Structure

88. Ref. 3 lists the high-level claims related to Severe Accident Analysis, and the more detailed "Sub-Claims" which support those claims. As stated in Ref. 3 the "Sub-Claims" relevant to the Severe Accident Analysis safety case are:

- Sub-Claim 3.2.3.SC13.2: The understanding of severe accident progression and phenomena related to the UK HPR1000 is adequate.
- Sub-Claim 3.2.3.SC13.3: The analysis codes and models used for severe accident analysis are appropriate to simulate severe accident phenomena and progression.
- Sub-Claim 3.4.7.SC13.2: The severe accident management strategies and engineered measures are proved to be effective and ALARP.
- Sub-Claim 3.4.7.SC13.3: UK HPR1000 is capable to deal with extreme events like Fukushima accident.
- Sub-Claim 3.4.7.SC13.4: The behaviour of fission products during a severe accident is properly considered.

89. The arguments and evidence that underpin the above claims can be found in PCSR Chapter 13 (Ref. 3) and its supporting references. Put simply, the RP's claim is that it has identified all relevant severe accident sequences, has designed mitigation for phenomena arising from those sequences and has demonstrated that the safety features are effective such that the containment will remain intact during a severe accident.

90. Figure 2 below is a pictorial representation of the RP's safety case which can be found in the RP's production strategy for Chapter 13 (Ref. 23). Whilst the diagram does not directly identify the individual documents submitted, it does provide a useful depiction of the safety case which underpins the above safety claims. The key elements to the Severe Accident Analysis safety case are highlighted in blue and orange and are described in further detail below.

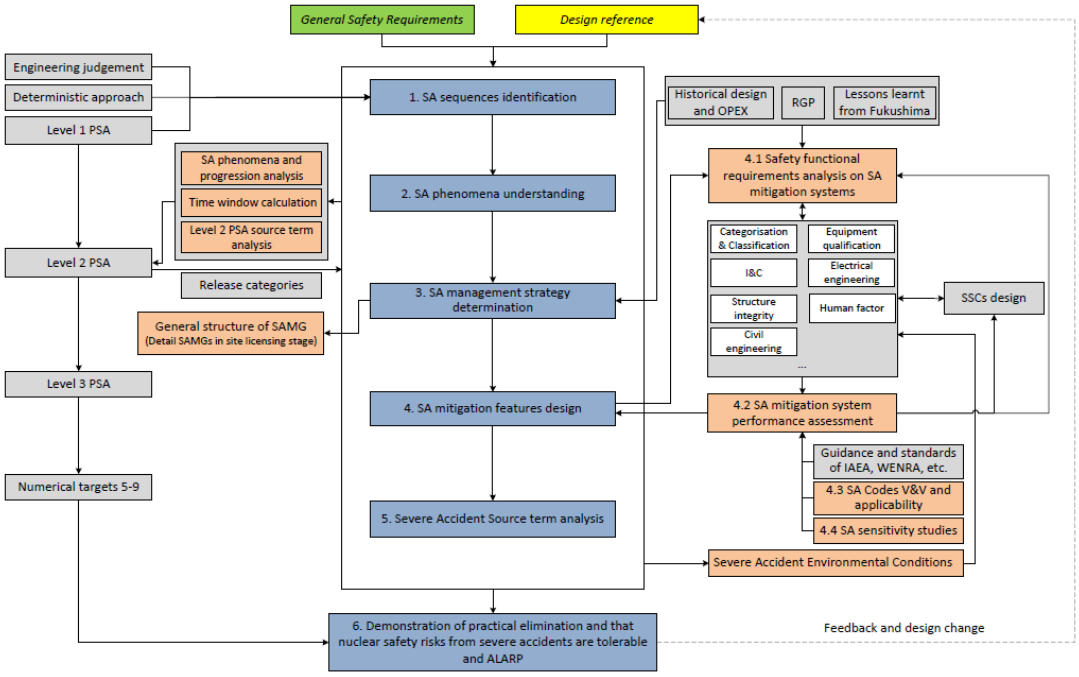

Figure 2: "F-4-1 Golden thread of Severe Accident Analysis safety case" - Ref. 23

91. The main aspects of the safety case for the UK HPR1000 are:

- Severe Accident Sequences Identification – The RP has used the Level 1 PSA (Ref. 24) to identify appropriate severe accident sequences which result in core damage states. From this, the RP determines a small selection of 'scenarios' on which to base the design of severe accident safety features (Refs 25 and 26). The scenarios are modified by the RP depending on the safety case claim it is aiming to substantiate.
- Severe Accident Phenomena Understanding – The RP has identified important severe accident phenomena that should be considered in the UK HPR1000 design, and has identified which of those should be prevented or mitigated, and those which can be excluded from analyses of the effectiveness of the severe accident safety features (Refs 27 and 28).
- Severe Accident Management Strategy Determination – For each phenomenon that is required to be prevented or mitigated the RP has identified a severe accident management strategy and appropriate safety features (Refs 27 and 28).
- Severe Accident Mitigation Safety Features:
  - Safety functions - The RP has derived safety functions and assigned severe accident safety features to carry out those safety functions (Refs 29 to 34).
  - Effectiveness of Safety Features - The RP has performed deterministic analyses using several computer codes to demonstrate that appropriate safety criteria can be met with the correct performance of safety features (Refs 35 to 39).
  - Verification and validation - The RP has provided verification and validation for the appropriate codes, identified the parameters with the largest uncertainties and performed sensitivity studies on those parameters (Refs 40 to 47).
  - System Design Manuals – A system design manual has been provided for each important system credited in the Severe Accident Analysis

topic area. This acts as the interface between the engineering and the fault analysis (Refs 48 to 75).

- Severe Accidents Source Term Analysis – The RP has performed source term analysis using the ASTEC code (Ref. 76), which has been used in the Level 3 PSA (Ref. 77). As stated previously, the assessment of the source term analysis has been performed by the Chemistry inspector (Ref. 7).
- Demonstration of Practical Elimination and ALARP – The RP has provided substantiation for the claim that early or large releases have been practically eliminated using both deterministic and probabilistic arguments (Ref. 78). This includes practical elimination of severe accidents occurring in the spent fuel pool or when the reactor is in a shutdown state during refuelling. In addition, the RP has provided a separate demonstration that the UK HPR1000 design meets RGP and has reduced risks to ALARP (Ref. 79).

4 ONR ASSESSMENT

4.1 Structure of Assessment Undertaken

92. As explained in sub-section 3.2.2 the RP has established a number of key claims associated with Severe Accident Analysis and presented its safety case accordingly. The structure of my report largely follows that of the RP's safety case, but has been adapted where necessary to improve readability. I have therefore broken up my assessment report into the following sections:

- Sub-section 4.2: Assessment of the RP's Identification of Severe Accident Phenomena - I summarise my assessment of the RP's identification of relevant severe accident phenomena for consideration in DEC-B analysis.
- Sub-section 4.3: Assessment of the RP's Identification of Severe Accident Management Strategies and Safety Features – I summarise my assessment of how the severe accident management strategies and safety features have been identified. I also present my assessment of the safety function identification process related to the safety features.
- Sub-section 4.4: Assessment of the RP's Identification of Severe Accident Scenarios – I summarise my assessment of how the RP has used the PSA and deterministic judgement to derive scenarios to determine the design characteristics of the severe accident safety features.
- Sub-section 4.5: Assessment of RP's DEC-B Analyses – I summarise my assessment of the analyses which demonstrates the effectiveness of the DEC-B safety features for severe accident mitigation.
- Sub-section 4.6: Assessment of the Severe Accidents Codes – I summarise my assessment of the application of the computer codes that have been used to substantiate safety claims, the verification and validation of those codes, and the sensitivity analysis performed to account for uncertainties in the codes.
- Sub-section 4.7: Assessment of Engineering Requirements: I summarise my assessment of the adequacy of the engineering requirements of the safety features and the associated supporting SSCs.
- Sub-section 4.8: Other Aspects of Severe Accident Management – I summarise my assessment of the adequacy of the supporting systems that enable severe accident management, the relationship between the severe accident analysis and the human actions which support severe accident management.
- Sub-section 4.9: Assessment of Claims Related to Practical Elimination of Early or Large Releases of Radioactivity – I summarise my assessment of the RP's probabilistic and deterministic arguments that the UK HPR1000 has been designed such that early or large releases have been practically eliminated.
- Sub-section 4.10: Demonstration that the Relevant Risks have been Reduced ALARP – I summarise my assessment of the RP's claims that the UK HPR1000's severe accident mitigation strategies meet RGP, are comparable to other Generation-III reactors and that, in relation to severe accidents, no further improvements can be made to reduce risks ALARP.
- Sub-section 4.11: Consolidated Safety Case (Chapter 13) – For the majority of the time during GDA only PCSR Version 1 and responses to RQs were available. I summarise my assessment of whether the RP has adequately incorporated important information exchanged in RQ responses into Version 2 of the PCSR.
- Sub-section 4.12: Comparison with Standards, Guidance and Relevant Good Practice – In this section I summarise which standards, guidance and RGP I have applied to come to my judgements on the adequacy of the RP's safety case.

93. The RP has taken the approach to 'practically eliminate' sequences which lead to severe accidents in the SFP and in the reactor in some shutdown states. Since the

claims related to practical elimination are based on the prevention of occurrence of a severe accident, I have chosen to focus my assessment on the reactor for plant states where the RCP [RCS] and containment are closed. Sub-sections 4.2 through to 4.8, therefore, only consider severe accident mitigation of the reactor. My assessment of claims related to prevention of sequences that could lead to an early or large radioactive release (such as those in the SFP) is summarised in sub-section 4.9.

4.2 Assessment of the RP's Identification of Severe Accident Phenomena

94. It is my expectation that a Severe Accident Analysis safety case clearly sets out which phenomena are of importance for severe accident analysis, and which should be designed to be prevented or mitigated. My general expectations for which I have judged the adequacy of the RP's submissions are informed by SAP FA.15 and NS-TAST-GD-007. My expectations for what constitutes RGP for the analysis of a modern PWR design are also informed by IAEA SSG-2 (Ref. 6).

95. In Ref. 3, the RP claims that the design of the severe accident safety features should be based on appropriate severe accident scenarios, underpinned by an adequate understanding of relevant severe accident phenomena. As mentioned, this approach is aligned with the IAEA's approach to design extension conditions with core melting (Ref. 6), and is referred to by the RP as DEC-B analysis.

96. In Ref. 3, the RP has made the high-level claim that "the understanding of severe accident progression and phenomena related to the UK HPR1000 is adequate" (Sub-Claim 3.2.3.SC13.3). This section presents my assessment of the RP's identification of relevant severe accident phenomena, and which ones it has chosen to design the safety features to prevent or mitigate, and which ones it has chosen to exclude from further consideration in the DEC-B analysis of the effectiveness of the safety features.

97. Ref. 27 describes the RP's methodology for its Severe Accident Analysis safety case. Within this reference, the RP aims to demonstrate an adequate understanding of the relevant severe accident phenomena and to justify which phenomena its DEC-B analysis of the effectiveness of the severe accident safety features should be based upon.

98. In Ref. 3, the RP presents a qualitative description of the progression of a typical unmitigated severe accident in a PWR. Whilst the description is brief, the RP has suitably referenced appropriate publications and demonstrated that it understands the main aspects of severe accident progression in PWRs. For example, the RP includes the appropriate physical processes presented in paragraph 7.66 of SSG-2 (Ref. 6). Using the learning from the progression of the severe accident and a review of RGP for similar reactors, the RP has identified important phenomena that should be considered in the design of the UK HPR1000 severe accident management strategies. The RP lists these as:

- In-vessel steam explosion
- Re-criticality
- Ex-vessel steam explosion
- HPME and DCH
- MCCI
- Hydrogen combustion
- Containment overpressure

99. The RP puts these into two groups: those which should be considered for the design of severe accident safety features, and those which it considers can be discounted. The adequacy of RP's justification for what phenomena should be included in the design of the safety features is discussed below.

4.2.1 Phenomena Excluded from Further Consideration in the Design

100. Two internationally recognised severe accident phenomena which have the potential to occur in PWR are in-vessel steam explosions and re-criticality (Ref. 80):

- In-vessel steam explosions can be initiated as corium slumps from the core region into a pool of water in the RPV lower head. The process is caused by the Fuel Coolant Interaction (FCI) in which the collapse of the steam blanket on a fuel fragment can cause a fast vaporisation of surrounding water, propagating to adjacent fragments resulting in the collapse of steam blankets of other fragments and further propagation. The resulting pressure increase may challenge the integrity of the RPV and ultimately challenge the containment.
- Re-criticality of a partially melted core has the potential to occur if the RPV is re-flooded when the fuel matrix is in a favourable geometry and in the absence of absorber rods (which could melt before fuel materials). Re-criticality has the potential to generate additional energy and invalidate assumptions in the DEC-B analysis used in the design of severe accident measures.

101. The RP has chosen not to design severe accident safety features to mitigate these phenomena, and to exclude these phenomena in its DEC-B analysis of the effectiveness of its safety features.

102. In early revisions of PCSR Chapter 13 (Ref. 3), the RP provided a limited discussion of why in-vessel steam explosions should be excluded from consideration of the design of severe accident safety features based on the low likelihood of occurrence of in-vessel steam explosions and the associated energy generated. I judged that the RP had not provided adequate arguments for excluding in-vessel steam explosions and that the implications of this phenomenon on the IVR strategy had not been fully considered. Through challenges that I provided in RQ-UKHPR1000-0241 (Ref. 81), the RP has significantly improved its arguments presented in Ref. 3. The RP has collated findings from the US Nuclear Regulatory Commission's Steam Explosions Review Group workshop (Ref. 82) and OECD's Steam Explosion REsolution for Nuclear Applications (SERENA) (Ref. 83) and other research on the lower head of the RPV (Ref. 84) to provide arguments that the energy generated would not challenge the integrity of the RPV, and therefore the containment. I judge that the arguments are compelling and apply to any civil PWR of a similar size to the UK HPR1000.

103. The RP has also provided arguments related to the low likelihood of an in-vessel steam explosion arising as a result of FCI. These arguments are based on findings from several experimental facilities (KROTOS, FARO and MIXA) (Ref. 3) which aim to replicate the conditions within a PWR such as the UK HPR1000. Below I summarise the RP's arguments presented in Ref. 3:

- Without an external trigger the likelihood of the initiation of steam explosions is very low (where a trigger is a sufficiently large shockwave from an external source is required to collapse the steam blanket at the same time as the corium debris is descending).
- Specific premixing of liquid metal is required in order to reach the conditions required for a sustained steam explosion. As the liquid metal moves through the water it changes geometry and can separate into smaller parts. The geometry, size and spatial separation between droplets are important for achieving the right conditions. These conditions are hard to achieve in the UK HPR1000.
- Saturated water and water with voidage supresses steam explosions. This is directly applicable to the UK HPR1000 because any water in the lower head during a severe accident in these conditions.

- Compared to other materials, it is difficult for metals with similar properties to corium to trigger a steam explosion. The materials used in the experiments had similar properties to corium that would form in the HPR1000, and the findings are directly applicable.

104. The RP concludes that the combination of the above findings means that the occurrence of an in-vessel steam explosion is very unlikely to occur in the UK HPR1000 (Ref. 3). The RP also concludes that even if an explosion did occur, the consequences are very unlikely to challenge the integrity of the RPV (and therefore the containment). Given that the arguments are based on well-established international understanding and backed up by findings from experimental facilities, I conclude that it is reasonable to exclude in-vessel steam explosions from further consideration in the design of the severe accident safety features.

105. Similarly, early versions of Chapter 13 of the PCSR (Ref. 3) did not identify re-criticality as a relevant phenomenon for consideration because re-flooding of the reactor is not credited in the design of IVR (i.e. IVR can remove all required heat without the need to flood the reactor). I did not consider this a valid argument per se, because it is internationally recognised that slowing the core melt scenario is beneficial to the IVR strategy (Ref. 20). In RQ-UKHPR1000-0241 (Ref. 81), I challenged the RP because I considered it likely that late re-flooding would be considered in a 'real world' severe accident scenario and that re-criticality due to late re-flooding has the potential to generate more onerous conditions for the IVR strategy (i.e. through additional heat generation). In response to RQ-UKHPR1000-0241 (Ref. 81), the RP stated that the likelihood of re-criticality was very low due to the short time window in which re-criticality could occur and that the operator would preferentially inject boronated water. In addition, the RP argued that the operator would consider the advantages (additional heat removal and reduction of fission product transfer to the containment) and disadvantages (potential steam explosions, additional hydrogen generation, re-criticality and risk of creep rupture to SG tubes) before taking the action to re-flood the RPV.

106. In response to RQ-UKHPR1000-0241 (Ref. 81), the RP has also provided a criticality analysis of several degraded core configurations that demonstrates that criticality is not reached when boronated water is injected (Ref. 85). My assessment of this analysis can be found in sub-section 4.5.7. My assessment found that the RP's claims that re-criticality would not occur if boronated water was injected for the worst-case core configurations are justified.

107. On the basis that the RP has clearly stated that its assumption is that reflooding is not required for success of the IVR strategy, that the time window for re-criticality is short, and that the additional analysis provided by the RP demonstrates that criticality is not reached (Ref. 85), I am content with the arguments that the phenomenon can be excluded from the conditions analysed in the submitted GDA DEC-B analysis. The actual severe accident management guidelines (SAMGs) which will inform the actions taken by an operator following a severe accident in a UK HPR1000 reactor will be a matter for a future licensee. If it was to make different assumptions from those made by the RP in GDA, the site-specific safety case may need to revise the DEC-B scenarios considered. However, this is a matter for a future licensee and I cannot predetermine its choices during GDA.

4.2.2 Phenomena Included for Consideration in the Design

108. The RP has identified the following phenomena that should be designed to be prevented in the UK HPR1000:

- high energy hydrogen combustion;

- containment overpressure;
- HPME and DCH;
- ex-vessel steam explosions; and
- MCCI.

109. The RP argues that these phenomena have the potential to result in an early or large release and should be 'practically eliminated'. For the Severe Accident Analysis topic area, this means that the severe accident safety features should be designed to prevent the conditions in which these phenomena should occur during severe accidents. The RP's approach is not to analyse the consequences of the occurrence of the above phenomena (i.e. unmitigated sequences), but to design its severe accidents safety features in order to prevent the conditions in which they could occur.

110. These phenomena are broadly consistent with the appropriate severe accident phenomena described in paragraphs 3.56, 3.57 and 7.68 to 7.72 of SSG-2 (Ref. 6). However, I note that the RP has not identified consequential containment bypass as a phenomenon for consideration in the design of safety features (i.e. SG tube creep rupture). Nevertheless, the RP has made claims that the consequential containment bypass are avoided by the UK HPR1000 design within Ref. 37. This therefore only a slight omission in the RP's safety case.

111. I am satisfied that the RP has adequately identified and justified appropriate severe accident phenomena in accordance with the expectations of SAP FA.15 and NS-TAST-GD-007. The resulting list of phenomena that has been considered in the design of severe accident safety features is consistent with guidance provided in IAEA SSG-2 (Ref. 6), and I am content with the final list.

4.2.3 Strengths

112. The RP has provided adequate demonstration that it has identified the relevant phenomena for consideration of the design in of the severe accident safety features of the UK HPR1000. Where challenged, the RP has provided additional evidence in the form of results from international experiments and its own deterministic analysis to demonstrate that in-vessel steam explosions and re-criticality phenomena should be excluded from further consideration in the design of the severe accident safety features. This meets the expectations of FA.15 and NS-TAST-GD-007.

113. The phenomena identified are consistent with internationally recognised phenomena that require mitigation and match closely to those listed in IAEA SSG-2 (Ref. 6). The RP's methodology of identifying phenomena in which the UK HPR1000 severe accident safety features should be designed to prevent or mitigate is aligned with IAEA SSG-2 (Ref. 6).

4.2.4 Outcomes

114. I have identified no Assessment Findings or minor shortfalls related to the RP's identification of severe accident phenomena.

4.2.5 Conclusions

115. I have assessed the RP's identification of severe accident phenomena against the expectations of FA.15, NS-TAST-GD-007 and IAEA SSG-2.

116. My conclusion is that the RP has identified appropriate phenomena for consideration in design of severe accident safety features.

4.3 Assessment of the RP's Identification of Severe Accident Management Strategies and Safety Features

117. It is my expectation that a Severe Accident Analysis safety case should identify lower level safety functions to support control of the fundamental safety functions listed in the SAPs (Ref. 2) as:

- control of reactivity (including re-criticality following an event);
- removal of heat from the core; and
- confinement of radioactive material.

118. It is my expectation that SSCs are also designated to fulfil these safety functions. My general expectations are informed by SAP FA.15 paragraph 671, FA.16 paragraph 672, EKP.4 and EKP.5. My expectations for what constitutes RGP for a modern PWR design are also informed by IAEA SSG-2 (Ref. 6).

119. The UK HPR1000 severe accident strategy for ensuring that heat removal and confinement functions are delivered is to control (and therefore prevent) the conditions that could lead to the phenomena listed in paragraph 108 (for example, preventing high energy hydrogen combustion modes provides control of the confinement fundamental safety function). As stated previously, the melted core is predicted to be subcritical even when boronated water is injected into the core. The control of the reactivity fundamental safety function is therefore not taken into consideration in the design of severe accident safety features of the UK HPR1000.

120. Prevention of the phenomena listed in paragraph 108 is dependent on the severe accident management strategy chosen. For example, for MCCI the RP has chosen to prevent basemat melt through by employing the severe accident management strategy of in-vessel corium retention, whereas some other reactors, such as the EPR, employs corium spreading.

121. The RP has assigned a severe accident mitigation strategy for each phenomenon (Ref. 3). A safety feature is then identified to carry out each mitigation strategy (Ref. 3). Although not expressed in the same terms, my interpretation of the RP's hierarchy of fundamental safety functions to lower level safety function to be carried out by safety features is listed below:

- Fundamental safety functions
- Phenomena to be controlled
- Severe accident mitigation strategies
- Safety functions (of the safety features)

122. The RP's starting point is to analyse how a severe accident progresses without mitigation (Ref. 28) in order to gain insights into the mitigation strategy required and the more detailed safety functions that the safety features should perform. I have therefore structured the following sections on this basis. In the following sections, I summarise my assessment of:

- the RP's use of the unmitigated severe accident scenario to gain insights into accident progression;
- the RP's methodology to derive appropriate severe accident management strategies to prevent phenomena; and
- the identification of safety functions that enable those strategies, and the safety features that carry out those safety functions.

4.3.1 Unmitigated Severe Accident Scenario

123. Ref. 28 presents analysis of an unmitigated Large Break Loss Of Coolant Accident (LB-LOCA) using the ASTEC code in order to further understand the progression of a severe accident. The RP describes various relevant phenomena during the progression of the severe accident from the initial core degradation, corium relocation to the lower core support plate, slumping to the RPV lower head and the eventual failure of the RPV. Although the RP has not gone into detail regarding all phenomena that influence the core degradation process (e.g. clad ballooning), I am satisfied that the RP has demonstrated an adequate understanding of the unmitigated severe accident progression and that appropriate physical processes are modelled. I am therefore satisfied that the expectations of SAP FA.15 paragraph 671 and IAEA SSG-2 paragraph 7.66 (Ref. 6) have been met.

124. The RP argues that all of the UK HPR1000 reactor DEC-B scenarios present the same challenges to the containment and learning from the unmitigated LB-LOCA is applicable to all severe accident scenarios. The RP has chosen the LB-LOCA as it is the fastest acting severe accident which presents the most onerous conditions in terms of decay heat to be removed.

125. In my opinion, the RP's analysis of the unmitigated LB-LOCA cannot provide insights to phenomena associated with high pressure severe accidents, such as high pressure melt ejection. Ref. 28 notes, however, that insights on how the safety features should be designed have been taken from RGP, CGN's earlier reactor designs, and from other comparable Generation-III reactors.

126. The purpose of this analysis is to demonstrate a logical approach to determining severe accident strategies. Moreover, the RP's other analyses (Refs 35 to 39) demonstrates that severe accidents in the UK HPR1000 do progress in a similar way to the LB-LOCA, regardless of the initiator. I therefore judge that the RP's approach is appropriate and allows for the identification of severe accident management strategies and the safety functions of the safety features which support those strategies, aligned with the expectations of FA.16 paragraph 672.

4.3.2 Derivation of Severe Accident Management Strategies and Assignment of Safety Features

127. The RP assigns a single safety feature for each severe accident management strategy identified. Because of this, the RP then derives the safety functions required by each safety feature. In Ref. 28, the RP presents the below table, explaining the link between severe accident mitigation strategies and the safety features.

Table 2: Severe Accident Mitigation Strategies and Severe Accident Safety Features

Severe Accident Phenomena	Severe Accident Mitigation Strategy	Severe Accident Safety Feature
HPME /DCH	Primary System Overpressure Protection	SADV
High Energy Hydrogen Combustion	Combustible Gas Control	EUH [CCGCS]
Ex-Vessel Steam Explosion	In-Vessel Corium Retention	IVR (subsystem of EHR [CHRS])

Severe Accident Phenomena	Severe Accident Mitigation Strategy	Severe Accident Safety Feature
MCCI		
Containment Overpressure	Containment Heat Removal	EHR [CHRS]
	Containment Filtration and Venting	EUF [CFES]

128. The strategies identified are well established internationally for mitigating severe accident phenomena in PWRs (see paragraph I-25 of SSG-2 (Ref. 6), for example).

129. Neither the PCSR (Ref. 3) or the supporting reference , Ref. 28, identify a severe accident management strategy to avoid containment bypass as a consequence of severe accidents. The pipework which penetrates the containment and is in operation during a severe accident is qualified for severe accident conditions. By qualifying the pipework for severe accident conditions, the risk of bypass via this route is reduced significantly (see sub-section 4.6). However, creep rupture of the SG tubes induced by high pressures and temperatures is a possible bypass that could occur if the primary system is not depressurised. Nevertheless, the primary system overpressure protection provides protection against this phenomenon and the safety function to avoid bypass is identified in Ref. 32. This is therefore only an omission in the documentation (Ref. 28), and I regard this as a minor shortfall.

130. To support the majority of the severe accident management strategies above, the RP also identifies the severe accident instrumentation and control (KDA [SA I&C]) platform as a supporting system. I address the adequacy of the derivation of safety functions for the KDA [SA I&C] in section 4.3.3.1 below.

131. To conclude this sub-section:

- the RP has identified a severe accident safety feature against each of the severe accident mitigation strategies as shown in Table 2 above.
- The safety features identified are similar to those employed in other Generation-III reactors assessed through ONR's GDA process.
- I am satisfied that the RP has identified appropriate safety functions and severe accident safety features to perform those severe accident management strategies.

4.3.3 Identification of Safety Functions

132. As stated previously, it is my expectation that safety functions are identified to support control of the fundamental safety functions and that SSCs are assigned to carry out these safety functions. In doing so, it is my expectation that the safety case is clear, auditable and traceable, so that the reasoning can be understood by a future user of the safety case. My expectations for this are informed by the general expectations of SAPs EKP.4, EKP.5 and SC.2.

133. The RP has derived safety functions that are required to be carried out by the safety features in order to deliver the severe accident management strategies. The RP refers to these as "safety functional requirements". In the majority of the cases these "requirements" are high level, and I have therefore referred to these using ONR's terminology of "safety functions".

134. The RP submitted a summary (Ref. 86) of the severe accident safety features and the associated safety functions. The safety functions delivered by each safety feature, the categorisation of those functions and the classification of the equipment are described in Ref. 86. Ref. 86 is also supported by a suite of documents for the corresponding severe accident safety features (Refs 29 to 34). Within these documents, the RP has attempted to further decompose the safety functions.

135. I have sampled the identification of safety functions process carried out by the KDA [SA I&C] and IVR subsystem to determine whether the safety functions have been identified adequately. I have chosen to sample these as they encompass different types of engineering systems. A summary of my assessment is presented in the following subsections.

4.3.3.1 KDA [SA I&C] Safety Functions

136. The KDA [SA I&C] is a two division, software and hardware based, F-SC3 system (which is equivalent to ONR's definition of a Class 3 system). The RP claims that the KDA [SA I&C] supports all of the functions required for severe accident mitigation (Ref. 29):

- Primary system depressurisation to avoid the high-pressure core melt accident;
- Corium retention to retain corium in the RPV and keep the reactor vessel intact;
- Hydrogen control to prevent containment failure caused by hydrogen risk;
- Containment pressure control strategies (EHR [CHRS] and EUF [CFES]) to keep the containment pressure lower than the design pressure;
- Limiting and monitoring the radioactive release to the environment.

137. Lower level safety functions that sit below these safety functions are also identified. The structure of Ref. 29 generally takes the form of identification of indications that prompt the operator to take action, any manual actuation of the related safety features and how the related parameters are monitored.

138. My assessment has found that description of the safety functions is at a high level and the reasoning or details of fault analysis used to derive the safety functions is not included. Whilst I am content that the safety functions are adequately represented in the deterministic analysis, this presents a minor shortfall against my expectations for EKP.4 as there is no visible link between the analysis and the safety function.

139. In my opinion, there is a lack of narrative and reasoning for the further breakdown of safety functions and it is difficult to judge whether the functional breakdown is comprehensive. I consider that this lack of narrative presents a minor shortfall against my expectation that the safety case should be intelligible (NS-TAST-GD-051, paragraph 5.61 (Ref. 4)).

140. Nevertheless, I have assessed the comprehensiveness of Ref. 29 against my knowledge of the system and have found that the appropriate safety functions have been identified, and that they have been broken down to a level in which they can be assigned to an SSC. I am therefore satisfied that at a high level the expectations of NS-TAST-GD-094 (section 5.4 of Ref. 4), SAPs EKP.4 and EKP.5 (Ref. 2) have been met.

141. In terms of traceability of the safety functions to the engineering requirements, the interface between Ref. 29, the system design manual (Refs 70 to 75) and the design specification of the KDA [SA I&C] (Refs 87 and 88) is not described and it is difficult to understand how the safety functions listed are provided by the design. Using my knowledge of the safety case, I sampled the design specification and the system requirements specification of the KDA [SA I&C] (Refs 87 and 88). In the majority of

cases, I have found that the safety functions described in Ref. 29 assigned as requirements to the KDA [SA I&C] in Refs 87 and 88. However, safety functions described in Ref. 29 related to the opening of EHR [CHRS] spray and active injection lines are reallocated to a different C&I platform within Refs 87 and 88. Whilst I consider that this is convoluted, the link is traceable with wider knowledge of the safety case.

142. Traceability and management of the functional requirements is covered by the cross-cutting assessment (Ref. 89). However, I have identified traceability of requirements through to engineering requirements in the safety case as a minor shortfall against the expectations of SAP SC.2, in that, the safety case documentation should be clear and logically structured so that the information is easily accessible to those who need to use it.

4.3.3.2 In-Vessel Retention Safety Functions

143. Ref. 30 presents the breakdown of safety functions assigned to the IVR sub-system. The IVR sub-system is part of the EHR [CHRS] however in Ref. 30 the RP has considered it separately to demonstrate a logical breakdown of severe accident management strategies to safety functions (see Table 2).

144. Ref. 30 breaks down the levels of safety functions in a sensible way, progressively becoming more detailed. However, there is a general inconsistency in the level of detail provided in the safety functions when compared to the KDA [SA I&C]. For example, the IVR safety functions identify flow rates (Ref. 30), whereas for KDA [SA I&C] (Ref. 27) only the signals are identified without details of a detection range or how it is linked to expected severe accident conditions. The inconsistency and lack of reasoning presents a minor shortfall in my expectations for a safety case, in that, I expect that the safety case documentation should be clear and logically structured so that the information is easily accessible to those who need to use it (SAP SC.2 Ref. 2).

145. Notwithstanding this, I judge that the important actions related to severe accidents management that have been identified are consistent with the assumptions made. Based on this, and my assessment of the deterministic analysis (see sub-section 4.5) I am therefore satisfied that the RP has demonstrated an adequate link between the severe accident analysis, the safety functions and the requirements of the IVR sub-system. I am therefore satisfied that the RP has met the expectations of SAP EKP.4, EKP.5 and FA.16 paragraph 672 (Ref. 2) for GDA.

146. In terms of traceability of the safety functions to the engineering requirements, visibility of the promulgation of the safety functional requirements to the more detailed design specification is not provided, nor is there a link to the system design manual of the EHR [CHRS] (Refs 48 to 53). As a result no further details of SSCs that provide the safety functions can be found without wider knowledge of the safety case. As I do have wider knowledge of the safety case, I sampled the EHR [CHRS] system design manual (Refs 48 to 53) and found that whilst there is no clear link between the safety functions derived in Ref. 29 and those listed in Ref. 35, the safety functions are consistent and sub-system SSCs are assigned to perform the identified safety functions. Moreover, the same “safety functional requirements codes” also appear in Ref. 27.

4.3.4 Strengths

147. Using an unmitigated sequence, the RP has demonstrated the appropriate phenomena are understood and that the mitigation strategies have been assigned appropriately, meeting my expectations for FA.15 and SSG-2 (Ref. 6).

148. I am satisfied that the RP has identified appropriate safety functions and has identified appropriate safety features to perform those functions. I am also satisfied that the

safety functions derived are consistent with the analysis. With this in mind I am content that the expectations of EKP.4, EKP.5 and FA.16 have been met.

4.3.5 Outcomes

149. I have identified five minor shortfalls related to the identification of severe accident mitigation strategies and safety functions.

150. These relate to the intelligibility of the RP's safety case and the traceability between the analysis, safety functions and engineering requirements.

4.3.6 Conclusions

151. I am satisfied that the RP has adequately identified safety functions that maintain the appropriate fundamental safety functions for severe accidents. From my sampling of the KDA [SA I&C] system and IVR sub-system I am satisfied that relevant safety functions have been identified and that these have been linked to safety features (SSCs) that will deliver them. However, the safety case could be improved if the future licensee developed the traceability further.

4.4 Assessment of the RP's Identification of Severe Accident Scenarios

152. It is my expectation that the severe accident safety features are designed to mitigate or prevent possible severe accident phenomena. It also my expectation that deterministic analysis is performed to inform the design of safety features using appropriate severe accident sequences. In order to come to my judgement that the RP has identified an appropriate list of severe accident scenarios to demonstrate the effectiveness of the safety features, I have applied the general expectations of SAPs FA.2, FA.3, FA.15, FA.16 and FA.25 (Ref. 2). I have also applied the expectation detailed in IAEA SSG-2 (Ref. 6) relating to identification of design extension conditions with core melt.

153. From the PSA, there are many low probability sequences which can lead to a severe accident scenario. Rather than analyse every sequence that leads to core melt, the RP has chosen to reduce this to a more manageable list. This is normal practice for deterministic analysis. The RP has identified a short list of five scenarios for severe accident analysis.

154. From a large list of core damage sequences output from the Level 1 PSA, supplemented by deterministic judgement, the RP has derived a short list of severe accident scenarios that can be used to demonstrate the effectiveness of the safety features. This short list is intended to capture all of the main phenomena and limiting conditions during a severe accident. Different severe accidents present different levels of challenge to the provided suite of safety features, and some may represent a large challenge to one safety feature but not another. For example, the LB-LOCA is challenging for containment overpressure and therefore the EHR [CHRS], but it is not challenging for the SADVs as the primary circuit depressurises as part of the accident.

155. For each safety feature, the RP has selected multiple scenarios to analyse in order to demonstrate its effectiveness. This is done to ensure that the effectiveness of the safety feature is demonstrated using the most limiting conditions. This process is described further in sub-section 4.4.1.

156. As stated previously, the RP first identifies the phenomena which are to be prevented (sub-section 4.2) and the safety features to provide severe accident mitigation (sub-section 4.3) prior to identifying the most challenging scenarios for these safety features. In this section, I present a summary of my assessment of the process by which the RP identifies the severe accident scenarios (Refs 25 and 26) which it uses to demonstrate the effectiveness of the severe accident safety features.

4.4.1 Assessment

157. The RP's process for the identification of severe accident scenarios (Ref. 25) can be summarised as follows:

- The RP has used the Level 1 PSA to derive an initial list of core damage sequences.
- This list is then supplemented if any types of faults not similar to those already identified have been missed from the list.
- From this list, using engineering judgement, the RP has selected those sequences which pose the largest challenge to the safety features.

158. The RP has made extensive use of the output of Level 1 PSAs for reactor internal events (Ref. 24) to identify scenarios for the demonstration of the effectiveness of the UK HPR1000 severe accident safety features. The adequacy of the Level 1 PSA for internal events has been considered in ONR's PSA assessment report (Ref. 9), and I am content that it is suitable for use for the derivation of sequences to be considered in the Severe Accident Analysis topic area. The use of the PSA to identify faults and consider the consequences for severe accidents is aligned with my expectations of FA.2, FA.3 and FA.25.

159. The methodology for identifying severe accident scenarios to be included in the RP's deterministic DEC-B analysis to demonstrate the effectiveness of the safety features is described in Ref. 25. It involves using the Level 1 PSA to identify sequences that lead to core damage states initiated from all Plant Operating States (POS) and then using deterministic and engineering judgement to derive a short list of severe accidents to be analysed. The RP's definition of the POS of the UK HPR1000 are described in Annex 3 of this report.

160. The process applies a probabilistic cut-off such that sequences that are in the top 95% of contributors to the core damage frequency (CDF) or sequences which have a contribution of greater than 1% are included in the initial list. The initial list is then reviewed using 'deterministic judgement' (rather than purely probabilistic means) to ensure that the list is comprehensive. The RP state that this is done because by using only the probabilistic cut off frequency some sequences may be lost on frequency alone. For example, loss of feedwater faults are backed up by ASG [EFWS], bleed and feed and the ASP [SPHRS]; the CDF is therefore very low and falls below the 1% contribution to the overall CDF and is also beyond the 95 percentile for CDF. However, the RP has added this fault to the list to ensure a wide range of fault types that progress in different ways is considered. Once this list is populated, by using grouping and bounding principles and engineering judgement described below, as stated previously, the list is finally condensed to five severe accidents.

161. The initial list of accident sequences for the reactor consists of 58 sequences which account for 95.15% of the CDF, with the lowest sequence frequency being 4.56×10^{-10} pa. The list is further condensed to a more manageable list by:

- Grouping sequences with similar progression and taking forward a sequence considering the most onerous conditions (for example, total loss of feedwater with failure of bleed and feed results in a core damage state both with or without successful reactor trip; the sequence without reactor trip is bounding and is therefore taken forwards).
- Grouping sequences with similar initiating events, and taking the most onerous initial conditions (for example, loss of feedwater at full power is more onerous than that at low power).
- Grouping sequences that are of a similar fault type (for example, for the purposes of demonstrating the effectiveness of the severe accident safety

features, loss of Residual Heat Removal (RHR) can be bound by Loss Of Main Feedwater (LOMFW) as they are both loss of heat removal faults)
- Excluding faults which are very fast and for which severe accident mitigation cannot be provided (e.g. RPV failure).
- Excluding faults for which the focus is on practical elimination of the sequence by prevention of severe accidents (the purpose of the population of the list is to test the effectiveness of the severe accident safety features, not prevention).

162. By applying the above process the following scenarios are identified by the RP, all from full power:

- Small Break LOCA (SB-LOCA)
- LOMFW with Anticipated Transient Without Scram (ATWS)
- Intermediate Break LOCA (IB-LOCA)
- Station Black Out (SBO)
- LB-LOCA

163. The RP excluded the following types of accidents from analysis of the effectiveness of the safety features (Ref. 26):

- Loss of RHR
- SG tube rupture (SGTR)
- Loss of cooling chain
- RPV rupture
- Interfacing System (IS) LOCA
- Steam Line Break (SLB)

164. Whilst Ref. 26 provides limited narrative on the first two grouping processes described in paragraph 161, the processes are traceable and relatively simple. However, the arguments for why certain fault types can be bounded by the final list of five accidents is difficult to follow, and requires an in depth knowledge of the plant systems in order to understand. I have therefore identified this as a minor shortfall related to clarity of the safety case. Nevertheless, I judge that the RP's methodology has resulted in a range of accidents that encompass the most challenging scenarios for the phenomena that should be practically eliminated. For example:

- An SBO results in high pressure and high temperature conditions in the RPV for which the SADV is required in order reduce the pressure such that if RPV failure were to occur HPME and DCH would be avoided. However, HPME and DCH are not of concern for the LB-LOCA, as the break itself depressurises the RCP [RCS].
- For high energy hydrogen combustion, it is more difficult to determine which scenario will result in the most onerous conditions. For example a fast depressurisation may result in large peak hydrogen concentrations which decrease relatively quickly as the hydrogen generation slows and gases mix, but a slow depressurisation may result in higher total mass of hydrogen generated. It is difficult to determine the most onerous accident conditions which will provide the largest challenge to the EUH [CCGCS] without analysing a range of accidents. However, the range of accidents chosen by the RP, from no break (the SBO), small break to large break, provide a reasonable range of accidents to be looked at in further detail.

165. Based on a similar logic to the examples I have provided above, the RP concludes by choosing, out of the five scenarios, which scenarios should be used to demonstrate the effectiveness of the severe accident safety features (Ref. 26). The scenarios presented are similar to those presented for previous GDAs, and cover two main accident types

provided as an example in IAEA SSG-2 (Ref. 6) (i.e. loss of cooling and loss of integrity of pressure boundaries, such as the primary circuit).

166. IAEA SSG-2, paragraphs 3.45 to 3.50 (Ref. 6) provide guidance on the expectations for the identification of design extension conditions with core melting. Based on this, it is my expectation that:

- A wide range of fault types should be considered in the analysis, and the most onerous of those fault types should be considered.
- It should be assumed that any SSCs that would act to prevent core melting would have failed.
- That sequences should not be dismissed on frequency alone.
- That a range of representative sequences should be analysed to identify the most severe plant parameters resulting from the phenomena associated with a severe accident.

167. In my opinion, the RP's process has met my expectations for the following reasons:

- The use of the Level 1 PSA, with a cut off frequency of around 4.56 x 10^{-10} pa means that a wide range of sequences have been included for consideration.
- As the PSA is focussed on failure sequences, the assumption related to failure of safety measures to prevent core melt is accounted for.
- The process of applying deterministic judgement to identify sequences below the cut off frequency has ensured that a wide range of fault types has been included.
- The final list of five scenarios covers all of the limiting conditions for the prevention of phenomena that should be practically eliminated.

168. However, the process of determining the limiting conditions excludes less onerous conditions that have the potential to occur and would require severe accident management. For example, performing the analysis in this way excludes accidents at shutdown which may inform the design of alarm setpoints that are not used for at-power accidents (e.g. the plant radiation monitoring system (KRT [PRMS]) used as a SAMG entry point when the reactor is not closed). I consider that these scenarios will need to be considered in order to inform the development of SAMGs. However, considerations like these are a matter for a future licensee.

169. In my opinion, the RP's process is reasonable, aligned with RGP and is sufficient for GDA.

4.4.2 Strengths

170. The RP has used its Level 1 PSA to derive design extension conditions specific to the UK HPR1000 to inform the design of its severe accident safety features. This is aligned with my general expectations for FA.2, FA.3, FA.15, FA.16 and FA.25 (Ref. 2).

171. The RP's identification process aligns well with the expectations set out in IAEA SSG-2 (Ref. 6) and I am satisfied that the final list of representative scenarios is appropriate to inform the design of the severe accidents safety features.

4.4.3 Outcomes

172. I have identified a minor shortfall related to the description of the application the RP's process to derive the representative severe accident scenarios (see sub-section 4.4.1).

4.4.4 Conclusion

173. Although the description of the application of the process is limited, I am satisfied that the RP has identified an appropriate shortlist of severe accidents to analyse the effectiveness of its chosen severe accident management strategies and that it has used appropriate methods to identify this list. This is consistent with relevant guidance and my expectations for GDA.

4.5 Assessment of the RP's DEC-B analyses

174. For a new reactor, it is my expectation that deterministic analysis is performed in order to inform the design and to demonstrate the effectiveness of the severe accident safety features. My judgements and general expectations for the deterministic analysis are informed by SAP FA.15, FA.16 (Ref. 2) and NS-TAST-GD-007 (Ref. 4). I have also applied the expectations of IAEA SSG-2 (Ref. 6) as RGP for deterministic analysis of severe accidents for PWRs.

175. As stated previously, the UK HPR1000 is an evolution of several previous generation reactors. The RP claims that it has taken learning from previous generations and sought to improve upon them (Ref. 79). The RP has briefly described the design process of the severe accident safety features within Ref. 3. The RP notes that an iterative cycle to optimise the design has been performed and that the purpose of the DEC-B deterministic analysis provided within the Severe Accident Analysis safety case is to demonstrate that the safety features are effective in preventing conditions that could challenge the containment.

176. To this end, the RP has submitted the following safety case submissions which contain this DEC-B analysis:

- Assessment of In-Vessel Retention Strategy (Ref. 35)
- Assessment of EUH [CCGCS] by Lumped Parameter Method (Ref. 36)
- Assessment of EUH [CCGCS] by Computational Fluid Dynamics Method (Ref. 90)
- Depressurisation Capacity Analysis of the SADV (Ref. 37)
- Assessment of EHR [CHRS] (Ref. 38)
- Assessment of EUF [CFES] (Ref. 39)

177. In addition, the RP has also submitted analyses to demonstrate that late reflooding of the reactor, i.e. after the onset of core melt, will not lead to re-criticality (Ref. 85). Whilst the success of the IVR strategy is not dependent on in-vessel injection, and therefore not credited in the demonstration of the effectiveness of IVR, it may be desirable to inject water to slow the progression of core melt or to enhance heat removal whilst in the IVR configuration. Whilst the analysis (Ref. 85) mainly provides a basis for future SAMGs, re-criticality may result in conditions that are inconsistent with the assumptions made in the RP's analysis. I have therefore considered it within this section.

178. In the RP's analysis of effectiveness of the safety features, the core degradation process is similar for all accidents. An understanding of the core degradation process as predicted by ASTEC is important in order to understand my assessment that follows. Because of this, I have presented a general description of the core degradation process which is applicable to all accidents analysed by the RP. Based on this and the structure of the RP's safety case I have therefore structured this sub-section into the following further sub-sections:

- General Description of the Core Degradation Process in the UK HPR1000
- Effectiveness of the IVR Strategy

- Hydrogen Management and the Effectiveness of the EUH [CCGCS]
- Effectiveness of the SADVs
- Effectiveness of the EHR [CHRS]
- Effectiveness of the EUF [CFES]
- Analysis of Re-Criticality

179. The majority of the analyses used to demonstrate the effectiveness of the safety features has been performed using the ASTEC code, which is a severe accident integral code (i.e. one that couples codes of different kinds in attempt to simulate the whole severe accident from initiating event to severe accident phenomena). Another major code used in the RP's safety case is the GASFLOW-MPI code, which is used to model localised phenomena that are not modelled in the ASTEC code. My assessment of verification and validation of these codes and other codes used in support of the Severe Accident Analysis safety case (such as MOPOL and JMCT) is presented in sub-section 4.6 of this report.

180. The RP has also performed sensitivity analysis to support its safety case claims related to IVR (Ref. 46) and hydrogen management (Ref. 47). My assessment of the sensitivity analysis is also summarised in sub-section 4.6 of this report.

181. The RP has also performed analysis on ex-vessel steam explosions (Ref. 91) to understand how severe accidents progress beyond RPV failure using the Institut de Radioprotection et de Sûreté Nucléaire's (IRSN) MC3D code (Ref. 44). As the RP's safety case is that ex-vessel steam explosions are practically eliminated (Ref. 3), I have chosen not to sample this analysis, nor the verification and validation that supports the MC3D code.

182. The DEC-B analyses have largely been performed using the "realistic" approach described in IAEA SSG-2 (Ref. 6), using best estimate calculations and best estimate input assumptions. As described in sub-section 4.4 the RP has chosen to analyse different severe accident scenarios dependent on the safety feature. Depending on which safety feature is of concern, the RP has modified the scenarios either to make the conditions more onerous for that particular safety feature or to demonstrate its effectiveness in isolation of other factors.

183. The RP has not credited non-permanent equipment to demonstrate the adequacy of the design of its safety features. That is to say that the RP's safety case aims to demonstrate that the permanent equipment used for severe accident mitigation can regain control of the safety functions before mobile equipment would be required, and can maintain control for a length of time that it is likely mobile equipment would be available to perform safety functions. However, for the analysis of the effectiveness of EUF [CFES] (which assumes EHR [CHRS] has failed), the RP assumes that mobile equipment is in place in a timely manner (see sub-section 4.5.6), which I judge is necessary for the analysis. I judge that this approach is aligned with the expectation of IAEA SSG-2 (Ref. 6).

184. As the IVR strategy is key to the RP's safety case claims, I chose to target my assessment on the RP's analysis which demonstrates the effectiveness of IVR. I have used two TSCs to assist my assessment of the UK HPR1000 IVR strategy. The main submissions which have informed my assessment in this sub-section (4.5) are Refs 15 and 20. The TSCs have performed independent analysis of the IVR strategy (Ref. 15), using the AC2 code package, and reviewed the verification and validation of the ASTEC code and sensitivity analysis performed by the RP (Ref. 20). In addition, due to the complexity of the calculations related to hydrogen management and the associated potential for early failure of the containment due to high energy hydrogen combustion, I have also chosen to target the analysis of the effectiveness of the EUH [CCGCS] (Refs 36 and 90).

4.5.1 General Description of the Core Degradation Process in the UK HPR1000

185. The RP has provided a comprehensive description of the core degradation and relocation process within Ref. 35 for each of the five DEC-B scenarios analysed for IVR. In this section, I have summarised the general core degradation and relocation process based on Ref. 35. Although Ref. 35 is specific to IVR, the description here is valid for all variations of the analysis of DEC-B scenarios performed by the RP.

186. In general, there are two main categories that severe accidents in a PWR can be placed into: those which are caused by a loss cooling to the core where the primary system is intact, and those which there is a loss of integrity of the primary circuit (IAEA SSG-2 paragraph 3.48 (Ref. 6)). In either case, the heat removal function is lost and the core heats up until it melts unless cooling is restored. For the UK HPR1000, the core degradation and relocation process is similar for both types of accidents. This is because for accidents in which the RCP [RCS] is intact, before the onset of core degradation, the SADVs are designed to depressurise the primary circuit. The opening of the SADVs has a similar effect to a LOCA and the accident progresses similarly to a LOCA thereafter.

187. The timing of the depressurisation of the primary circuit has a large bearing on the timing for core degradation. In the case of the LB-LOCA and IB-LOCA, the break is large enough to lead to depressurisation of the primary circuit, whereas for the SB-LOCA, LOMFW and SBO the opening of SADVs is required to depressurise the primary circuit. This is reflected in the RP's prediction of timing of corium relocation from the core region to the lower head (hemispherical shaped bottom of the RPV). For the LB-LOCA and IB-LOCA, the RP predicts corium relocation at approximately 1.25 - 1.3 hours. For the others, the RP predicts corium relocation between 4 and 5.5 hours.

188. During this core degradation process, it is necessary for the operator to start to open all four IVR valves and SADVs. As stated previously, the signal to begin these actions is when the 650 °C COT signal is reached. The IVR subsystem is designed to fill the reactor pit with water within 30 minutes of initiation, therefore the pit is filled with water by the time the corium relocates to the lower head, and begins to cool the outer surface of the RPV.

189. During the depressurisation (either through a break or opening of the SADVs), whilst the active systems that are designed to protect against loss of coolant (such as MHSI and LHSI) are assumed to fail, the accumulators, which are pressurised tanks filled with boronated water, passively inject water into the RCP [RCS] when the pressure in the accumulator is higher than the RCP [RCS]. The accumulators provide some delay to the core degradation process but the core degradation begins once this water has been depleted. As water inside the RPV is heated and evaporates, the amount of water in the core decreases and the core temperature rises further. At high temperatures, the steam starts to react with the zircaloy cladding in the core, generating hydrogen and heat. The heat from this reaction further exacerbates the core degradation and the Rod Cluster Control Assemblies (RCCAs), fuel cladding and fuel begin to melt and form a pool of corium in the core region. Eventually, the steam-zircaloy reaction is limited by either blockages in the core, depletion of not yet oxidised zircaloy or the evaporation of all water.

190. The steel structures within the core and those that surround the core (such as the 'core baffle') also begin to melt due to radiated heat, and some of this becomes part of the corium pool. As the corium pool is a concentrated heat source it melts parts of the core that it comes into contact with. It can move sideways or downwards. In the UK HPR1000 design, the downward relocation of corium is predicted to be slowed significantly by cooling provided by the water that remains in the lower head and a relatively thick steel plate which supports the core, called the Lower Support Plate

(LSP). The corium therefore moves sideways until it reaches the 'core barrel', which is a steel barrel structure that encases the core and core baffle. The core barrel melts on contact and the corium pours down the downcomer and relocates to the lower head. The size of the initial relocation is accident dependent, but in general, the RP's analysis demonstrates that accidents with an early and fast depressurisation (i.e. the LB-LOCA and IB-LOCA) result in a fast core heat up and most of the core melts early in the accident, leading to a large early relocation of corium to the lower head.

191. During relocation, the corium is assumed to fragment and disperse as it falls through the water in the lower head. Fragmentation of the corium increases the surface area and the heat transfer, resulting in solidification of part of the corium. In addition, any partially solidified corium that has formed a crust round the edge of the pool may relocate. In reality, therefore, a mix of solidus and liquidus materials may be relocated from the core region to the lower head. There are large uncertainties in calculations from the initiating event up to the point of corium relocation which have an effect on the composition (both the chemical and structural makeup) of the corium that results in the lower head. For this reason, predictions of the composition of the corium in the lower head are very complex and any precise predictions of the geometry and make-up of the corium in the lower head would have large uncertainties associated with them. Severe accident codes therefore aim to simplify the problem and in doing so apply conservatism.

192. The ASTEC code simplifies this problem by assuming that the corium initially forms a uniform pool with a uniform layer of debris on top. The corium pool consists of a mixture of oxides (such as zirconium oxide (ZrO_2), UO_2 and fission products) and non-oxidised light metals (such as zirconium and steel). The ASTEC code then assumes that these will separate and form layers based on density. There are two models within ASTEC to simulate this process, but the RP has chosen to use the simple separation model in which an oxide pool forms with a layer of light metal above (it is therefore sometimes referred to the two layer model). The oxide layer contains all of the fission products and generates heat, whereas the light metal layer contains only metals and does not generate heat (but does conduct heat).

193. In the ASTEC code, the corium pool may be so large that some of the internal structures of the RPV are submerged. These internal structures are melted and are added to the pool.

194. The ASTEC code models heat transfer within the oxide pool in the sideways, upwards and downwards directions. The heat transfer models simulate convective flow in which the hot corium rises, transfers heat to the metallic layer above, cools, and moves downwards in a cyclic nature due to natural convection. A large portion of the heat generated in the oxide layer is transferred in the upwards direction to the metallic layer which then transfers that heat to its surroundings. Just after relocation, water may still exist at the bottom of the RPV which then resides above the metal layer. The metal layer is initially cooled by this water which boils off. After all water has evaporated, the heat transfer of the metallic layer to its surroundings is mainly through conduction to inner surface of the RPV wall that it is in contact with. As the metallic layer does not generate its own heat and is simply a path for the heat generated in the oxide layer to the surroundings, the thickness of the metallic layer (in the vertical direction) is closely correlated to the heat flux to the RPV wall. So long as this heat transfer mechanism exists, the thicker the metallic layer, the lower the concentration of the heat and therefore heat flux. Conversely, the thinner the layer (up to a certain point), the higher the heat flux is. This effect is sometimes referred to as the focussing effect, and particularly relates to the scenario where there is a step change in heat flux to the RPV wall from the metallic layer than the heat flux from the oxide layer to the RPV wall.

195. The heat from both the metallic layer and the oxide layer is transferred through the RPV wall to the water in the ERVC channel. The inside wall of the steel is ablated (by melting) until a heat balance between the input from the corium pool is balanced by the heat removed from the outside wall of the RPV. The ablated steel is added to the corium pool, increasing the thickness of the metallic layer and decreasing the focussing effect significantly. Eventually, an equilibrium is reached (before the RPV wall thickness is consumed) where no further ablation occurs.

196. In this configuration the RP claims that system is stable and can be cooled in the long term.

4.5.2 Effectiveness of the IVR Strategy

197. The UK HPR1000 IVR system is designed such that the conditions in which ex-vessel steam explosions or MCCI could occur are prevented. This is achieved by maintaining the structural integrity of the RPV throughout the severe accident thereby ensuring corium is retained within the RPV and cannot interact with water or concrete in the reactor pit.

198. The RP has performed deterministic analysis, supplemented by Monte-Carlo calculations, to demonstrate that the IVR strategy is successful in retaining corium within the RPV, thereby preventing the conditions that could lead to a potential ex-vessel steam explosions or MCCI.

199. Ref. 35 describes the RP's methodology for assessing the effectiveness of the IVR strategy. The RP's safety arguments are that, so long as the CHF on the outer RPV wall is not reached and that there is sufficient thickness of the RPV to support the internal loads, then IVR is effective and the corium will be successfully retained within the RPV.

200. There are three types of analysis that support the RP's demonstration of the effectiveness of IVR:

- Deterministic analysis performed using ASTEC – The RP has performed analysis of all five DEC-B scenarios identified in sub-section 4.4. The analysis models the initiating event, the core melting, relocation to the lower head and heat removal via IVR. The aim of the analysis is to demonstrate that CHF is not reached by making comparisons of the predicted heat fluxes to experimental values (measured at the REVECT-II facility) and to calculate parameters required for more specialised codes.
- Monte-Carlo analysis performed using MOPOL – This analysis takes some of the parameters output from the ASTEC calculations and performs steady-state heat transfer calculations using 10,000 random parameter combinations. The output is 10,000 heat flux curves which are compared to experimental values (measured at the REVECT-II facility) to demonstrate that the heat flux remains below the CHF.
- Structural integrity analysis of the RPV using ANSYS – The analysis takes some of the parameters output from the ASTEC calculations to perform further calculations to determine whether the RPV maintains its mechanical strength throughout the severe accident.

201. Although ASTEC alone can provide a prediction of whether CHF is reached and whether the RPV will maintain sufficient mechanical strength, the RP claims that the MOPOL and structural integrity analysis are also key arguments and evidence to underpin the claim that IVR is effective. Therefore my judgement on whether IVR is effective cannot be made without considering all three legs of the RP's arguments. I have therefore structured the remainder of this section (sub-section 4.5.2) as follows:

- Assessment of deterministic analysis using the ASTEC code – I summarise my assessment of the RP's modelling of various severe accident scenarios using the ASTEC code. I also summarise the insights gained from the TSC analysis (Ref. 15) which applies to all analyses performed in ASTEC. I conclude on whether the analysis has been performed adequately in support of the demonstration that CHF is not reached and whether it forms a suitable input to the uncertainty and structural integrity analyses.
- Assessment of the RP's statistical uncertainty analysis – I summarise my assessment of the RP's MOPOL analysis, and conclude on whether the RP has adequately demonstrated that CHF will not be reached.
- Assessment of the RP's structural integrity analysis – I summarise my assessment of the evidence to underpin the claim that thermal shock will not result in failure of the RPV and that adequate mechanical strength remains throughout the implementation of IVR.
- Conclusions related to IVR – Only with the three above legs of the RP's arguments can a conclusion as to whether IVR is effective can be made. In this section, I summarise my conclusions.

4.5.2.1 Assessment of Deterministic Analyses using the ASTEC Code

202. As an output of the severe accident scenario identification process (see sub-section 4.4), the RP has identified five severe accident scenarios in order to demonstrate the effectiveness of the IVR system. These accident scenarios are as follows:

- LB-LOCA
- IB-LOCA
- SB-LOCA
- ATWS (LOMFW)
- SBO

203. The chosen scenarios represent a range of conditions at both high and low pressures. For IVR, the RP claims that the LB-LOCA is the most limiting accident, and that the others have been performed as sensitivity studies. In my opinion, due to the large uncertainties in the initial progression of severe accidents and competing phenomena, it is not always intuitive which scenario will result in the most limiting conditions during severe accidents. I therefore judge that the RP's approach of analysing a range of scenarios is appropriate.

204. As the LB-LOCA (which is a double-ended guillotine break of the cold leg) and the SBO present the fastest and slowest progressing accidents, respectively, I chose to sample the analyses of these accidents. I also chose to sample the IB-LOCA, as it presents a slower and less severe version of the LB-LOCA.

205. As stated previously, for each scenario listed above, the RP judges whether CHF is reached by making a comparison of the predicted heat flux to measurements made in the REVECT-II experimental facility (Ref. 92). The REVECT-II facility enables measurement of the CHF along a prototype of the HPR1000 hemispherical RPV lower head (Ref. 92). The measurement from the REVECT-II can be used to derive a polynomial curve of CHF as a function of angle. In the below image, I have provided an example of a typical CHF curve that is derived from measurements at a facility such as the REVECT-II facility. The CHF increases with angle due to the differences in flow and buoyancy effects at different angles. The outputs of the ASTEC and MOPOL codes are heat fluxes which are dependent on angle. The curves can be compared to the experimental CHF value. Below I have also provided an example of a curve of the heat flux that may be output from the ASTEC code.

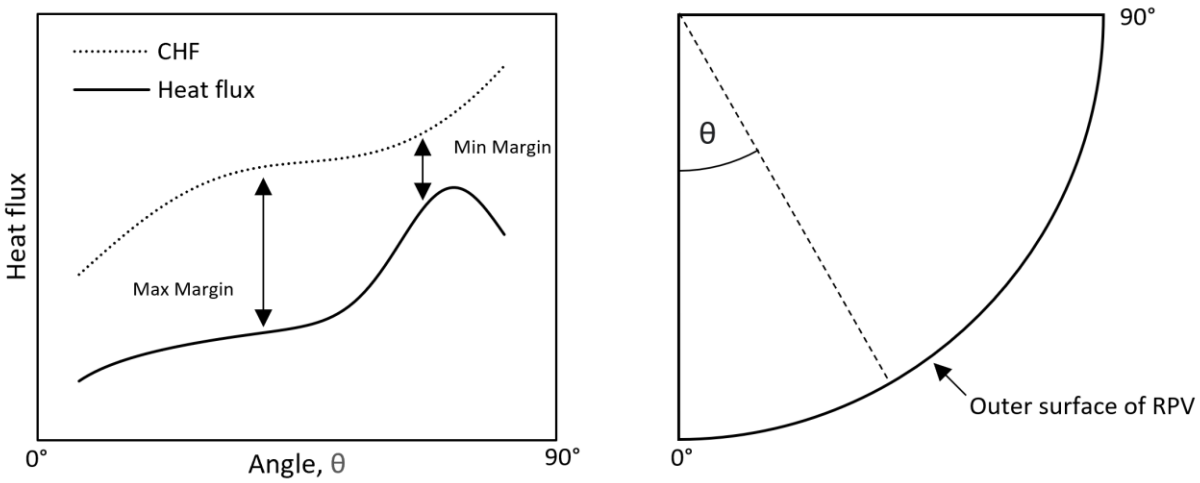

Figure 3: left – an example heat flux curve calculated in ASTEC and a CHF curve; right – a representation of the lower head.

206. The curves presented above are representative examples and are not taken from the RP's safety case. In the example, it can be seen that the point of minimum margin sits just left of the peak of the heat flux calculated, demonstrating that the peak heat flux does not necessarily represent the point at which there is lowest margin to CHF. The height of the corium pool and the thickness of the oxide and metallic layers affects where this peak is. The smaller the pool height, the lower the angle this peak will occur at. The RP provides its results for margin to CHF in a similar way to the above example, and specific numbers for margin are not provided.

207. Whilst I have assessed the RP's analysis of the severe accident scenarios individually, I have also assessed general methodology of the ASTEC analysis and modelling of IVR. My assessment of the RP's general methodology and analysis of IVR has been informed by my TSC's independent analysis (Ref. 15). In addition, my TSC's analysis has also provided insights into the design. The insights gained from my TSC's analysis apply to all severe accident scenarios, and as such my conclusions on the adequacy of the ASTEC analysis are dependent on these. With this in mind, I have structured the remainder of this sub-section (sub-section 4.5.2.1) into:

- Analysis of the LB-LOCA, IB-LOCA and SBO – The adequacy of the assumptions made in the analysis and the conclusions that can be drawn from the ASTEC analysis.
- Insights gained from the TSC analysis – insights into the methodologies and analysis, and the UK HPR1000 design which I have gained from the independent analysis.
- Conclusions related to the ASTEC analysis which supports the substantiation of the IVR design

Analysis of the LB-LOCA

208. It is important to note that the safety measures provided to protect against design basis faults must be assumed to fail in order to reach conditions for a core melt scenario to occur in the analysis. For the design basis LB-LOCA, the MHSI, LHSI and accumulators provide design basis protection. The DEC-B analysis therefore assumes that MHSI and LHSI have failed, which I judge is appropriate given that these systems would prevent core melt. This approach is aligned with the expectations of IAEA SSG-2 (Ref. 6). As described previously, the accumulators are passive and they are assumed to work correctly. The accumulators are designed for short term refilling of the core prior to the initiation of active safety injection in LB-LOCAs, however they cannot alone prevent a core melt scenario. I judge that the assumption that the

accumulators work is realistic, effects the progression of the severe accident, and is therefore appropriate, meeting my expectation that a realistic approach is taken where possible (SAPs FA.15 and FA.16 (Ref. 2)).

209. In addition to the failure of the MHSI and LHSI, the RP also assumes that all secondary cooldown (ASG [EFWS], ASP [SPHRS], VDA [ASDS]) fails. This has the effect of making the accident slightly faster. The containment spray is also assumed to fail which penalises heat removal from the core. Both of these assumptions result in a greater heat load for the IVR system to remove, and I judge that they are appropriately conservative.

210. The SBO generators are assumed to successfully start up when required. The SBO generators provide power for cooling to the IVR sub-system and the active flow to the reactor pit once the IVR tank is depleted (after 10 hours). I judge that this is appropriate and is similar to what is assumed for the severe accident analysis of other reactors for GDA.

211. Ref. 35 provides a detailed description of the progression of the LB-LOCA as calculated using the ASTEC code. The depressurisation due to the LB-LOCA leads to a fast uncovery of the core at around 0.7 seconds. Steam in the core becomes super-heated and the 650 °C COT signal is reached at ~347 seconds.

212. The analysis assumes that there is a 30-minute delay time between the COT signal and operator actions to open all four IVR valves. The 30-minute delay, along with an approximate 30-minute filling time after initiation, means that the RP predicts that the reactor pit is filled with water at 4159 seconds after the initiating event. The analysis also predicts that the corium is relocated to the lower head at 4,289 seconds, which is only 130 seconds after filling the pit.

213. One objective of the RP's safety case is to demonstrate that the reactor pit is filled with water prior to relocation of corium, so that the IVR system is ready to remove heat as soon as corium is relocated. In my opinion, these calculations therefore demonstrate that there is very limited margin for error when considering the 30-minute delay already assumed (4289 – 4159 = 130 seconds). The total available time predicted by the ASTEC analysis for operator action is approximately 32 minutes in order to ensure the reactor pit is filled before corium relocation occurs. This has led to design modifications to reduce the number of actions required for IVR initiation, referred to as design modification M63 by the RP (Ref. 93). My assessment related to this specific topic is presented in sub-section 4.7 of this report.

214. In the RP's analysis (Ref. 35), following the core barrel melt, the large corium pool in the core region relocates to the lower head sideways, down the downcomer. The corium has a peak decay heat of 24.24 MW just after relocation. The maximum heat flux calculated for the LB-LOCA using the ASTEC code for each point along the RPV wall is presented in Ref. 35. The maximum heat fluxes occur around the boundary between the metallic and oxide layers and are calculated at the worst point in time during the accident as approximately 905 kW m^{-2}. As stated previously, the margin is angle dependent, but is approximately 400-500 kW m^{-2} around the peak of the heat flux (see F-8-15 of Ref. 35). In my opinion, the margin to CHF appears reasonable.

215. After around 11,000 seconds, no more of the steel of the RPV is ablated and the minimum calculated residual thickness is 4.15 cm. The RP claims that this is acceptable as it is above the minimum thickness used in the structural integrity analysis (see sub-section 4.5.2.3).

216. The RP claims that the analysis demonstrates that CHF is not reached and that adequate thickness of the RPV is available to maintain the structural integrity of the

RPV. The RP appears to have applied appropriate assumptions in its analysis of the LB-LOCA and the results appear reasonable, with an adequate margin to CHF and a minimum thickness which is greater than that used in the structural integrity analysis. The results also appear to form a reasonable input to the MOPOL and structural integrity analysis. I judge that the results provide confidence that the IVR system of the UK HPR1000 are sized adequately to retain corium within the RPV during the LB-LOCA. However, for the reasons described in paragraphs 201, 203 and 207, my judgement of the adequacy of the ASTEC analysis, or indeed the adequacy of IVR, cannot be based solely on the ASTEC analysis LB-LOCA.

Analysis of the IB-LOCA

217. Ref. 35 presents the RP's analysis of the IB-LOCA. The same assumptions related to availability of safety systems as the LB-LOCA have been applied. Since the IB-LOCA progresses in a similar manner to the LB-LOCA, but at a slower pace, I judge that using the same assumptions is appropriate.

218. The RP's analysis shows that the blowdown phase is slower in the IB-LOCA case than the LB-LOCA case. The 650 °C SAMG entry criterion is reached at 930 seconds, and the relocation to the lower head occurs at 5,446 seconds. In my opinion, the analysis therefore demonstrates that there is sufficient time to account for a delay in operator actions and to fill the reactor pit.

219. In a similar manner to the LB-LOCA, the corium melts the core barrel and relocates to the lower head sideways, down the downcomer. The corium has a peak decay heat of 22.84 MW just after relocation. The slightly lower decay heat is due to the slower pace of the IB-LOCA, allowing the decay heat to reduce prior to relocation.

220. The maximum heat flux calculated for the IB-LOCA using the ASTEC code for each point along the RPV wall is presented in Ref. 35. The maximum heat fluxes occur around the boundary between the metallic and ceramic layers and are calculated at the worst point in time during the accident as approximately 886 kW m^{-2}. The margin is approximately 400-500 kW m^{-2} around the peak of the heat flux (see F-8-45 of Ref. 35). The decay heat and margin is comparable to the LB-LOCA. I judge that since the IB-LOCA progresses in a similar way to the LB-LOCA, the analysis results are reasonable and sufficient margin to CHF exists (specifically for the IB-LOCA).

221. After around 13,000 seconds, no more of the steel of the RPV is ablated and the minimum calculated residual thickness is 4.15 cm, which the RP claims is acceptable as it is above the minimum thickness used in the mechanical analysis (see sub-section 4.5.2.3)

222. The RP claims that the analysis demonstrates that CHF is not reached and that adequate thickness of the RPV is available to maintain the structural integrity of the RPV. The RP appears to have applied appropriate assumptions in its analysis of the IB-LOCA and the results appear reasonable, with an adequate margin to CHF and a minimum thickness which is greater than that used in the structural integrity analysis. The results also appear to form a reasonable input to the MOPOL and structural integrity analysis. I judge that the results provide confidence that the IVR system of the UK HPR1000 are sized adequately to retain corium within the RPV during the IB-LOCA. However, for the reasons described in paragraphs 201, 203 and 207, my judgement of the adequacy of the ASTEC analysis, or indeed the adequacy of IVR, cannot be based solely on the ASTEC analysis IB-LOCA.

Analysis of the SBO

223. The RP defines an SBO as loss of offsite power with the additional failure of the EDGs. In a loss of off-site power, the main goal is to reduce the pressure and temperature of the primary circuit. This is normally achieved by the F-SC1 ASG [EFWS] and VDA [ASDS]. However, in the SBO the ASG [EFWS] is assumed to fail as the EDGs also fail. The diverse F-SC2 back up, feed and bleed of the primary circuit, also protects against this fault; this can be powered by the SBO generators and is also assumed to fail.

224. In addition to these two lines of protection, the RP also assumes that the F-SC3 ASP [SPHRS] fails. The ASP [SPHRS] is designed to start automatically and is battery backed for up to 24 hours. If the ASP [SPHRS] were assumed to be successful, this would significantly slow the accident progression and reduce the decay heat. I therefore consider the assumption of failure to be conservative.

225. Even with the assumed failure of the ASP [SPHRS], the accident progression in the SBO case is significantly slower than both the IB-LOCA and the LB-LOCA. Unlike the IB-LOCA and LB-LOCA the success of the IVR strategy is dependent on the manual depressurisation of the primary circuit. Whilst the 650 °C SAMG entry criterion is reached at 347 seconds in the LB-LOCA, the same point is reached at 9,549 seconds for the SBO. Unlike the IB-LOCA and LB-LOCA, which assume a 30-minute delay to operator action after the 650 °C COT signal is reached, the RP assumes that the operator acts immediately to depressurise the primary circuit by opening the SADVs. The RP argues that enough time is available prior to this point to diagnose the fault and determine a course of action. I judge that this is a reasonable assumption, given that the actions are carried out from the MCR and that approximately 2 hours and 40 minutes are available to diagnose and prepare.

226. After the depressurisation, the RP predicts that the core slumps to the lower head at 19,920 seconds with a decay heat of 19.14 MW and similar corium masses to the LB-LOCA and the IB-LOCA (Ref. 35). The maximum decay heat is approximately 80% of the LB-LOCA case, and because the corium masses and composition is similar, the spread of heat is similar, and the maximum heat flux is lower than the LB-LOCA case.

227. The maximum heat flux calculated for the SBO using the ASTEC code for each point along the RPV wall is presented in Ref. 35. The heat flux curve is similar to that of the IB-LOCA and LB-LOCA (Ref. 35), and the maximum heat fluxes occur around the boundary between the metallic and ceramic layers and are calculated at the worst point in time during the accident as approximately 739 kW m^{-2}. The margin is approximately 600-650 kW m^{-2} around the peak of the heat flux (see F-8-30 of Ref. 35). The margin is larger than that found for the IB-LOCA and LB-LOCA. I judge that this is a reasonable result as the SBO is much slower than IB-LOCA and LB-LOCA, with a lower associated decay heat.

228. After around 31,000 seconds, no more of the steel of the RPV is ablated and the minimum calculated residual thickness is 4.96 cm, which the RP claims is acceptable as it is above the minimum thickness used in the mechanical analysis (see sub-section 4.5.2.3)

229. The RP claims that the analysis demonstrates that CHF is not reached and that adequate thickness of the RPV is available to maintain the structural integrity of the RPV. The RP appears to have applied appropriate assumptions in its analysis of the SBO and the results appear reasonable, with an adequate margin to CHF and a minimum thickness which is greater than that used in the structural integrity analysis. The results also appear to form a reasonable input to the MOPOL and structural integrity analysis. I judge that the results provide confidence that the IVR system of the

UK HPR1000 are sized adequately to retain corium within the RPV during the SBO. However, for the reasons described in paragraphs 201, 203 and 207, my judgement of the adequacy of the ASTEC analysis, or indeed the adequacy of IVR, cannot be based solely on the ASTEC analysis SBO.

Insights Gained from the Independent Analysis of IVR

230. My TSC has performed independent analysis of the LB-LOCA, IB-LOCA and SBO (Ref. 15). In all cases, the progression of the accident prior to core degradation is similar with only small differences appearing in the timings of events in the simulation of the SBO due to differences in secondary cool down. Whilst it is recognised in the severe accident analysis community that there are large uncertainties in the core degradation process (Ref. 80), the independent analysis has provided me with confidence that the modelling of the accident progression from initiating event to core degradation has been performed adequately.

231. My TSC's analysis (Ref. 15) predicted that for both the IB-LOCA and SBO the reactor pit will be filled prior to relocation of corium to the lower head. For the LB-LOCA, my TSC's analysis predicted that the reactor pit is only partially full when corium is relocated. However, the analysis also demonstrates that the channel can effectively remove heat in this configuration until the channel is completely filled, which provides me with confidence that there are no cliff-edge effects are associated with relocation of the corium to the lower head prior to filling of the reactor pit.

232. My TSC's analysis (Ref. 15) predicts that natural circulation will establish in the ERVC following the filling of the reactor pit, and that the heat removal capacity is similar to that predicted by the RP. Both analyses predict filling of the reactor pit in similar times, that the IVR tank will deplete at approximately 10 hours and that active injection rate of 40m^3 per hour is sufficient to remove the required heat in the long term. This provides me with confidence that the related safety functions will be met.

233. For all analyses, although the predicted decay heat that is relocated to the lower head is similar to that predicted in the RP's analysis, the independent analysis predicts maximum heat fluxes of approximately 1600 kW m^{-2} in the metallic layer region for the worse point in time (Ref. 15). This value exceeds the CHF correlation measured at the RP's REVECT-II facility (Ref. 92). However, there are significant differences in the codes and calculations which required further investigation.

234. Significant differences do arise between my TSC's analysis (Ref. 15) and the RP's analysis (Ref. 35) during and after the relocation phase of calculations. The following differences are of particular note:

- Relocation pathway - the RP's analysis predicts sideways relocation, whereas my TSC's analysis predicts downwards relocation.
- Corium temperature - the RP's analysis predicts corium temperatures 500 K lower than that predicted in my TSC's before and following relocation to the lower head.
- Decay heat distribution - The RP's analysis assumes that all decay heat is within the oxide layer, whereas my TSC's analysis assumes that 10% is generated within the metallic layer.
- Metallic masses - the RP's analysis predicts significantly higher steel masses than my TSC's analysis.

235. These key differences are applicable to all severe accident scenarios analysed and are discussed in further detail below.

236. With regards to differences in relocation pathways:

- The ASTEC code is capable of modelling both sideways relocation through the core barrel and downwards relocation through the LSP (Ref. 40). In my TSC's analysis, the AC2 code only assumes that downward relocation from failure of the LSP is possible (Refs 14 and 15). The differences in modelling approaches means that different relocation criteria are applied within the codes for when corium is relocated.
- Following an investigation using different methods than the AC2 code, my TSC found that the prediction of sideways relocation down the downcomer in the RP's analysis is the most likely relocation pathway. My TSC, therefore, attempted to modify its criteria for corium relocation in order to better replicate this behaviour and circumvent the limitation in the AC2 code (Ref. 14); however these differences could not be completely resolved and affect the timing of events and corium composition (Ref. 15).

237. With regards to differences in corium temperature:

- The main reasons for the differences are related to a user input of the solidus and liquidus corium temperatures. The RP has artificially reduced temperatures at which all of the corium mixture is a solid (solidus temperature) and a liquid (liquidus temperature). As the core melts, it can become hotter than its melting temperature, this is referred to as super heat. In the ASTEC analysis, the corium tends to lose most of its super heat and stays around the liquidus region. Therefore this assumption results in a lower temperature and a lower maximum heat flux. My TSC recommended that I seek justification for the liquidus and solidus temperatures used by the RP (Ref. 15). I am content with the RP's approach the following reasons:

  - In response to RQ-UKHPR1000-1763 (Ref. 81), the RP explained that for ASTEC, IRSN (the code developer) recommend that the solidus and liquidus temperatures should be artificially reduced in order to simulate a debris bed formed immediately after relocation. My TSC has not made the same assumption, and a debris bed is not predicted to form in my TSC's analysis. This recommendation has been reviewed by my other TSC as part of my assessment of the ASTEC code, and has been found to be a sensible recommendation (Ref. 20).
  - Also in response to RQ-UKHPR1000-1763 (Ref. 81), in my opinion, the RP provided sensible reasoning for why the difference in temperature would not on its own result in a significantly larger heat flux in the metallic region.
  - The RP has also provided sensitivity analyses (Ref. 46) which show that higher liquidus and solidus temperature actually result in less challenging conditions because the fuel melts at a higher temperature and less fuel relocates to the lower head, which results in a lower decay heat for the IVR sub-system to remove (see sub-section 4.6.1).

- The heat transfer mechanisms during relocation are also modelled differently in the ASTEC and AC2 codes. Whilst jet fragmentation is modelled in the ASTEC code, no such model is implemented in AC2. In ASTEC, when jet fragmentation occurs, heat loss is enhanced due to the increase surface area, some corium solidifies and a porous debris bed is initially formed on the upper surface of the corium pool. The surface area for heat transfer in the porous bed is significantly increased, resulting in a rapid transfer of the majority of the super heat stored in the corium. In the ASTEC calculation, this difference results in the fast evaporation of the water lying above the corium pool and may explain why the

heat balance appears to be reached significantly earlier. Moreover, the temperature is so high in the AC2 calculation that crust formation is not predicted to occur, further exacerbating the heat transfer to the RPV wall and the metallic layer. Whilst I have not assessed the jet fragmentation model, I am content that it aims to model realistic heat transfer and it has been developed as part of an international effort to validate the ASTEC code.

- The AC2 code does not account for the latent heat of melting of the structures in the lower head. This difference means that energy used to melt the structures in AC2 is not accounted for and the liquid temperature is higher. Again, I am content that the RP's approach aims to replicate realistic processes.

238. With regards to differences in decay heat distribution:

- My TSC's analysis assumes that 10% of the fission products remain within the metallic layer following phase separation. The simple separation model of the ASTEC code assumes that 0% decay heat remains.
- Whilst I judge that both approaches apply simplistic representations of the phase separation, I am content with the RP's approach as the RP has provided a sensitivity study, using a more sophisticated separation model, that demonstrates that even when much higher decay heats (>20%) are retained within the metallic layer there is still significant margin to the CHF (Ref. 46).

239. With regards to differences in light metallic masses:

- My TSC's work (Ref. 15) demonstrates that the difference in light metallic masses is the most significant difference in the two calculation approaches. As stated previously, the total light metal mass directly effects the heat flux conducted to the RPV wall.
- The ASTEC code is capable of modelling the melting of more internal structures than the AC2 code, such as the core barrel. In addition, due to modelling differences, my TSC allocated a lower decay heat to the outer sections of the core (Ref. 14). As a result, steel from the outer sections in the AC2 model takes longer to melt and is not relocated until later in the accident.
- This conservatism results in around 20 – 30% less melted steel mass predicted in the AC2 analysis (Ref. 15). The heat conducted to the RPV wall is therefore more focussed in my TSC's analysis (i.e. it is distributed over a smaller area in the metallic region), resulting in a higher heat flux in the metallic region.
- To investigate the sensitivity of the heat flux to the metallic mass, my TSC added 20 te of steel to the corium pool and found that the maximum heat flux in the metallic region reduced significantly to lower than 1,000 kW m^{-2} (Ref. 15). Therefore my TSC found that if the melt of the core barrel, the entirety of the flow distribution device and LSP were taken into account in its main calculations the calculated heat fluxes would be significantly lower.
- My TSC therefore concluded that, even if the other differences were not resolved, if the additional mass was available to melt then the CHF limit would likely not be exceeded in the AC2 calculation. Because of this, my TSC made the recommendation that I seek further justification that this steel will indeed melt in the progression of the accident.
- In response to RQ-UKHPR1000-1695 (Ref. 81), the RP provides supporting arguments for why the prediction of greater steel mass is reasonable in the ASTEC calculation. The RP's reasons relate to the relatively low elevation of the core barrel in comparison to previous generation PWRs, the relatively thick LSP, and the relatively thin structures that surround the core. The RP states that the ASTEC calculation simulates a pool which submerges the LSP, and this large structure provides a significant mass of steel. Moreover, the baffle and barrel are relatively thin and melt relatively quickly, and at least parts of

them must melt for the corium to relocate. I judge that the reasons are compelling and I am satisfied with the RP's arguments.

240. To summarise, although my TSC found that the CHF limit was reached, my TSC also concluded that it is most likely due to the differences in the metallic masses predicted to melt, and that if the AC2 code predicted similar masses to that in the ASTEC code, that CHF would not be reached. I am satisfied that this is likely to be attributable to differences in modelling approach and that the ASTEC code represents a more realistic modelling of the melting of the metallic structures. Moreover, I am content that the RP has provided adequate substantiation for the other, less important differences in corium relocation pathway, corium temperature and decay heat distribution.

241. With this in mind, the TSC's analysis has provided me with confidence that the RP's ASTEC analysis has been performed adequately, and also provides me with confidence that the UK HPR1000 IVR safety feature is adequately designed to mitigate the IB-LOCA, LB-LOCA and SBO DEC-B scenarios.

Conclusion related to the ASTEC analysis of IVR

242. The RP has performed analysis of the SB-LOCA, IB-LOCA, LB-LOCA, SBO and ATWS (LOMFW) DEC-B scenarios using the ASTEC code to support the claim that IVR is effective.

243. I have sampled the IB-LOCA, LB-LOCA, and SBO to gain confidence in the RP's analysis and the adequacy of the HPR1000 design. Informed by the TSC's independent analysis, I have found that the RP has performed the analysis adequately, that there is sufficient margin to CHF and that a sufficient residual thickness of the RPV exists for the DEC-B severe accident scenarios analysed. This provides me with confidence that no cliff-edge effects are associated with the DEC-B scenarios analysed and that the IVR strategy is adequately designed for the DEC-B scenarios analysed, which goes toward meeting my expectations for FA.16. In addition, I consider that the analysis forms a suitable basis for the MOPOL and structural integrity analyses (see sub-section 4.5.2.2 and 4.5.2.3).

244. However, as stated previously, to gain confidence in the overall adequacy of the design of the IVR strategy I have also assessed the RP's statistical uncertainty analysis (sub-section 4.5.2.2) and structural integrity analysis (sub-section 4.5.2.3).

4.5.2.2 Assessment of the RP's Statistical Uncertainty Analysis

245. The RP has performed a statistical uncertainty analysis of the heat flux using the steady state code MOPOL and presented the results in Ref. 35. The MOPOL analysis outputs thousands of angle dependent heat flux profiles, depending on randomly selected parameters. Any single calculation provides a heat flux profile similar to "Heat flux 1" or "Heat flux 2" in the below example plot (Figure 4).

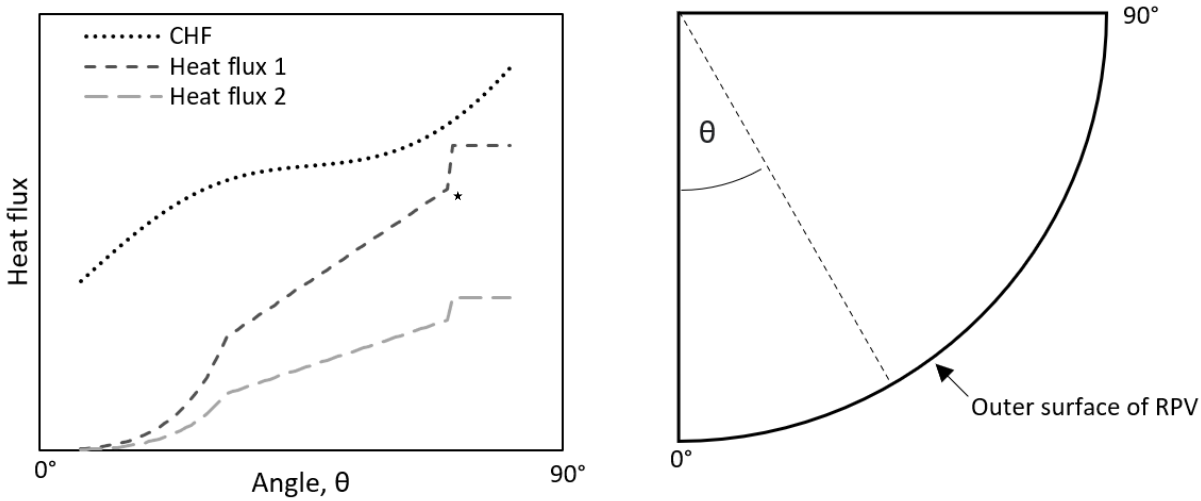

Figure 4: left – examples of heat flux curves calculated in MOPOL and a CHF curve; right – a representation of the lower head.

246. The plot presented is not based on the RP's data, and I have only included this for illustrative purposes. In the plot, the two heat flux profiles each represent one calculation performed by MOPOL. The star highlights the transition between the oxide layer and the metallic layer. In these examples, it can be seen that there is a strong focussing of the heat flux in the metallic layer, as there is a large jump between the layers. The result of the 10,000 calculations is a spread of these profiles.

247. In Ref. 3, the RP compares these profiles with the measured CHF correlation from the REVECT-II experiments (illustrated as the "CHF" curve above) (Ref. 92). The RP claims that this is supplementary analysis to provide additional confidence that the IVR strategy will be effective. The methodology is based on an approach developed for the AP600 reactor (Ref. 94). My assessment of the verification and validation of the MOPOL code is presented in sub-section 4.6.3.

248. The RP has applied the internationally recognised Risk Orientated Accident Assessment Methodology (ROAAM) (Ref. 94) to determine probability distribution functions of the decay heat, zirconium oxidation fraction and steel mass based on the deterministic analysis performed using the ASTEC code. The methodology involves using the Level 1 PSA and engineering judgement to derive simple probability distributions based on whether a given range is likely (10^{0}), unlikely (10^{-1}) or very unlikely (10^{-2}). For example, as there are significantly more sequences in the PSA that lead to slow core degradation than fast ones, the RP considers that the decay heat that is relocated to the lower head is more likely to be in the region of that predicted in the ASTEC calculations of SBO and SB-LOCA, rather than that for the LB-LOCA. It therefore assigns the decay heat that is in the region of that calculated for SBO and SB-LOCA as likely (10^{0}) and the decay heats in the region as those in the LB-LOCA as very unlikely (10^{-2}).

249. The analysis is performed using 10,000 combinations of parameters to understand the uncertainty in the calculations. Through the use of probability distributions, the calculations include unlikely combinations of parameters. For example, the unlikely combination of highest decay heat (normally associated with a very fast progressing severe accident) with high zirconium oxidation fraction (normally associated with slower accidents) is possible in the code. The RP claims that even in the most adverse combinations of parameters, the heat flux remains below the CHF correlation.

250. However, in my opinion, the RP has made several simplifying assumptions which have the potential to make the calculated heat flux less onerous. These are described below:

- The RP has assumed that the entire core barrel, core baffle, lower support plate and flow distribution device melts during the accident and bases the probability distributions on this assumption. Therefore, the minimum steel mass is 48 te. In Ref. 3 the RP provides arguments that the core barrel is supported by the LSP and once the LSP melts, the core barrel will fall into the molten pool. In my opinion, this is an over-simplistic view. I note, however, that the minimum steel mass of 48 te is still included as an input parameter (albeit at low frequency) and is significantly below the masses predicted by ASTEC, as the MOPOL code does not account for the large steel mass which is added through ablation of the RPV.
- The RP assumes that all fuel melts and is relocated to the lower head. The result is that the height of the oxide pool is similar in all calculations. The minimum margin is therefore always roughly at an angle close to where the star is on the above image (Figure 4). If the start were to move left in this plot there may be a smaller margin.
- The calculation is performed in the steady state and transient effects during phase separation cannot be observed. This is inherent in the code and is discussed in sub-sections 4.6.1.

251. Similar observations to the above have also been highlighted independently in my TSC's review of the MOPOL code and overall IVR methodologies (Refs 17 and 20), and by a TSC commissioned to support the Chemistry inspector's assessment of the methodologies for IVR (Ref. 95).

252. Whilst some of the observations made by the TSCs relate to the MOPOL code itself, all reviews conclude the shortfalls do not undermine the RP's safety case (Refs 17, 20 and 95). This is because the uncertainty analysis provides a supplementary argument to the ASTEC analysis that IVR will be effective.

253. Aligned with the expectations of FA.15, in general I consider that when realistic analysis cannot be performed with confidence, a conservative or bounding case approach should be adopted to avoid optimistic conclusions being drawn. The MOPOL analysis goes a long way to achieving this, and since the ASTEC analysis forms the main basis of the RP's evidence, I consider the points raised above only represent a minor shortfall against my expectations for FA.15.

254. Whilst I have identified a minor shortfall in the application of the MOPOL code, it should be noted that the RP's claims that IVR is effective are evidenced in the main part by the ASTEC analyses. Moreover, the RP has provided additional ASTEC analysis which allays my concerns with the use of the MOPOL code. I am therefore satisfied that the RP's uncertainty analysis provides sufficient additional confidence in the demonstration that the IVR subsystem is effective, by preventing conditions in which CHF could occur.

4.5.2.3 Assessment of Structural Integrity Analysis of the RPV during IVR condition

255. As stated previously, the RP aims to demonstrate that the integrity is maintained by preventing CHF and melt through of the RPV, and separately demonstrating that there is enough strength in the RPV wall to prevent mechanical failure. The RP has presented two acceptance criteria for the success of IVR which are related to the CHF and the mechanical strength of the RPV during the accident. The RP claims that the CHF is most limiting criterion. At Ref. 35, the RP compares the minimum thickness required to support the load of a relocated core and reactor internals for a yield

strength at 550 °C (0.3 mm), with the minimum required thickness to support the maximum experimental CHF value (8.5 mm). On this basis the RP determines that the most limiting criterion is the CHF. My TSC agreed with this reasoning (Ref. 20), but considered that it was overly simplistic and optimistic as it did not take in to account the transient nature of the material creep that occurs during implementation of IVR. My TSC, therefore, recommended that a finite element analysis should be performed using the minimum thickness of the RPV determined in the RP's sensitivity analyses (3 cm) (Ref. 46).

256. Independently of my TSC's recommendation described above, the RP has performed this finite element analysis of the mechanical strength of the RPV following relocation and during the implementation of IVR (Ref. 97). The RP claims that the RPV has sufficient mechanical strength to prevent failure throughout the DEC-B scenarios analysed. To substantiate this claim, the RP has used more sophisticated analysis (in respect to mechanical strength) than that possible in using the ASTEC code. The RP has performed two analyses important for the Severe Accident Analyses topic area and submitted the following:

- A thermal shock analysis of the RPV (Ref. 96) – The RP has analysed crack propagation that could lead to failure of the RPV when IVR is required (i.e. during a severe accident).
- A structural integrity analysis of the RPV (Ref. 97) – The RP has analysed the longer-term failure of the RPV after the wall has ablated (e.g. from creep failure).

257. Whilst the assessment of the analysis has been led by ONR's Structural Integrity inspector (Ref. 98) I have assessed whether the inputs from the severe accident analysis are appropriate.

258. Ref. 97 lists the conservative assumptions made in the analysis. The RP has used inputs from the ASTEC calculations to determine the temperature gradient over the RPV wall. As an initial condition, the RP assumes that steel over 600 °C does not provide any structural support and is not included in the calculation. This results in a thinner RPV wall than that calculated in the ASTEC analysis. For example, for the SBO, ASTEC calculates the minimum RPV thickness as 4.96 cm, however, the structural integrity analysis (Ref. 97) uses a thickness of 1.3 cm (RQ-UKHPR1000-1763 (Ref. 81)). The difference arises because the ASTEC code assumes that the steel provides some structural strength up to its melting point (which is in the range of 1300 to 1600 °C); although this strength is significantly reduced at higher temperatures. As my TSC made the recommendation that a value of 3 cm should be used, I am satisfied that the RP has met this recommendation by using a more conservative value of 1.3 cm.

259. In addition, the buoyancy effect due to the filled reactor pit is not accounted for in Ref. 97. Buoyancy counteracts the weight of the RPV and therefore accounting for it would provide additional margin to failure of the RPV. In addition, the heat flux used is higher than that calculated in the deterministic analysis (Ref. 35) and assumed to remain constant at a conservative value. The internal load and dead weight also appears to be conservative. Even with these conservatisms, the RP demonstrates that there is a margin to failure of the RPV during the IVR condition (Ref. 97).

260. Whilst the internal pressure and dead weight appears conservative for the situation of a dry RPV, it should be noted that the calculation is based on the assumption that no water is in the RPV. It is therefore not clear whether the analysis presented in Ref. 97 is bounding of a scenario where water has been injected following relocation. Since late reflooding will likely form part of the SAMGs I judge that the effect on the internal pressure (e.g. from a fast vaporisation of steam) and deadweight should be accounted

for in any supporting analysis. I therefore consider this a shortfall against the expectations of FA.16 as I consider that it does not enable a suitable basis for accident management. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0079 – The licensee shall determine whether reflooding following corium pool formation will challenge the structural integrity of the reactor pressure vessel. The potential impact of reflooding should be accounted for in the severe accident management guidelines.

261. In addition, the RP has submitted an analysis of thermal shock during the filling phase of IVR (Ref. 96). The analysis is akin to an analysis that the RP has performed at normal operating pressure and temperature (Ref. 99). This analysis (Ref. 99) provides substantiation for the claim that thermal shock will not lead to failure of the RPV during normal operations, at nominal pressure and temperature. The analysis (Ref. 99) was submitted as part of the RP's response to RO-UKHPR1000-0032 (Ref. 100), and is within the scope of ONR's Fault Studies (Ref. 10) and Structural Integrity (Ref. 98) assessments. The Structural Integrity assessment (Ref. 98) found that the analysis (Ref. 96) was adequate to demonstrate that the RPV would not fail due to thermal shock during normal operation, at nominal pressure and temperature. The initial conditions for the temperature of the lower head during severe accidents is slightly higher than that assumed for normal operation. However, the internal loads are significantly lower owing to the consequential or deliberate manual depressurisation of the reactor coolant system (RCP [RCS]) using the SADVs prior to flooding the reactor pit. Because the pressure is significantly lower than in normal operation, the margin to failure due to thermal shock is large.

262. In summary, in both Refs 96 and 97, the initial conditions appear to be conservative and I am satisfied that the severe accident analysis has been used appropriately as an input to these analyses where late reflooding is not considered. The Structural Integrity assessment (Ref. 98) has found that the analyses adequately demonstrate that a margin to failure exist in both the thermal shock analysis and the longer-term structural integrity analysis.

263. To conclude, in cognisance of the Structural Integrity assessment (Ref. 98) I am satisfied that from a Severe Accident Analysis point of view that the RP's analysis adequately demonstrates that thermal shock resulting in failure of the RPV will be avoided, and that the RPV will maintain adequate mechanical strength during IVR.

4.5.2.4 Conclusions Related to the Analysis of the Effectiveness of IVR

264. The RP's deterministic analysis using the ASTEC code (Ref. 35) has demonstrated that CHF will not be reached and that the minimum thickness calculated is sufficient to support the RPV.

265. The RP's deterministic analysis using the ASTEC code (Ref. 35) provides a suitable basis for the input to the uncertainty analyses using the MOPOL code, and the structural integrity analysis.

266. Despite the minor shortfall I have identified related to the uncertainty analysis performed using MOPOL (Ref. 35), I judge that it does still provide additional confidence that on a conservative basis an adequate margin to CHF still exists.

267. Based on ONR's Structural Integrity assessment (Ref. 98), I judge that the structural integrity analyses (Refs 96 and 97) support the RP's claim that the structural integrity of the RPV will be maintained during the DEC-B scenarios identified.

268. I have raised one Assessment Finding (AF-UKHPR1000-0079) related to structural integrity of the lower RPV following reflooding of the RPV during the IVR condition.

269. Overall, I am satisfied that the RP has demonstrated that the UK HPR1000 IVR strategy would be successful in maintaining RPV integrity for the DEC-B scenarios identified, and that, in the context of IVR, my expectations for SAP FA.15 and FA.16 have been met.

4.5.3 Hydrogen Management and the Effectiveness of the EUH [CCGCS]

270. As described in Section 3 of this report, a severe accident in a PWR has the potential to lead to conditions in which several processes can generate combustible gases. These processes are the oxidation of metals, radiolysis and MCCI (IAEA-TECDOC-1661, Ref. 6).

271. The RP claims that the EUH [CCGCS] is designed to reduce the concentration of these gases (Ref. 3). It consists of PARs and hydrogen monitors. Whilst not part of the EUH [CCGCS], the RP claims that the containment has been designed to enable combustible gas management.

272. The MCCI process generates combustible gases such as carbon monoxide and hydrogen. Since the UK HPR1000 is designed to prevent MCCI from occurring, even during severe accidents, I only refer to the management of hydrogen in this section.

273. The process for hydrogen generated as part of the steam-metal reaction (particularly the steam-zircaloy reaction) in the core is fast, and can result in large quantities of hydrogen within the containment in a short space of time. This can lead to an early failure of the containment (IAEA-TECDOC-1661, Ref. 6).

274. In the long term, slower processes for hydrogen generation that occur during an accident in a typical PWR, such as radiolysis and oxidation of structures within the containment, which can lead to hydrogen accumulation over time (IAEA-TECDOC-1661, Ref. 6). These processes can lead to a late failure of the containment.

275. Of these, the accidents with fast hydrogen generation rates (due to the steam-zircaloy reaction) which are sustained for a significant length of time are the most challenging (IAEA-TECDOC-1661, Ref. 6), as they can potentially lead to the generation of hundreds of kilograms of hydrogen present within the containment at a given time. The slower processes result in much lower masses of hydrogen at any point in time because the generation rate is more comparable to the recombination rate of the PARs.

276. These gases pose a risk of different combustion modes that can damage equipment in the containment and threaten the containment structures, resulting in an early or large release. It is an established international expectation that new reactors are designed to manage the risks from hydrogen generated in severe accidents, both in the long term and short term (Ref. 22).

277. In this report I refer to both local and global phenomena and effects. By global effects or phenomena, I mean those which involve phenomena throughout the majority of the containment, or the impact that a phenomenon can have on the containment as a whole. By local phenomena or effects, I mean those which are localised to a certain part or parts of the containment, and do not spread to the rest of the containment.

278. The RP claims that there are several combustion modes which can threaten the containment structures and the equipment within it during a severe accident:

- Global detonation – this is characterised by a supersonic propagation of a flame front and a large pressure wave that could threaten the containment and requires ignition directly leading to detonation (such as a spark). It is generally accepted that, for reactor containments, when the concentration is below 10% vol it is extremely unlikely that global detonation will occur (Ref. 80).
- Slow deflagration – this is characterised by laminar flow and is generally related to a localised burn (e.g. at a point of discharge of flammable gas). Surrounding structures or components can be threatened by direct contact with the flame, hot gases or heat radiation. If the flame propagates through the containment it can have a global effect on pressure.
- Fast deflagration – this is localised phenomenon characterised by turbulent flow with a flame that propagates at subsonic speeds. The properties of the flame can cause the flame front to propagate and can lead to large pressure waves locally and cause the global pressure to increase.
- Flame acceleration and Detonation to Deflagration Transition (DDT) – In the fast deflagration regime the propagation can transition to supersonic speeds resulting in detonation. This is a localised phenomenon. When the flame transitions to detonation it can cause a global overpressure. It is generally accepted that this is the most likely cause of a detonation in a PWR containment (Ref. 80).

279. The RP claims that the design of the EUH [CCGCS], including the layout and sizing of the PARs, is such that both global effects and localised effects are mitigated such that they do not lead to failure of the containment (Ref. 3).

280. Below, I have summarised the arguments which support this claim, which are substantiated through the deterministic analysis (Refs 36 and 90):

- The RP claims that the most limiting accidents and initial conditions have been identified and analysed using the ASTEC and GASFLOW-MPI codes.
- The RP has used the ASTEC code to (Ref. 36):
    - Calculate the progression of the entire severe accident
    - Demonstrate that the global hydrogen concentration remains below that which may result in a global detonation.
    - Demonstrate that the global pressure loads from slow deflagration are within acceptable limits.
    - Identify the most limiting local conditions, for which slow deflagration, fast deflagration, flame acceleration and DDT have the potential to occur as an input to the GASFLOW-MPI CFD code.
    - Calculate the mass and energy release of gases hydrogen, steam and water from the RPV into the containment, as a function of time, to use as an input into the GASFLOW-MPI calculation.
- The RP has used the GASFLOW-MPI code to demonstrate that localised phenomena will not challenge the UK HPR1000 containment. The RP argues that (Ref. 90):
    - The local heat loads from slow deflagration are within acceptable limits.
    - Pressure loads from fast deflagration are within acceptable limits.
    - Flame acceleration does not result in the deflagration to detonation transition.
- The RP has used the GASFLOW-MPI code to demonstrate that the EUH [CCGCS] and containment have been designed to optimise hydrogen management (Ref. 90).

281. As stated, the RP has performed its analysis using the ASTEC and GASFLOW-MPI codes. The ASTEC code's modelling of the thermal hydraulics in the containment is relatively simple in comparison to the GASFLOW-MPI code. However, the calculations of the accidents in a PWR containment using the GASFLOW-MPI code are computationally intensive. The RP has therefore used the ASTEC code to determine cases which may result in conditions that are limiting for local phenomena in order to reduce the number of accidents required for analysis to a more manageable list (Ref. 36).

282. Initially, several scenarios, using various initial conditions, have been analysed using the ASTEC code. From this analysis the global detonation risk and the challenge from the pressure load from slow deflagration has been determined by the RP. These analyses are also used to determine which scenarios have the potential to lead to localised phenomena and to understand the conditions that could lead to those phenomena (Ref. 36). The RP has then taken the most limiting cases in terms of potential for localised phenomena and performed more sophisticated calculations, using the CFD code GASFLOW-MPI and the boundary conditions from the ASTEC analysis, to determine whether fast deflagration, flame acceleration and DDT can be avoided (Ref. 90).

283. The RP use several criteria for determining the risk of flammability (Ref. 36), flame acceleration and DDT (Ref 90). These criteria relate to the Shapiro diagram, Sigma and Lambda criteria, respectively. As confirmed by my TSC (Ref. 20), these criteria are well established. Moreover, these criteria have also been applied in previous GDAs. I am therefore satisfied with the use of these criteria for these analyses.

284. Ultimately, if the RP determines that the phenomena can occur, the RP uses acceptance criteria related to containment pressure and containment liner temperatures to determine whether the observed phenomena will challenge the containment. The pressure limit is based on the severe accident design basis pressure curves, discussed in sub-section 4.7. The temperature limit of the liner is determined by a simple calculation related to the saturation temperature at the design pressure of the containment (which is roughly 154 °C), and does not relate to the actual material properties of the liner.

285. The RP has also presented additional best estimate analyses (Ref. 90) that support the claim that the most limiting case (in terms of localised effects) has been analysed. Further sensitivity analyses related to uncertainties are also included in Ref. 47. My assessment of the methodologies and the sensitivity analyses are presented in sub-section 4.6.

286. The RP claims that all of the aspects listed paragraph 280 are important for the demonstration that the EUH [CCGCS] is effective. Therefore, a conclusion regarding the design of the EUH cannot be made on any of these aspects in isolation. In the following subsections, I summarise my assessment of the evidence that underpins the RP's arguments, summarised in paragraph 280, in turn.

4.5.3.1 Identification of the Most Limiting Scenarios and Initial Conditions

287. It is my expectation that the limiting conditions expected during a postulated DEC-B scenario are used to demonstrate that the EUH [CCGCS] is effective in the management of hydrogen.

288. From the severe accident scenario selection process (see sub-section 4.4), the RP has selected the following DEC-B scenarios as a starting point for deriving the most limiting cases in demonstrating the effectiveness of the EUH [CCGCS]:

- SBO
- SB-LOCA
- IB-LOCA
- LB-LOCA

289. In my opinion, it is difficult to determine, using engineering judgement alone, which accidents will lead to the most limiting conditions for accident management. For example, an accident with a high depressurisation rate, which occurs early in the accident (for example, a LB-LOCA) may lead to an early overheating of the core and onset of the steam-zircaloy reaction, leading to large quantities of hydrogen generated in a short space of time. However, in an LB-LOCA, the steam-zircaloy reaction ends relatively early as the water and steam is depleted from the primary circuit. Conversely, in an SBO, it takes significantly longer for the core to get to temperatures at which steam-zircaloy reaction begins, and the reaction is prolonged as more water is available than in the LOCA. The longer period at which the steam-zircaloy reaction occurs during the SBO means that a larger mass of hydrogen than in the LB-LOCA case is generally expected to be generated. However, in the SBO, the reaction rate is slower than the LB-LOCA and therefore the local accumulation of hydrogen within compartments of the containment are generally less challenging as there is sufficient time for the hydrogen to mix with the larger containment space. Based on this, I judge that the RP's approach to analysing multiple accident types is appropriate.

290. Out of these four scenarios, the RP recognises that there are many different variations of these scenarios which lead to different conditions for hydrogen in the containment (Ref. 36). The RP therefore aims to refine these scenarios to determine the limiting conditions which could challenge the EUH [CCGCS] (Refs 36 and 47). The RP recognises that the worst conditions for a given aspect of management are dependent on four significant factors. From my assessment of the RP's analysis (Refs 36 and 47), I have observed that the following factors are of importance:

- Break location / discharge location – For all LOCAs, the location of the break effects whether hydrogen generated in the core accumulates in small, localised pockets in the containment, or whether it quickly mixes with the larger containment space. For the faults where the SADV is still required to depressurise the primary circuit (e.g. intact circuit faults and smaller LOCAs), the location of the SADV discharge is of importance as hydrogen is transported there once the SADV is opened. The SADV discharges into the room in which the RCP of loop 2 is located.
- Break size – the LOCA break size determines the hydrogen generation rate and the longevity of the hydrogen generation in the core. A larger break may result in a high hydrogen generation rate, but the reactions may not last as long as a small break. For accidents where the SADV is necessary to reduce the primary pressure, the break size is equivalent to the SADV capacity once the SADV is opened.
- Timing of depressurisation – For larger LOCAs (e.g. IB-LOCA and LB-LOCA), this occurs at the start of an accident and are less effected by opening of the SADVs (although some hydrogen still leaves via the SADVs if opened). For faults in which the SADV is required to depressurise the primary circuit, the timing of opening the SADVs plays an important role in the hydrogen generation.
- Secondary cooldown – The automatic secondary cooldown procedures, Medium Pressure Rapid Cooldown (MCD) and Low Pressure Full Cooldown (LCD), which remove heat via the SGs can slow down core degradation (prolonging the phase of hydrogen generation) and also reduce the amount of steam present in the containment.

291. Using these parameters, the RP state that there are 44 combinations that have been considered for the reference plant, Fangchenggang NPP Unit 3 (FCG3) (Ref. 36). The RP aims to reduce the number of cases that are required for a more detailed analysis of global and local effects.

292. The RP has considered the above factors to determine a shortlist of accidents and performed deterministic analysis in order to derive three limiting cases for further analysis of global and local risk (Ref. 36). Since the timing of a depressurisation in an SBO and a LOCA are very different, the RP has chosen to analyse both LOCAs and the SBO. The RP includes two LOCAs by considering different break sizes, locations and secondary cooldown assumptions.

293. The RP identifies the following for more detailed analysis:

- SBO – SBO with 30-minute delay of depressurisation
- SB-LOCA - 5 cm SB-LOCA at top of pressuriser with MCD and LCD available
- IB-LOCA - 7.5 cm IB-LOCA at the top of the pressuriser with MCD available

294. The cases are chosen because they present the highest peak local concentration (IB-LOCA), the highest hydrogen mass generated (SBO), and an accident with a relatively high hydrogen mass generated with a relatively high peak local concentration (SB-LOCA).

295. As part of my assessment of the methodologies employed, my TSC reviewed the RP's process for deriving the limiting conditions for hydrogen management (Ref. 20). My TSC found that the RP had used relatively coarse nodalisation of the containment when making comparisons of the accidents. However, in response to RQ-UKHPR1000-0545 (Ref. 81), the RP provided evidence that despite the relatively coarse nodalisation, the thermal hydraulics and hydrogen distribution predicted by the ASTEC code were similar to the equivalent calculation performed using the GASFLOW-MPI code. My TSC therefore found that the RP's analysis to determine the limiting accidents and conditions was comprehensive and used appropriate tools (Ref. 36).

296. With this in mind, I am satisfied that the RP has identified appropriate scenarios and initial conditions to capture the most limiting global and local effects, as set out in paragraph 280.

4.5.3.2 ASTEC Analysis of the Risk of Global Detonation, Pressure Load of Slow Deflagration and Identification of Most Onerous Local Conditions

297. As stated previously the RP has used ASTEC, using the three scenarios described above (paragraph 293), to demonstrate that the conditions for global detonation are not reached, to demonstrate that pressure from slow deflagration does not challenge containment, and to determine the limiting conditions for localised phenomena. In this section I summarise my assessment of the RP's supporting arguments and evidence for each of these aspects. However, the analysis of the global detonation, pressure load from slow deflagration and the identification of the most limiting conditions for local phenomena are based upon a common set accident analyses, which is important for the conclusions that the RP draws. I have therefore broken this section down into the following subsections:

- The RP's Analysis of the Progression of the Hydrogen Related Aspects using ASTEC
- Risk of Global Detonation
- Pressure Load from Slow Deflagration
- ASTEC input to GASFLOW-MPI calculations of localised phenomena

- Conclusion

The RP's Analysis of the Progression of the Hydrogen Related Aspects using ASTEC

298. As stated, the ASTEC code is used to determine the progression of the severe accident and aspects related to hydrogen on a global level (i.e. considering the whole containment). The analysis described in this section is used by the RP to determine whether global detonation is prevented, pressure loads from slow deflagration are tolerable, and to determine the most limiting case for analysis of localised phenomena.

299. Ref. 36 describes the initial conditions used and the assumption related to the availability of systems. On the most part the assumptions appear appropriate (e.g. failure of the RIS [SIS]). However, for each scenario simulated the RP has assumed that containment spray is not used. I consider that during a severe accident in the UK HPR1000, the containment spray has the potential to reduce the steam concentration and increase the relative concentration of hydrogen. In a 'real world' severe accident, there are benefits to using the containment spray for heat removal, and the operator would have to decide whether to implement containment spray. Therefore, this assumption may not be adequately conservative for the analysis of hydrogen management.

300. The RP has argued that, whilst it is true that the hydrogen concentration may increase, the containment spray also promotes mixing and may be beneficial to hydrogen management. The RP also argues that the decision to use the containment spray would need to consider prevailing conditions, and be based on the SAMGs. The RP argues that because the SAMGs are not available in GDA as they will be developed by a future licensee, and because the decision is based on prevailing conditions, the analysis performed in GDA cannot make an assumption on the time which spray would be implemented. Based on these two arguments, the RP has concluded that the analysis should not include the containment spray during GDA.

301. To support this position, the RP has provided sensitivity analyses (Ref. 47) regarding whether containment spray is used or not. In Ref. 47, I judge that the RP has adequately demonstrated that the hydrogen concentrations, particularly local concentrations, are relatively insensitive to containment spray actuation. With this in mind I am satisfied with the RP's assumption that containment spray is not actuated for GDA.

302. Importantly, the IVR system is assumed to be available in the analysis. This assumption means that combustible gases generated by MCCI are not considered when demonstrating the effectiveness of the EHR [CHRS]. The RP argues that the IVR system has been demonstrated to be effective, and that sequences that lead to MCCI are practically eliminated. The RP's safety case for the demonstration that IVR is effective is in preventing failure of the RPV (see sub-section 4.5.2). In addition, as demonstrated by the RP's level 2 PSA (Ref. 102), the sequence frequency for a sequence involving failure of IVR is extremely low (~10^{-9} pa). Given this, I judge that it would be disproportionate to account for gases generated in the MCCI process when demonstrating the effectiveness of the EUH [CCGCS] during GDA. During the development of SAMGs, the licensee may choose to demonstrate that the EUH [CCGCS] can also mitigate scenarios where MCCI also contributes to the combustible gases in the containment; however, my judgement here is only for GDA.

303. The RP has also not included any hydrogen generated due to much slower processes (e.g. radiolysis and oxidation of metals in the containment). The RP has provided analysis of these processes for design basis faults (Ref. 103). In my judgement, the analysis adequately demonstrates that the hydrogen generation rates are significantly

lower than those in the steam-zirconium reaction by orders of magnitude (Ref 36). Moreover, the assumption is aligned with RGP for the design of a severe accident combustible gas control system (Refs 20 and 22). I am therefore satisfied with the RP's assumption that these do not contribute to the mass of hydrogen to be included in the demonstration that the EUH [CCGCS] is effective DEC-B scenarios chosen.

304. Based on the above, I am satisfied that the RP has used adequate assumptions in the demonstration of the effectiveness of the EUH [CCGCS] on a global level (Ref. 36).

305. The results of the calculation of the progression of the severe accident scenarios and the containment thermal hydraulics are presented in Ref. 36. For each scenario Ref. 36 describes the accident progression and provides plots related to hydrogen concentration (mass and Shapiro diagrams). Below I have summarised the hydrogen aspects of the severe accident progression for the three scenarios considered (Ref. 36):

- SBO **-** The generation rate for hydrogen peaks when the SADVs are opened and again after reflooding of the core has occurred when the core begins to reheat. Relatively high concentrations of hydrogen build up in the reactor coolant pump 2 compartment (6 - 8% vol). This is because the pressure relief valves discharge into the pressuriser relief tank (PRT) compartment, which is adjacent to the compartment for the reactor coolant pump 2.
- SB-LOCA - LCD is credited as a conservative assumption to reduce the steam generated. Because of this the pressure is reduced gradually and only one peak of hydrogen generation is observed when the fuel is uncovered. The hydrogen concentration accumulates near the break location (pressuriser compartment) and reaches a maximum of 11.4 vol%.
- IB-LOCA - Two peaks of hydrogen generation are observed. One due to the initial uncovery of the core and the other after the SADVs are opened. The hydrogen concentration reaches a maximum of 13.3 vol% at the break location (pressuriser compartment). Another peak in concentration is observed at a maximum of 5.4 vol% in the reactor coolant pump 2 compartment due to the opening of the SADVs.

306. In all three cases, the RP claims that its analysis demonstrates that the PARs effectively remove 80% of the hydrogen and reduce the concentration of the hydrogen in the upper dome space of the containment to less than 4% (vol), which is a widely recognised dry limit for combustion (Ref. 20). In addition, I observe that the results indicate that local accumulations of hydrogen are dispersed over time to concentrations of safe levels due to convection and mixing with the larger containment space.

307. To conclude, I am content that the initial conditions and assumptions made in the ASTEC analysis provide an adequate basis for the demonstration of the effectiveness of the EUH [CCGCS], and that the sequence progression modelled by the RP is reasonable.

Risk of Global Detonation

308. As stated previously, detonation of hydrogen is a highly energetic process which presents the largest challenge in terms of dynamic loads to the containment (IAEA-TECDOC-1661, Ref. 6). It is widely recognised that there are two ways in which detonation can occur in the containment (IAEA-TECDOC-1661, Ref. 6): detonation directly from an ignition in a volume with high concentrations of hydrogen, and through a complex mechanism where a flame front accelerates to beyond the speed of sound, transitioning into a detonation. The risk of the former can be evaluated using ASTEC as it is a larger scale (or global) effect. The latter is related to local phenomena and the

local geometry in which the volume of hydrogen, air and steam mixture is located, which requires more sophisticated codes (such as GASFLOW-MPI). Global detonation is covered in this section, and DDT is covered in sub-section 4.5.3.3.

309. It is an internationally recognised view that if the hydrogen concentration within the containment is kept below 10% vol, then the risk of detonation is negligible (IAEA-TECDOC-1661, Ref. 6). The RP has included as a safety functional requirement, that the average containment concentration of hydrogen should be kept below 10% (Ref. 31). As such I expect that the RP demonstrate that this requirement is reflected in the deterministic analysis.

310. Whilst specific arguments are not presented, the RP has presented hydrogen concentrations from the upper dome of the containment, with and without PARs, for the three accidents listed in paragraph 305 above. From this, it can be observed that the hydrogen concentration remains below 10 vol% for all cases even when the PARs are not credited. As the hydrogen concentration is likely to be highest in the upper dome region after stratification, I judge that the uniform distribution of hydrogen in all cases would be lower than the 10 %vol requirement.

311. The RP has not explicitly made the argument in Ref. 36 that the concentration is kept below 10% and therefore global detonation is avoided. Therefore, whilst I am satisfied that the requirement set out in Ref. 36 is demonstrated in the deterministic analysis, I consider this a minor shortfall in the safety case documentation.

312. Notwithstanding this, based on Ref. 36, I am satisfied that the RP has demonstrated that global detonation is avoided during the DEC-B scenarios analysed.

Pressure Load from Slow Deflagration

313. Although deflagration may be caused by a localised effect, the flame can propagate and result in a global overpressure. Whilst slow deflagration can be calculated using the more sophisticated GASFLOW-MPI code, the RP has chosen to perform conservative calculations using the output from ASTEC. However, the heat loads that are observed from a slow deflagration only occur locally, and therefore the RP has chosen to calculate these using GASFLOW-MPI. My assessment of the RP's analysis is summarised in sub-section 4.5.3.3.

314. For each of the accidents described above in paragraph 305, Ref. 36 presents the maximum theoretical energy that can be output by burning the entirety of the hydrogen present in the containment in a slow deflagration at the most limiting point in time. This calculation results in the so called Adiabatic Isochoric Complete Combustion (AICC) pressure, which is widely used to determine an upper limit of the amount of energy that could be generated if all hydrogen is burned at the same time (Ref. 20). The pressure loads calculated for the SB-LOCA, IB-LOCA, and SBO are 0.329, 0.402 and 0.483 MPa, respectively. The design pressure of the containment is 0.52 MPa (Ref. 36). However, the RP claims that the ultimate capacity of the containment is significantly larger than this value (> 1 MPa). In my opinion, although the calculation is simplistic it is also conservative as it does not take into account any heat losses from the deflagration. Because of these reasons, although the margin to the design pressure curve is relatively low (see section 4.7 for a description of the curves), I am satisfied this simple calculation adequately demonstrates that pressure loads from a slow deflagration would not challenge the containment.

315. To conclude, I am satisfied that the RP has adequately demonstrated that for the DEC-B scenarios analysed the pressure load from the slow deflagration will not challenge the UK HPR1000 containment on a global level.

ASTEC input to GASFLOW-MPI calculations of Localised Phenomena

316. As stated previously, the RP has used the ASTEC code to determine the most limiting conditions for localised phenomena for analysis using the CFD code, GASFLOW-MPI. This is based on the analysis described in paragraphs 298 to 307. As stated, the ASTEC calculation of the hydrogen, water and steam mass and energy released into the containment as a function of time is also used in the GASFLOW-MPI calculation. Therefore the ASTEC analysis has a direct impact on the GASFLOW-MPI analysis.

317. The conditions for flammability are dependent on three components: air, steam and hydrogen concentration. As stated previously, the RP has used the well-known Shapiro diagrams (Ref. 80) to determine whether (using the concentrations of air, steam and hydrogen calculated using ASTEC) the scenarios analysed can result in conditions necessary for localised phenomena to occur. The knowledge from this is then used in more sophisticated calculations performed using GASFLOW-MPI (Ref. 90).

318. Using Shapiro diagrams, the RP argues that only the IB-LOCA results in conditions in which fast deflagration may occur (Ref. 36). Therefore the RP has performed GASFLOW-MPI calculations of the IB-LOCA to support the arguments related to localised phenomena which are summarised in paragraph 280 (Ref. 90). The mass and energy release of hydrogen, steam and water from the RCP [RCS] to the containment as a function of time, which are calculated in the ASTEC calculation of the IB-LOCA (Ref. 36), are used as an input to this GASFLOW-MPI analysis (Ref. 90). The RP has analysed the IB-LOCA in GASFLOW-MPI using conservative assumptions. The conservative analysis of this one scenario, the IB-LOCA, forms the majority of the evidence that underpins the RP's arguments related to localised phenomena (Ref. 90).

319. As stated, the mass and energy release of the hydrogen, steam and water from the RCP [RCS] to the containment is used in the GASFLOW-MPI calculations that support the arguments that I have summarised in paragraph 280. Whilst the explanations provided appear reasonable and should result in an appropriate mass and energy release for the GASFLOW-MPI calculation, in my opinion, there is already large uncertainty in the ASTEC calculation which is then passed to the calculations in the GASFLOW-MPI calculation (for example, there are uncertainties associated with the accident progression prior to the onset of core degradation, uncertainties in the core degradation process and oxidation model used). In addition, for GDA, there are unknowns related to the future development of SAMGs, and the actual actions of the operator in a real event (e.g. the decision to use containment spray or to reflood the core isn't taken into account by the RP in GDA, as it is not possible to predict operator actions). Both of these factors mean that the mass and energy release calculated by ASTEC have large uncertainties associated with them.

320. To account for this uncertainty, the RP has made a conservative assumption for the IB-LOCA that all of the zirconium in the core is oxidised during the accident. The ASTEC calculation of the IB-LOCA results in 475 kg of hydrogen generation (Ref. 36). The 100% zirconium oxidation assumption means that the rate of hydrogen generation is therefore approximately doubled and results in 904 kg of hydrogen assumed in the GASFLOW-MPI calculation (Ref. 90). This is clearly a conservative assumption, however I consider that it is appropriate for the reason stated above and is aligned with my expectations for SAP FA.15. The results of the GASFLOW-MPI calculation are discussed in sub-section 4.5.3.3.

321. In my opinion, the ASTEC calculation alone may not reveal all limiting conditions as the nodalisation of the containment is relatively coarse. For example, a large compartment that is represented by one zone in the ASTEC code does not provide information regarding the distribution of hydrogen in that zone. Instead, the code assumes that the hydrogen is uniformly distributed within the zone. This has the potential to mask

stratification, in which hydrogen pockets are accumulated at the top of the compartment. Moreover, it is internationally recognised that the potential for flame acceleration and the evolution to DDT is geometry dependent (Ref. 104). Therefore in my opinion, it is difficult to determine that the IB-LOCA considered is the most limiting case for flame acceleration when only considering one hydrogen release location. To address this the RP therefore provided GASFLOW-MPI analysis of the risk of DDT for the SB-LOCA, IB-LOCA and the SBO (Ref. 90) using the best estimate assumptions (as opposed to the conservative assumption of 100% zirconium oxidation used in the base case IB-LOCA described above), which I consider is appropriate.

322. To conclude, I am satisfied that, by using the ASTEC code, the RP has identified appropriate conditions for analysis of localised phenomena.

Conclusions Related to the ASTEC Analysis of the Risk of Global Detonation, Pressure Load of Slow Deflagration and Identification of Most Onerous Local Conditions

323. I am satisfied that the RP, through its ASTEC analysis (Ref. 36), has:

- Adequately demonstrated that EUH [CCGCS] is effective in preventing conditions necessary for global detonation in the DEC-B scenarios analysed.
- Adequately demonstrated that EUH [CCGCS] is effective in mitigating the hydrogen hazard such that global pressure loads from slow deflagration in the DEC-B scenarios analysed.
- Adequately identified the most onerous conditions for the analysis of localised phenomena.

4.5.3.3 GASFLOW-MPI Calculations of the Localised Phenomena

324. As stated previously, the RP has identified the most limiting case for localised phenomena using the ASTEC code (Ref. 36). This limiting case for this is the IB-LOCA (the reasons for this are described in the previous section). As also stated, for the GASFLOW-MPI calculation (Ref. 90) the RP has scaled up the mass and energy release of the hydrogen to account for 100% oxidation of the cladding.

325. The GASFLOW-MPI analysis performed by the RP uses the modified mass and energy release from the ASTEC code as a boundary condition, and calculates the transient thermal hydraulics of the containment. Amongst other things the GASFLOW-MPI code is used to calculate wall temperatures, localised gas temperatures, flow directions, flow velocity, gas concentrations and flame propagation (Ref. 90). These data are then used by the RP to determine whether the conditions are likely to lead to challenges to the containment and the outcome of these considerations is reported in Ref. 90.

326. The RP has performed the following analysis using the GASFLOW-MPI code to demonstrate the EUH [CCGCS] is effective in preventing local phenomena which can challenge the containment:

- Analysis of the heat loads from slow deflagration, using the conservative IB-LOCA (the pressure loads are calculated conservatively using the AICC with the data generated using ASTEC and have already been discussed in sub-section 4.5.3.2).
- Analysis of pressure waves from fast deflagration, using the conservative IB-LOCA.
- Analysis of flame acceleration and the likelihood of DDT, using the conservative IB-LOCA and the best estimate IB-LOCA, SBO and SB-LOCA.

327. The RP has used the models specific to the containment geometry of the UK HPR1000, and the specification for the PARs which are defined in Chapter 4 of the EUH [CCGCS] system design manual (Ref. 56). My assessment of these models is summarised in sub-section 4.6.

328. In the paragraphs 329 to 348, I summarise my assessment of the RP's analysis of localised phenomena that has the potential to challenge the containment.

Heat Loads From Slow Deflagration

329. The RP explains in Ref. 90 that whilst the pressure load from a slow deflagration has a global effect on the containment and can be calculated using ASTEC code (Ref. 36) (see sub-section 4.5.3.2) the heat load effects things which are local to the slow deflagration and is therefore calculated using the CFD code, GASFLOW-MPI.

330. In Ref. 90, the RP presents analysis of the heat load from a slow deflagration of the IB-LOCA (applying the 100% zirconium oxidation assumption).

331. The GASFLOW-MPI code requires the user to select an ignition time and location to begin the slow deflagration. The RP claims that it has chosen the most limiting time and location. The time is related to the hydrogen concentration, and, in my opinion is relatively straight forward. The RP has chosen to ignite the hydrogen cloud in the dome space as it allows the heat generated from the burn to promote further reactions and the open area allows the flame to propagate more freely to adjacent areas. Specifically, the RP selected the outlet of a PAR in the dome area, which is in the direction of the hydrogen jet from the break, to ignite the hydrogen cloud. The RP claims that this simulates a possible recombiner ignition (Ref. 90), which appears reasonable.

332. As the flame propagates, it heats the steel liner of the containment. Since the steel liner provides the leak tightness of the containment, the RP aims to demonstrate that the integrity of the liner is maintained throughout the accident. The RP has set an acceptance criterion for the steel liner of the containment as 154 °C. This is far below the melting temperature of steel, but is the value used for the maximum allowable temperature for equipment qualification in the containment (see sub-section 4.7). I am therefore satisfied that it is appropriate for use as an acceptance criterion.

333. To determine whether temperatures of the liner remain below this limit, the RP has used different locations in the steel liner dome to track the temperature throughout the simulation. Following the ignition it can be seen that the flame propagates through most of the containment (except lower parts of the annulus). The deflagration propagates throughout the hydrogen cloud within about 10 seconds. The RP report that the maximum temperature of the containment liner reaches 147.6 °C, which is below the maximum temperature limit of 154 °C (Ref. 90).

334. The analysis appears to have been performed in a logical way, using the worst-case time and location of ignition, and tracking the most heated parts of the containment wall. I am, therefore, satisfied that the RP has demonstrated that the temperature of the whole containment wall will remain below the 154 °C temperature limit, and that the heat load from a slow deflagration will not challenge the integrity of the containment.

335. To conclude, I am satisfied that the RP has, for the most limiting conditions, adequately demonstrated that the local heat loads from slow deflagration are tolerable and will not challenge the containment. Therefore, I am satisfied that the EUH [CCGCS] is effective in mitigating the hazard posed by hydrogen such that local heat loads from slow deflagration are tolerable.

Analysis of Fast Deflagration

336. As discussed previously, the speed in which a flame front propagates is dependent on the local hydrogen concentration and geometry of the space in which the hydrogen cloud exists (Ref. 104). A fast deflagration has the potential to accelerate and result in DDT. However, even without the occurrence of DDT, this fast deflagration has the potential to generate large pressure waves that could challenge the containment.

337. The RP claims that fast deflagration does not result in pressure loads that challenge the containment. This section addresses this claim (flame acceleration and DDT are addressed in paragraphs 343 to 348 below). To support this, the RP has therefore performed analysis to determine whether the conditions for fast deflagration and flame acceleration exist, and whether the pressure loads associated with it are acceptable. The analysis is presented in Ref. 90.

338. The RP has applied the GASFLOW-MPI code to determine whether the conditions for fast deflagration and flame acceleration exist at any time during the progression of the IB-LOCA (with the conservative 100% zirconium oxidation assumption). The RP applies the sigma criterion to determine whether the conditions for flame acceleration are met. This criterion is well known and widely used internationally (Refs 80 and 104), and my TSC has concluded that they are also applicable and conservative for use in the analysis of flame acceleration in the UK HPR1000 (Ref. 20). Moreover, this criterion has been used in previous GDAs. I therefore consider that the use of this criterion is appropriate.

339. The RP's analysis shows (Ref. 90) that for short periods of time (tens of seconds), clouds of hydrogen that meet the conditions for flame acceleration exist (referred to as sigma clouds by the RP). The analysis shows that as the accident progresses, hydrogen accumulates causing sigma clouds to form in three places:

- The upper part of the containment, referred to as the upper compartment by the RP (between +17.5 m and +38.2 m, which is the space that the pressuriser compartment opens to);
- reactor pump room 2; and
- the pressuriser compartment.

340. In a similar way to that for the slow deflagration, the RP has chosen the most penalising ignition point to start the fast deflagration. The RP has therefore set the ignition point within these clouds and at a time when the clouds have the greatest potential for flame acceleration.

341. The RP claims that there are two effects that should be considered: the global pressure wave due to the flame front of the fast deflagration, and local effects on containment structures, such as walls between compartments. The RP claims that these do not challenge the containment for the following reasons:

- For the global effect of the pressure wave on the containment, the RP calculated the speed of the wave front based on the GASFLOW-MPI calculation. The RP claims that the analysis demonstrates that the flame front velocity is below the speed of sound, ranging from ~35 to 97 ms^{-1} (Ref. 90). The RP claims that a wave front of this velocity is not challenging to the containment. In my opinion, the RP's assertion is reasonable as the flame velocity is well below the speed of sound, which is the velocity at which detonation is defined.
- With regards to the dynamic pressure loads to the compartment walls, the RP presents the pressures that are obtained in compartments when the fast deflagration is initiated. The RP concludes that the loads are within acceptable

limits. To gain confidence in the RP's conclusion, I used the dynamic load analysis performed for design basis accidents involving high energy pipe failures as a reference point (Ref. 105). The differential pressures obtained from the fast deflagration analysis (Ref. 90) are an order of magnitude lower than those presented in Ref. 105. I am therefore satisfied that the dynamic pressure loads from fast deflagration will not challenge the internal structures of the containment.

342. To conclude, I am content the RP has adequately demonstrated that the flame front from a fast deflagration will not challenge the containment, and that the dynamic loads within compartments will not challenge the internal structures of the containment (Ref. 90). I am, therefore, satisfied that the EUH [CCGCS] is effective in mitigating hazard posed by hydrogen such that, even in the most limiting conditions, the UK HPR1000 containment will not be challenged by global and local pressure loads caused by fast deflagration.

Analysis of Flame Acceleration and DDT

343. As stated previously, the RP claims that flame acceleration has the potential to change a fast deflagration combustion mode to a detonation, which is a combustion mode characterised by on in which the velocity of the flame front is at or greater than the speed of sound (Ref. 90).

344. Using the sigma criteria, the RP has identified sigma clouds which have the potential for flame acceleration. The RP has identified the sigma in locations list in paragraph 339, using the GASFLOW-MPI code. The RP has then applied the lambda criterion using the conditions calculated by the GASFLOW-MPI code to determine the likelihood of the occurrence of DDT. This criterion is well known and widely used (Refs 80 and 104). My TSC also concluded that this is conservative when applied to a PWR containment and is appropriate for use for the UK HPR1000 safety case (Ref. 20).

345. The RP claims that the analysis demonstrates that there are clear margins to the acceptance criteria throughout the entire progression of the IB-LOCA with the conservative assumption that 100% of the zirconium in the core is oxidised (Ref. 90). Moreover, the RP has also performed the analysis using the best estimate IB-LOCA (i.e. not applying the assumption of 100% zirconium oxidation) and found that the margin is significantly higher (an exact value of how much less likely DDT is cannot be quantified easily) (Ref 90).

346. In addition, the RP has also presented best estimate analysis results of GASFLOW-MPI calculations for the SB-LOCA and SBO (i.e. without the 100% zirconium oxidation assumption) (Ref. 90). The RP claims that the analysis demonstrates that the margin to DDT is adequate, and far larger than for the IB-LOCA with the conservative assumption applied. I judge that the sensitivity studies provide a compelling argument that different accident types will also not present a risk of flame acceleration and DDT.

347. In my opinion, given the openness of the containment (as discussed in the previous section) and the lack of corridors to promote flame propagation, the result is not surprising. I judge that even with the conservative assumptions applied, the RP has adequately demonstrated that DDT is avoided in the limiting case.

348. To conclude, I am satisfied that, even in the most limiting case, the EUH [CCGCS] is effective in preventing the necessary conditions for DDT.

Conclusions Related to GASFLOW-MPI calculations of Localised Phenomena

349. I am satisfied that the RP has adequately demonstrated that the EUH [CCGCS] is effective in preventing conditions such that local phenomena do not challenge the containment, even in the most limiting condition. In particular, I am satisfied that the RP has demonstrated that, even in the most limiting conditions, the EUH [CCGCS] is effective in reducing the hazard posed by hydrogen such that:

- local heat loads from slow deflagration are tolerable;
- the UK HPR1000 containment will not be challenged by global and local pressure loads caused by fast deflagration; and
- the necessary conditions for DDT are prevented.

4.5.3.4 GASFLOW-MPI Analysis of the Optimisation of the EUH [CCGCS] and Containment Layout

350. The RP claims that the EUH [CCGCS] and containment layout have been optimised for hydrogen management (Refs 36 and 90). Below, I have summarised the RP's main arguments as to why it considers that the EUH [CCGCS] and containment have been designed to be optimised:

- The layout of the containment is such that it allows for free movement of flow between compartments, encouraging mixing.
- The layout of the containment is such that it allows for natural convection to occur, and as such encourages mixing.
- The PARs are positioned to take advantage of natural draughts and promote natural circulation.
- The PARs are positioned such that they do not cause damage to surrounding SSCs.
- The hydrogen monitors are placed in locations that provide a broad understanding of the hydrogen risk during a severe accident, and enable decision making (for example, whether to use containment spray).

351. To demonstrate this, the RP has used the conservative IB-LOCA using GASFLOW-MPI and using the same containment and PAR model used in sub-section 4.5.3.3.

352. In the following paragraphs (paragraphs 353 to 362), I have summarised my assessment of the RP's evidence which it claims demonstrates that the EUH [CCGCS] and containment have been optimised for hydrogen management.

Layout of the Containment

353. To demonstrate that the containment compartmentalisation adopted by the UK HPR1000 is beneficial to convection and therefore hydrogen mixing, in Ref. 90 the RP has presented the containment thermal hydraulic conditions during the IB-LOCA as calculated by the GASFLOW-MPI code. The analysis results are presented in various plots. Notably, these include 2D cross-sectional representations of the containment in which the temperature distribution, steam concentrations and velocities of gases (including directions) can be easily read at different points in time during the progression of the IB-LOCA (Ref. 90).

354. As with the ASTEC analysis, the containment spray is assumed unavailable. From the analysis (Ref. 90) I observe that shortly after the break, and again after opening the SADV, the condensation on the containment walls allows for cooling and downwards movement of gases near the containment wall. In addition, the steam concentrations in the rooms adjacent to the reactor coolant pump 2 compartment and larger containment space follow closely the concentration of the reactor coolant pump 2 compartment. In

my opinion, this indicates that a good connection is available for steam to move freely from reactor coolant pump 2 compartment and the wider containment space, and vice versa. At the end of the calculation, a slight gradient in temperature from the bottom of the containment to the top can be seen. The vector diagrams for velocity and temperature gradients indicate that natural convection is established. From 9,000 seconds onwards, I observe that the steam concentration is relatively uniform throughout the containment.

355. In Ref. 90, the RP has also presented plots of hydrogen concentration at different times for two cross sections of the containment during the progression of the IB-LOCA using the GASFLOW-MPI code. The analysis predicts that the hydrogen concentration is closely linked to the movement of gases in the containment. I observe that whilst some stratification is seen in the upper dome, in my opinion the hydrogen appears to be well mixed from 9,000 seconds onwards. It can also be seen that although stratification does occur temporarily, the hydrogen concentration remains below 10% (vol) throughout (Ref. 90).

356. Given the analyses discussed above, and the fact that containment spray would be available to further promote mixing, I am satisfied that the RP has provided adequate evidence that the containment compartmentalisation adopted by the UK HPR1000 enables natural convention and good mixing.

Location of the PARs

357. Ref. 90 also presents plots related to recombination rates of the PARs predicted by the GASFLOW-MPI code during the IB-LOCA. The RP explains the differences in the trends, noting that some PARs have higher recombination rates at different times due to the location of the break and the opening of the SADV. After the opening of the SADV, the recombination rates follow similar trends with similar recombination rates. The RP therefore draws the qualitative conclusion that the PARs are well positioned because no single PAR has an abnormally high or low recombination rate (Ref. 90).

358. The PARs chemically combine oxygen with hydrogen, which generates water (in the steam phase). The reaction is exothermic, and the steam that exits the PAR is of a higher temperature that the gases that enter it. It is my expectation that PARs are positioned such that they do not cause damage to the SSCs within the containment, or the containment structure itself. The RP recognises this in the system design manual for the EUH [CCGCS], Ref. 68. Ref. 68 states that the EUH [CCGCS] layout design should consider the potential damage to surrounding SSCs.

359. To demonstrate that the containment is not challenged by the additional heat load from the PARs, the RP has presented results of analysis of the IB-LOCA using the GASFLOW-MPI code, which it claims demonstrates that the average gas containment temperature rise is roughly 20 °C in comparison to when PARs are not operated. The RP concludes that this results in an average gas temperature lower than the temperature limit for survivability in the containment (154 °C).

360. I note however, that the RP has not provided evidence that the hot gases exiting the PARs would not directly impinge on all equipment required for severe accident management. In my opinion, it should be demonstrated that the operation of the PARs does not prevent the delivery of other severe accidents safety functions (Position 2 of WENRA safety for new reactors (Ref. 12)). Nevertheless, the RP does show that the hot gas quickly dissipates and I judge that it is unlikely that the hot gases would challenge the survivability of severe accident management equipment (e.g. hydrogen sensors and spray rings). However, the RP has not explicitly addressed this, and there may also be SSCs that could be used in severe accident management that have not been captured in the DEC-B analysis. Bearing in mind more detailed design

information and details of the SAMGs are required to understand whether SSCs will be affected by these hot gases, I judge that this should be revisited by a future licensee and have therefore raised the following assessment finding:

AF-UKHPR1000-0080 – The licensee shall, as part of detailed design and as part of development of severe accident management guidelines, demonstrate that equipment used for severe accident management is not negatively impacted by the exhaust of the passive autocatalytic recombiners of the containment combustible gas control system.

361. Notwithstanding this Assessment Finding, I am satisfied that the RP has adequately demonstrated that the PARs are well positioned to optimise the effectiveness of the EUH [CCGCS].

Location of the Hydrogen Monitors

362. The RP also has analysed the hydrogen concentrations detected at the hydrogen monitors and made comparisons to those of the average hydrogen concentrations for large spaces (e.g. the containment dome) (Ref. 90). Within this reference, the RP demonstrates the differences that can be observed in concentration are due to the difference in elevation of hydrogen monitors and some stratification of the hydrogen. The arguments provided by the RP for the positioning of the monitors appears reasonable, and I am satisfied that the positioning should enable an understanding of the global hydrogen concentration during a severe accident. This meets my expectations as informed by SAPs AM.1 paragraph 778 (Ref. 2).

4.5.3.5 Conclusions Related to Hydrogen Management and the Effectiveness of the EUH [CCGCS]

363. The RP has adequately identified appropriate severe accident scenarios for analysis of the global and local phenomena.

364. The RP has provided adequate demonstration that global detonation will be avoided by the UK HPR1000 design.

365. The RP has adequately demonstrated that the pressure and heat loads associated with slow deflagration in the limiting case are within acceptable limits.

366. The RP has adequately demonstrated that fast deflagration that could potentially occur in the limiting case does not result in unacceptable dynamic pressure loads.

367. The RP has adequately demonstrated that the conditions for flame acceleration and DDT are not met during the limiting case.

368. The RP has adequately demonstrated that the EUH [CCGCS] and containment have been optimised for hydrogen management.

369. To summarise, I am satisfied that through submissions Refs 36 and 90, the RP has demonstrated that the EUH [CCGCS] (combined with the containment design) is effective in preventing a challenge to the integrity of the containment posed by hydrogen accumulation during severe accidents.

4.5.4 Effectiveness of the Severe Accident Depressurisation Valves

370. As stated previously, in a PWR severe accident, DCH has the potential to result in early failure of the containment leading to a large release of radioactivity (Ref. 80).

371. Based on guidance provided in IAEA SSG-2 (Ref. 6), it is my expectation that new reactors are designed to practically eliminate sequences in which DCH could occur.

The UK HPR1000 aims to achieve this by depressurising the primary circuit during a severe accident such that if RPV failure were to occur, the pressure would be low enough to avoid HPME (and therefore DCH).

372. Also based on IAEA SSG-2 (Ref. 6), it is my expectation that severe accident sequences that can lead to containment by-pass are practically eliminated. Related to this, a secondary, but important, role of the SADVs is to halt natural circulation of hot gasses in the primary circuit and avoid creep rupture of the SG tubes, preventing bypass.

373. The RP has submitted DEC-B deterministic analysis to demonstrate the effectiveness of the SADVs in preventing these phenomena (Ref. 37). In comparison to the analysis for IVR and EUH [CCGCS], the RP's methodology for the assessment of the SADVs is relatively simple. Only the ASTEC code is used to model high pressure core melt scenarios. The IVR system is disabled in the model, deliberately causing RPV failure in order to determine the RPV pressure at the time of failure.

374. The acceptance criteria that the RP has chosen to demonstrate effectiveness of the SADVs is that the RPV pressure is reduced to below 2 MPa at the point of failure of the RPV and originates from the European Utility Requirements (EURs) (Ref. 106), which I consider is reasonable.

4.5.4.1 Assessment of Analysis for the Effectiveness of Depressurisation to Prevent HPME and DCH

375. From the severe accident scenario selection process (see sub-section 4.4), the RP has selected the following DEC-B scenarios as representative cases in demonstrating the effectiveness of the SADVs in preventing HPME and DCH:

- SBO
- ATWS (LOMFW)

376. This is because they represent high pressure core melt scenarios. The SB-LOCA, IB-LOCA and LB-LOCA all, to different extents, involve some depressurisation and loss of inventory through the break; whereas for the SBO and ATWS (LOMFW), the only energy removed from the system prior to actuation of the SADVs is through the PSVs. I therefore judge that the use of the SBO and ATWS (LOMFW) to demonstrate the effectiveness of the SADV is appropriate and aligned with the expectations of SSG-2 that the limiting conditions should be used to demonstrate the effectiveness of the safety features.

377. For each scenario, the RP has undertaken analysis which it claims demonstrates effective depressurisation at the time of the COT signal and depressurisation at 30 minutes after the COT signal. In addition, the RP has calculated the time to failure of the RPV if neither the SADVs or IVR is actuated (Ref. 37).

378. As discussed previously, the RP claims that if IVR is implemented the ASTEC code predicts that the RPV will not fail. Therefore, the RP states that it is necessary to assume that IVR is not working in the analysis in order to understand whether the SADVs alone are capable of avoiding HPME. In my opinion, this is appropriate and allows for the requirements of the SADV to be determined in isolation of the IVR system.

379. The analysis (Ref. 37) only credits one train of the SADV. As the RP claims that there is in built redundancy within the SADV, I am satisfied that this is an appropriate assumption to make in the analysis.

380. I have chosen to sample the ATWS (LOMFW) as RP's analysis demonstrates that it results in higher RCP [RCS] pressures than the SBO. Ref. 37 presents the which systems it assumes are available in the analysis. The MHSI, LHSI, reactor trip, ASG [EFWS] and containment spray are considered unavailable. The accumulators are assumed to be available as they are passive. In my opinion it is realistic that the accumulators would actuate and that the only effect in the analysis is to slightly delay the reduction of pressure of the RCP [RCS] down to the RP's acceptance criterion of 2 MPa. Given this, I am satisfied that the RP's assumptions are reasonable and aligned with the expectations of IAEA SSG-2 (Ref. 6) and SAP FA.16 (Ref. 2).

381. In addition, the PSVs are considered unavailable after the SADVs are opened. I judge that this assumption allows the RP to demonstrate the effectiveness of the SADVs independently of the capacity of the Level 3 defence in depth PSVs, and is appropriate.

382. The RP has analysed three different cases of each severe accident scenario (Ref. 37). Each case has slightly varying assumptions. Three cases are presented for the ATWS (LOMFW) severe accident scenario. The three cases can be summarised as follows:

- Case 4: SADVs not actuated – RPV fails at 20,387 s at 15.9 MPa
- Case 5: SADVs actuate at 650 °C – RPV fails at 17,320 s at 0.28 MPa
- Case 6: SADVs delayed by 30 mins – RPV fails at 25,798 s at 0.28 MPa

383. Ref. 37 states that a comparison of the pressures at the time of failure demonstrate that the SADVs are effective in reducing the pressure significantly below the acceptance criteria and therefore that the SADVs are effective in preventing HPME. Whilst not stated by the RP, by a comparison of the cases above, I observe that the analysis shows that delaying opening the SADVs actually slows down core degradation and RPV failure, which may be beneficial for severe accident management. This presents a clear difference between the aim of the analysis to demonstrate the effectiveness of the SADVs, and analysis that may be used to inform SAMGs. My assessment of this area is presented in sub-section 4.8.

384. In addition to the evidence provided, in response to RQ-UKHPR1000-0545, the RP has also demonstrated that a similar depressurisation rate is observed using the LOCUST code (which has been subject to assessment in the Fault Studies topic area (Ref. 10). Moreover, the independent analysis of the SBO performed by my TSC (Ref. 15) shows a similar depressurisation rate to that presented by the RP in Ref. 37, which provides me confidence that the SADVs are sized adequately to depressurise the RCP [RCS] during a severe accident. With this in mind, I am satisfied that the RP's analysis provides reasonable predictions of the RCP [RCS] pressure transient once the SADVs have opened.

385. Given this, the relative simplicity of the calculation in comparison to demonstrating the effectiveness of IVR, I am satisfied that the RP has demonstrated that one train of the SADV is sufficient to prevent HPME during the DEC-B scenarios identified.

4.5.4.2 Assessment of Analysis for the Effectiveness of SADVs in Preventing SGTR and Containment Bypass

386. In addition to the avoidance of HPME, the SADVs perform an important role in the avoidance of creep rupture of the SG tubes which would result in a containment bypass scenario. The RP's ASTEC simulation does not model creep rupture failure of the SG tubes. The RP therefore use the calculations of SBO with and without opening of SADV in order to form arguments that the SADVs effectively prevent SG tube creep rupture (Ref. 37).

387. In response to RQ-UKHPR1000-0685 (Ref. 81) the RP updated Ref. 37 to include a justification that the SADVs are effective in avoiding creep rupture. Ref. 37 provides creep rupture data for Inconel 600 for varying pressures and temperatures. Using the conditions at the point in which the SADVs are opened (i.e. if the temperature remained constant at 717 °C and the differential pressure remained constant of 8.5 MPa) it would take at least 100 hours until creep rupture of the Inconel 600 is expected. From this the RP argues that, because Inconel 600 is similar to the alloy used in the SG tubes (Inconel 690), and as the pressure is significantly reduced following opening of the SADVs the time to failure of the SG tubes would also be significantly increased. The RP therefore concludes that the SG tubes would not fail if the SADVs are opened (Ref. 37).

388. ONR's Structural Integrity inspector has assessed the response to RQ-UKHPR1000-0685 and the information within Ref. 37 and is satisfied with that the arguments presented are appropriate (Ref. 98). I am therefore satisfied that the RP has adequately demonstrated that, in a severe accident, actuation of the SADVs should reduce the likelihood of severe accident containment bypass.

4.5.4.3 Conclusion

389. I conclude that the RP has adequately demonstrated that the SADVs are capable of effectively reducing the primary pressure in the DEC-B scenarios identified such that both HPME and creep rupture of the SG tubes is avoided.

4.5.5 Effectiveness of the EHR [CHRS]

390. During a PWR severe accident, steam and non-condensable gases are generated which can lead to overpressure and late failure of the containment (Ref. 80).

391. It is my expectation, based on IAEA SSG-2 (Ref. 6), that accident sequences with the potential to lead to an early or large release due to containment overpressure are practically eliminated. The UK HPR1000 employs two severe accidents safety features in support of meeting this expectation, the EHR [CHRS] and EUF [CFES].

392. As described in Section 3, the EHR [CHRS] is designed to be capable of removing sufficient heat during severe accident scenarios without the need for containment venting via the EUF [CFES]. The EUF [CFES] is only claimed in a severe accident scenario where the EHR [CHRS] has failed, and that its functionality cannot be restored within 12 hours.

393. To demonstrate the effectiveness of the EHR [CHRS] in severe accident scenarios, the RP has submitted deterministic analysis (Ref. 38) using the ASTEC code.

394. The RP assumes that the passive IVR is available, and that active EHR [CHRS] is unavailable until after a grace time of 12 hours. After that time the RP demonstrates that the EHR [CHRS] can reduce and maintain the containment pressure and temperature to below acceptable limits.

4.5.5.1 Assessment of Analysis of the Effectiveness of EHR [CHRS]

395. From the severe accident scenario selection process (see sub-section 4.4), the RP has selected the following DEC-B scenario as the representative case in demonstrating the effectiveness of the EHR [CHRS]:

- LB-LOCA (hot leg)

396. Unlike the analysis performed other safety features (e.g. IVR, EUH [CCGCS] and SADVs), no other scenarios have been presented. The RP states that the LB-LOCA is

chosen as it represents the fastest progressing severe accident and the fastest pressurisation of the containment out of the five accidents listed in paragraph 162. I judge this is appropriate and intuitive because the other accidents identified as part of the severe accident scenario selection process release mass and energy into the containment at a slower rate than the LB-LOCA.

397. Ref. 38 summarises the assumptions made in the analysis. Importantly, the hot leg is chosen as the break location. This is a slight variation to the DEC-B scenario considered for the analysis of the effectiveness of IVR. The RP claims that a break in the hot leg results in a larger overpressure than the cold leg break. By making a comparison to the analysis performed for IVR, I observe that the this results in a slightly slower severe accident progression than the cold-leg LB-LOCA considered for the IVR scenario (the COT setpoint is reached at 784 s (Ref. 38) as opposed to 347 s (Ref. 35)). In my opinion, it is appropriate that the RP has chosen the hot leg break as the initial depressurisation of the RCP [RCS] as it has the largest effect on the maximum pressure in the containment. The RP also states that the worst system performance is assumed for the heat removal. I have checked this against the system design manual (Ref. 50) and I am content that the RP has applied conservative performance assumptions. I am therefore satisfied that the RP has chosen the most limiting conditions and assumptions in order to demonstrate the effectiveness of the EHR [CHRS].

398. The RP has applied the following success criteria to demonstrate the effectiveness of the EHR [CHRS] immediately following a severe accident.

- If two trains of EHR [CHRS] are actuated at 12 hours after the initiating event, the containment pressure should be reduced to below [redacted] MPa within 24 hours of initiation.
- If one train of EHR [CHRS] is actuated at 12 hours after the initiation event, it should be capable of maintaining the containment pressure below the design pressure of the containment (0.52 MPa).

399. In the long term, after the above criteria are met, the objective is reach and to maintain the pressure below [redacted] MPa.

400. The RP therefore presents the analysis of the containment pressure response for three cases of the same LB-LOCA severe accident. These are:

- Case 1 – one train of EHR [CHRS] available from 12 hours onwards.
- Case 2 – two trains of EHR [CHRS] available for 12 hours onwards.
- Case 3 – no trains of EHR [CHRS] available

401. The criteria related to the 12 hours appear to be related to the RP's general safety requirements (Ref. 107), that state: "In addition, the containment system shall be designed to withstand any severe accidents considered in DEC, without taking action from the operator within the first 12 hours from the beginning of the severe accident conditions." This requirement is taken directly from the European Utility Requirements (Ref. 106) and is related to "autonomy of the operator and plant personnel", which essentially sets expected grace times before the operator takes actions.

402. However, contrary to this requirement, the RP credits manual actuation of IVR after 10 hours following the severe accident. In my opinion, the manual action required to initiate active IVR injection is a potential shortfall against the RP's own expectations. However, ONR have no specific expectations for regarding the "autonomy of the operator and personnel" related to the containment, and I judge that the criteria applied are conservative for the LB-LOCA given that the EDG and SBO generators are designed to provide power to the EHR [CHRS] (i.e. EHR [CHRS] and ECS should be

available). If the RP were to perform a similar analysis of the EHR [CHRS] for the SBO severe accident scenario, where the EDGs and SBO generators have failed, I judge that the RP's 12-hour requirement would be achievable. As a result, I judge that this apparent discrepancy does not undermine my confidence in the RP's safety case and that the acceptance criteria are appropriate.

403. The core degradation and relocation processes are similar to those considered for the IVR case and all three cases listed in paragraph 400 progress identically. In terms of the containment response, the pressure initially increases to around 0.4 MPa as the steam and water leaks into the containment. The pressure begins to decrease as heat is lost to structures and the containment wall. The pressure continues to decrease until IVR is initiated and the water in the reactor pit begins to boil increasing containment pressure. In Cases 1 and 2, at 12 hours, when the pressure is 0.25 – 0.27 MPa, the EHR [CHRS] is initiated. Condensed steam and spray water is washed back into the IRWST. The water supplied to IVR and containment spray is cooled by the ECS and the pressure decreases sharply to below acceptance criterion of [redacted] MPa within 3 hours. The pressure remains stable in both calculations between 0.1 – 0.2 MPa until the end of the calculation at 350,000 s.

404. Although the calculations were not like for like, the independent analysis carried out by my TSC (Ref. 15) also found similar containment responses. The independent analysis results show that the containment pressure reduces to below the acceptance criterion of [redacted] MPa even without the containment spray. This might indicate that the RP has applied more conservative assumptions related to heat losses to the environment than my TSC. This has provided me with additional confidence that the analysis has been performed adequately conservatively.

405. Based on the above, I am satisfied that the RP demonstrated that even when applying conservatisms in delays to operator actions (i.e. to initiate containment spray) and conservative heat removal performance, the RP has demonstrated that the EHR [CHRS] is effective in removing heat from the containment, such that long term overpressure during the DEC-B scenarios considered is prevented.

4.5.5.2 Conclusion

406. I am satisfied that the analysis presented in Ref. 38 demonstrates that the EHR [CHRS] is effective in the prevention of containment over-pressure in the DEC-B scenarios considered.

4.5.6 Effectiveness of the EUF [CFES]

407. As stated previously, the RP claims that the EUF [CFES] provides a back-up to the EHR [CHRS] and is designed to prevent failure of the containment due to long-term overpressure (Ref. 3).

408. As the EHR [CHRS] is designed to prevent containment overpressure in a severe accident alone, the EHR [CHRS] must fail in order for a demand on the EUF [CFES] to be necessary. Because of this the total sequence frequency, in which a demand is placed on the EUF [CFES] is very low (~ 8×10^{-9} pa (Ref. 102)).

409. In a severe accident scenario in which the operators determine a need to utilise the EUF [CFES], despite the presence of a filter on the discharge route (which the RP claims will significantly reduce the radioactive content of vented gases), there would still be some radiological release. It is therefore important that any decision to open and close the EUF [CFES] is informed by appropriate analysis to allow the risk of containment failure to be compared with inevitable radioactive release.

410. In this section, I do not cover the radiological consequences associated with opening the EUF [CFES]. This is covered by the RP in its source term analysis, Level 2 and Level 3 PSA, the details of which are out of scope of this report and have been assessed by the Chemistry and PSA inspector (Ref. 7 and 9). However, the results of these analyses and associated radiological consequences are important arguments for whether the design has reduced risks ALARP. My assessment of this is summarised in sub-section 4.10.

411. There is not an international consensus on whether a means of venting should be included in new PWR designs (Ref. 108). International guidance (IAEA SSG-53 (Ref. 6)) notes that the requirements for the inclusion of a vent is country specific. In a UK regulatory context, the inclusion of a vent, in this case the EUF [CFES], is related to the requirement to reduce risks ALARP and should be judged on a case by case basis. I have therefore summarised my assessment of the RP's decision to include the EUF [CFES] in the UK HPR1000 in sub-section 4.10.

412. In this section, I only address the RP's analysis which demonstrates that the EUF [CFES] is effective in reducing the containment pressure to prevent containment failure when the EHR [CHRS] has failed (Ref. 39).

413. The deterministic analysis of the EUF [CFES] has been performed using the ASTEC code. The RP assumes that the passive IVR is available, and that the EHR [CHRS] is unavailable. The EHR [CHRS] normally provides cooled water to the containment spray and the active injection into the reactor pit. Therefore an external water source is required to inject water into the reactor pit.

4.5.6.1 Assessment of Analysis of the Effectiveness of EUF [CFES]

414. From the severe accident scenario selection process (see sub-section 4.4), the RP has selected the following DEC-B scenarios as representative cases in demonstrating the effectiveness of the EHR [CHRS] in Ref. 39:

- LB-LOCA (hot leg)

415. For similar reasons to those provided for the EHR [CHRS], I consider that the LB-LOCA on the hot leg is appropriate for consideration.

416. As stated, the analysis assumes that the EHR [CHRS] has failed. This assumption is required in order to analyse the effectiveness of the EUF [CFES] (as EUF [CFES] is not required if EHR [CHRS] is successful). However, EHR [CHRS] is the system that provides active flow to the IVR subsystem after the IVR passive filling tank has depleted (at around 10 hours). Therefore it is assumed in the analysis that a mobile water source can supply water externally, and that IVR is still successful.

417. Without mobile equipment, IVR would fail and a demonstration of effectiveness of EUF [CFES] would be meaningless as the corium could potentially cause ex-vessel steam explosions and MCCI. It is therefore a necessary assumption that the mobile equipment is available. Besides it being necessary to perform a meaningful assessment, I consider that this is a reasonable assumption as the mobile equipment is only required after 10 hours (see sub-section 4.8 for a summary of my assessment on mobile equipment). Moreover, sequences in which EUF [CFES] is required have a frequencies of the order of magnitude of 10^{-9} pa (Ref. 102). I therefore consider that the RP's assumption that IVR is successful (requiring mobile equipment) is appropriate.

418. The analysis results (Ref. 39) show that the containment pressure progresses in a similar way to that presented for the EHR [CHRS] (Ref. 38) up to the point of 10 hours after the 650 °C COT setpoint is reached. At this point, external injection is actuated

and instead of containment pressure declining, the pressure continues to rise as further steam is generated from the water injected. At approximately 62 hours after the initiating event, the EUF [CFES] is assumed to be opened when the design limit is reached. The EUF [CFES] then reduces containment pressure whilst filtering a large fraction of radioactivity from the gases released.

419. However, the filtration capacity is limited as the chemicals within the filter that absorb the radioactivity ae depleted. The filters must therefore be replenished (after 12 hours of operation) so that their filtration function is restored. During this time, the vent remains closed to prevent unfiltered releases of radioactivity.

420. The analysis (Ref. 39) shows that once opened, the pressure reduces gradually over 12 hours to approximately 0.38 MPa. It is assumed at this point that the filtration capability of the EUF [CFES] is depleted and therefore the isolation valves are closed. The pressure then begins to rise again at a similar rate to that prior to opening and the calculation ends at 84 hours.

421. After the filtration capability of the EUF [CFES] is depleted, the RP states that the EUF [CFES] can be replenished within 8 hours, and that the analysis demonstrates that this time is available (Ref. 39). However, elsewhere in the safety case (for example Ref. 109) and in response to RQ-UKHPR1000-1444 and RQ-UKHPR1000-1476 (Ref. 81), the RP has stated that the EUF [CFES] will not be replenished, as there is sufficient available time to implement other strategies between the initiating event, the demand on the system (62.5 hours) and the time until it would be required for a second time (>84 hours).

422. There is no clear safety case claim on whether the EUF [CFES] will be demanded again. This has important implications for whether any consumables (e.g. chemicals) are made available on site in order to replenish the EUF [CFES] so that it can be used multiple times after the first initial 12 hours. Whilst the RP has provided evidence that in principle the EUF [CFES] can reduce the pressure sufficiently, the details of how it will be used are unclear and will affect storage of consumables on site. The decision on whether the strategy will be to restore the EHR [CHRS], or to store sufficient stocks to replenish the EUF [CFES] multiple times is a decision for a licensee and may depend on the site layout and space available. Because the safety case position is unclear, and because it has potential implications for storage I have raised the following assessment finding to be resolved by the licensee:

AF-UKHPR1000-0081 – The licensee shall, as part of detailed design and as part of development of severe accident management guidelines, determine the required stocks of consumables to replenish the containment filtration and exhaust system. If necessary, the requirement for replenishment should be included in the severe accident management guidelines.

423. Nevertheless, the analysis clearly demonstrates that the EUF [CFES] would be effective to reduce the pressure below the containment design pressure, and demonstrates that 8 hours are available for replenishment of the EUF [CFES] should it be required.

4.5.6.2 Conclusion

424. I consider that there are inconsistencies in the RP's safety case regarding replenishment of the EUF [CFES] filter beds and have raised AF-UKHPR1000-0081 to resolve the issue at the point of compilation of the SAMGs by the licensee.

425. Nevertheless, the shortfall does not alter the fact that the RP has demonstrated that the EUF [CFES] will be capable of reducing the containment pressure to below the

containment design limit in the DEC-B scenario analysed, and that adequate time should be available for replenishment should the severe accident management strategy require it.

4.5.7 Re-Criticality Analysis

426. A common accident mitigation strategy is to reflood the core to both slow down or prevent core degradation or aid heat removal from relocated corium. Reflooding the core has the potential to cause moderation and result in re-criticality, which can result in additional heat loads which effect the progression of a severe accident. There are several water sources available that could be used during a severe accident. The most commonly used water sources on site used are either boronated water or demineralised unboronated water.

427. During a severe accident, there is a hypothetical period of time in which the RCCAs have melted but the fuel geometry remains intact. This is due to the difference in melting temperatures of the structures. This period is of the most concern as the all rods that normally keep the reactivity low have melted and the design of the core is such that it's geometry is favourable for criticality (Ref. 80).

428. In the RP's analysis (see Ref. 35 for example) as the core relocation progresses, the geometry of the core is lost and core debris is relocated downwards and stops temporarily upon the large LSP. In this configuration the moderator effect reduces and the margin to criticality increases. Once the core has completely relocated to the lower head, the risk of re-criticality will be further reduced as the geometry becomes even less favourable with less moderator available.

429. The RP has analysed the potential for re-criticality throughout this process if the core was to be reflooded, the results of which are presented in Ref. 85. This analysis supports the RP's arguments that reflooding would not cause re-criticality, it would not affect the assumptions made in the analysis of IVR and that it is a feasible strategy for severe accident mitigation of the UK HPR1000.

430. The re-criticality effect is not captured by most severe accident codes (SRS No. 56 (Ref. 6)) and therefore requires other more specialist codes to investigate its potential. The ASTEC code is used to analyse the progression of the LB-LOCA severe accident. Relevant information such as the mass distribution of the core melt is obtained as the input to the JMCT code which is used to carry out criticality analysis to obtain the effective multiplication factor, k_{eff}.

431. The JMCT code has been subject to assessment by ONR's RP inspector (Ref. 110). The relevance of the ONR's RP assessment to this assessment is summarised in sub-section 4.6.

4.5.7.1 Assessment of Analysis of Re-Criticality

432. The RP's analysis is presented in a dedicated re-criticality report (Ref. 85). This presents three states:

- State 1 - after the core uncovers the control rods have melted but the fuel geometry remains intact;
- State 2 - a significant molten pool is formed in the core region before relocation to the lower head; and
- State 3 - molten corium relocates into the lower head and forms a molten pool.

433. Intuitively, I would have expected the most limiting case for re-criticality should be when the fuel remains intact and the control rod structures have melted, which the RP has covered in State 1. I welcome the fact that the RP has not only analysed this state,

but also expanded its consideration to the other scenarios, thereby ensure a good range of core geometries are considered to demonstrate its safety case claims

434. An important assumption is made related to the water that is injected into the core. Whilst both boronated and unboronated water will be available to inject into the core during the core degradation process, the RP assumes that only water that is boronated is injected. The RP has stated (Ref. 27) that in a 'real world' scenario only boronated water will be injected into the core in severe accidents. I judge, however, that it is conceivable that a scenario may arise in which an operator may choose to inject unboronated water to the core to prevent further degradation. This is because to reach a severe accident, the boronated water is likely unavailable in the first place. The substantiation related to the ability to inject unboronated water will be dependent on the future SAMGs. For example, the SAMGs may state explicitly that no unboronated water should be injected. However, the development of SAMGs is normal business for a licensee, and I judge that it is likely that these aspects will be considered during the development of these SAMGs as part of normal business. I am content that this will be picked up as normal business in future permissioning activities.

435. In terms of the assumptions made in the analysis (Ref. 85), the RP has explained in response to RQ-UKHPR1000-1130 (Ref. 81) the reasoning for the input parameters such as fluid density, internal pressure, time in core life, debris porosity and fragment size. The RP asserts that the calculation includes overly conservative assumptions and that it represents an unphysical situation. Moreover, as is good practice when using a criticality code, the RP has provided sensitivity analyses on the fragment size and porosity for the appropriate cases (Case 2 & 3), which demonstrate low sensitivity. For State 1, the RP has provided sensitivity studies on the melting fraction of the control rods, which also shows low sensitivity. I am satisfied that the RP has chosen appropriate parameters to perform sensitivity studies and that the approach is reasonable.

436. The analyses demonstrate that State 1 is indeed the most limiting case. Nevertheless, the RP demonstrates positive margin to re-criticality in all cases. I am satisfied for the purposes of GDA that the RP's approach is adequate, and that the RP has demonstrated that if only boronated water is injected then re-criticality will not be reached.

4.5.7.2 Conclusions

437. The RP has provided adequate demonstration that the injection of boronated water for reflooding of the core will not result in re-criticality in the most limiting point in time for the LB-LOCA, which is the fastest progressing DEC-B scenario considered in the RP's severe accident analysis.

4.5.8 Strengths

438. The RP has performed deterministic analysis of the DEC-B scenarios identified to demonstrate the effectiveness of the severe accident safety features. This approach aligns well with the general expectations for SAPs FA.15, FA.16 (Ref. 2) and IAEA SSG-2 (Ref. 6).

439. The RP has used best estimate methodologies, appropriate assumptions and conservatisms for the purposes of GDA. This approach is also aligned with the expectations of SAPs FA.15, FA.16 (Ref. 2) and IAEA SSG-2 (Ref. 6).

440. In particular, for the purposes of GDA, I am satisfied that the RP has, through its deterministic analysis, demonstrated that:

- The IVR sub-system is effective in retaining corium within the RPV, such that the conditions for ex-vessel steam explosions and MCCI are not reached.
- The EUH [CCGCS] is effective in reducing the hydrogen to safe levels such that the conditions necessary for combustion modes that could challenge the containment are avoided.
- The containment layout and layout of the EUH [CCGCS] adequately enables hydrogen management.
- One train of the SADV is sufficient to depressurise the primary circuit which prevents creep rupture of the SG tubes, enables IVR and prevents the conditions necessary for HPME and DCH from occurring.
- The EHR [CHRS] is effective in removing heat from the containment, such that the design pressure of the containment is not challenged.
- In the low probability sequence that EHR [CHRS] has failed, the EUF [CFES] is effective in reducing the containment pressure to safe levels.
- Re-criticality will not be reached if boronated water is injected during degraded core conditions.

4.5.9 Outcomes

441. I have identified two minor shortfalls related to the assumptions made in the MOPOL analysis and the RP's demonstration that the conditions for global detonation are not reached (sub-section 4.5.3).

442. Due to limitations of the safety case, as reported in sub-section 4.5.2, 4.5.3 and sub-section 4.5.6, I have raised Assessment Findings AF-UKHPR1000-0079, AF-UKHPR1000-0080 and AF-UKHPR1000-0081.

4.5.10 Conclusion

443. Based on the outcome of my assessment of the severe accident analysis, I have concluded that the RP has adequately demonstrated the effectiveness of the UK HPR1000 severe accident safety features for the purposes of GDA.

444. In general, the RP's analysis is aligned with the expectations of SAPs FA.15, FA.16, FA.25 (Ref. 2), SSG-2 (Ref. 6) and NS-TAST-GD-007 (Ref. 4).

4.6 Assessment of the Severe Accidents Codes

445. Throughout section 4.5, I have provided information related to the codes and methodologies employed in the analyses supporting the RP's safety case. This section presents my assessment of the verification and validation which supports the use of these codes in the analyses.

446. The following codes have been used to perform severe accident analyses in the RP's safety case:

- ASTEC V2.1 – A severe accidents integral code which allows for modelling of the core, reactor coolant system and the containment of a PWR. The code is used to determine the effectiveness of all the severe accident management strategies and as an input to the PSA.
- GASFLOW-MPI – A CFD code used to determine the global thermal hydraulics and hydrogen distribution in the containment, as well as local risks of hydrogen accumulation.
- MOPOL – A Monte-Carlo code used to evaluate the uncertainty on the heat flux on the outer surface of the RPV during implementation of the IVR strategy.
- MC3D – This code is used to simulate ex-vessel steam explosions and the resulting impulse which can threaten the containment.

- Finite element codes – These codes are used for mechanical analysis of the RPV in the IVR condition. The application of the code is in the scope of the Structural Integrity assessment (Ref. 98).
- JMCT – This is a criticality code used to determine whether re-criticality occurs during late re-flooding.

447. The RP has summarised the applicability of the ASTEC, GASFLOW-MPI, MOPOL and MC3D codes in Ref. 40. These codes have been reviewed by my TSC in order to determine their applicability in the UK HPR1000 safety case (Refs 16 to 21). Since the ASTEC code is used in the bulk of the RP's analysis I have chosen to target the verification and validation and sensitivity studies related to this code in my assessment. In addition, a detailed review of the GASFLOW-MPI code has also been performed by my TSC. Regarding the MOPOL and MC3D codes, these codes are only used as a small part of the RP's justification. My TSC's review of MOPOL and MC3D codes was therefore commensurate with the significance of the arguments that they support.

448. In my assessment of these codes I have applied the expectations of SAPs AV.1, AV.2, AV.3, AV.5, AV.6 (Ref. 2) and NS-TAST-GD-042 (Ref. 4) where appropriate. For ASTEC and GASFLOW-MPI, the summary of my assessment makes links to the specific expectations of these SAPs. However, for the others I have taken a graded approach and my summary is against higher level expectations.

449. ONR's SAP AV.4 relates to the proficiency of the code users, quality assurance of the codes and the datasets used in the analysis. I have not applied the expectations of AV.4 in its entirety for the following reasons:

- The GASFLOW-MPI and ASTEC codes are both third party codes which are well established internationally and widely used in the severe accidents community. It is my expectation that the amount of effort related to quality assurance is related to the safety significance of the arguments which the codes support, therefore I expect that severe accidents codes should generally attract a lower level of attention of quality assurance than design basis codes. Since the GASFLOW-MPI and ASTEC codes are well established and internationally recognised, I have made the assumption that the quality assurance aspects of these codes will be at least as good as those expected for a severe accident code and I have chosen not to target their associated quality assurance aspects.
- Furthermore, I have chosen not to carry out any assessment of the RP's procedures for the development, maintenance and application of datasets. I have taken assurance from the fact that the RP's general approach has been considered by other ONR colleagues in relation to design basis analysis and found to be satisfactory (Ref. 10) and that the RP has for many years been carrying out severe accident analysis using integral codes.

450. However, I have chosen to sample the proficiency of the user of the ASTEC code, as it is the first time that the RP has used the ASTEC code to support licensing applications.

451. SAPs AV.7 (data collection through life) and AV.8 (update and review) will primarily be of relevance to the licensee. I would expect the licensee to learn from future developments in severe accident research and improved understanding of plant accidents, and to revise analysis for the UK HPR1000 as required after GDA.

452. The RP has also performed several experiments associated with the IVR strategy. The most important for supporting claims related to IVR being experiments related to CHF measurements, which were performed in the REVECT-II facility. The heat fluxes for the DEC-B analyses are predicted by the ASTEC and MOPOL codes. The success of the IVR strategy is measured by the RP through a comparison of predicted RPV heat

fluxes with the CHF curve derived from the REVECT-II experiments. I have therefore treated the validation of the CHF curve separately to these codes. My assessment of this aspect is presented in 4.6.4 below.

4.6.1 ASTEC V2.1

453. The ASTEC code is an internationally established best estimate code developed by IRSN. Amongst other things, it is capable of modelling progression from initiating events, through core melt, thermal hydraulic behaviour of the containment and behaviour of fission products (Ref. 80).

454. Inevitably, many severe accidents calculations have large uncertainties associated with them. This is mainly due to the limitations of knowledge, scaling of small scale experiments to full scale, and feedback of uncertainties from one part of the code to another (Ref. 80).

455. Because of this, the RP has provided sensitivity analysis related to the largest uncertainties to demonstrate that even with these large uncertainties applied, the safety features are still predicted to be effective (Ref. 46 and 47). Since the uncertainties cannot be eliminated, my assessment has focussed on the uncertainties and the RP's sensitivity analyses.

456. In the following subsections (sub-sections 4.6.1.1 to 4.6.1.3) I summarise my assessment of the ASTEC code, the sensitivity analyses performed by the RP and the UK HPR1000 model which has been built by the RP.

4.6.1.1 Verification and Validation of the ASTEC code

457. The RP has provided verification and validation documentation for the ASTEC V2.1 code (Refs 41 and 42). The documentation provides an explanation of the theoretical models and the experimental data that validate the models implemented in the ASTEC code. NS-TAST-GD-042 (Ref. 4) states that the limits of application, details of the models used, details of numerical methods, correlations used, treatment of uncertainty and details of experiments should be included in verification and validation documentation. The RP's submissions therefore meet my expectations for what should be included in a validation report. This, therefore meets my expectations for AV.5, that appropriate validation documentation should be provided.

458. My TSC reviewed the ASTEC code against ONR's SAPs (Ref. 2), NS-TAST-GD-042 (Ref. 4) and IAEA SSG-2 (Ref. 6). However, in addition to the general expectations for the verification and validation of codes provided in the SAPs (Ref. 2), my TSC also performed a review against expectations it derived from IAEA's Safety Reports Series: 'Accident Analysis for Nuclear Power Plants' and 'Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants' (Ref. 6). Independent of the application within the UK HPR1000 safety case, my TSC made the following observations about the ASTEC code (Ref. 20):

- The ASTEC code reproduces with good accuracy the plant characteristics and most of the phenomena that occur during a severe accident as well as severe accident management strategies.
- Complete documentation and training programmes are available.
- The code is subjected to systematic validation procedures through a number of international programmes along with a peer review.
- The code has a strong user group.
- The code is supported by comprehensive publications to facilitate the review of the models and correlations.
- The code is internationally recognised and an accepted severe accident tool.

459. On the basis of the above, my TSC advised that the code is clearly applicable for use for severe accident analysis and source term analysis of the UK HPR1000, and that a comprehensive validation of the thermal hydraulics models and physiochemical models exists (Refs 16 and 20).

460. Informed by my TSC's findings (Ref. 20), I judge that the code is capable of adequately representing the physical and chemical phenomena associated with severe accidents in a PWR such as the UK HPR1000.

461. In Ref. 40, the RP has described how these physical and chemical models represent a severe accident in the UK HPR1000. I judge that the RP has provided an adequate justification as to why the theoretical models within the ASTEC code represent those of the UK HPR1000 and I am satisfied that the expectations of AV.1 are met . Based on my TSC's findings and Ref. 20, I am satisfied that the expectations of AV.2 have been met, and that the physical and chemical phenomena that would occur in a severe accident in the UK HPR1000 are adequately represented by the ASTEC code.

462. My TSC's review (Ref. 20) found, however, that the areas of major uncertainty of the ASTEC code when applied to the modelling of a severe accident in the UK HPR1000 were as follows:

- Onset of melt relocation – large uncertainties related to the degradation mechanisms of in-core materials exist (i.e. loss of integrity criteria, dissolution of cladding and fuel and the melting temperatures of the in-core structures).
- Corium slumping into the lower plenum – there are large uncertainties in the relocation criteria applied (user defined), the flow rate of corium to the lower head and the phase separation of the corium pool.
- Iodine chemistry in the containment – the major uncertainties relate to partition coefficients, iodine adsorption and desorption coefficients and iodine chemical reaction rates.

463. The areas of uncertainty listed above have large impacts on the modelling of IVR, hydrogen management and the source term analysis. To account for these uncertainties identified above, the RP has produced sensitivity analysis for IVR (Ref. 46), hydrogen management (Ref. 47) and source term analysis (Ref. 112). My assessment of the sensitivity analyses for IVR and hydrogen management is presented below in turn. The assessment of the sensitivity analysis for the source term is presented in ONR's Chemistry assessment report (Ref. 7) and is out of the scope of my report.

4.6.1.2 The RP's ASTEC Model of the UK HPR1000

464. The UK HPR1000 ASTEC model has been reviewed by my TSC (Ref. 20) in order to confirm that it has been appropriately built. The model consists of three main parts, the thermal hydraulics model (CESAR module), the core region (ICARE module) and the containment (CPA module).

465. Regarding the thermal hydraulics, my TSC found that the RP has provided an adequate description of the primary and secondary circuit of the UK HPR1000 simulation, and that the RP has used appropriate structures in the RCP [RCS] and secondary side (e.g. the U tubes of the SG primary side and the rising part of the SG secondary side, which can be particularly problematic). Based on my TSC's review (Ref. 20), I consider that the primary and secondary circuit modelling adopted by the RP is in line with the recommendations of the user manual and sufficiently detailed to capture the thermal-hydraulic phenomena occurring in the RCP [RCS] and SGs during a severe accident.

466. Regarding the core, the RP has modelled the UK HPR1000 core region using 6 radial rings and more than 20 axial levels. Based on my TSC's review (Ref. 20), I consider that this core nodalisation is in line with the best practice developed by IRSN and sufficiently detailed to describe the core degradation phenomena taking place during a severe accident. Moreover, the model of the core is similar to that built independently in my TSC's analysis of IVR (Ref. 14). With this in mind, I am content that the modelling of the core is appropriate.

467. Regarding the containment, the RP has modelled the UK HPR1000 reactor building using 17 zones. The RP states that this is because the slow convective processes which characterise the hydrogen distribution in the containment are evaluated using CFD calculations while the ASTEC code is utilised to evaluate the overall containment response, containment safety system behaviour and the gas distribution for postulated severe accident sequences. Whilst the simplified CPA containment nodalisation appears to be quite coarse, the RP has demonstrated in response to RQ-UKHPR1000-0545 (Ref. 81) that this can reproduce similar results to the ones predicted by the GASFLOW-MPI code regarding the hydrogen and steam concentrations as well as temperature evolution in the containment compartments. Based on my TSC's review (Ref. 20) and the evidence provided in response to RQ-UKHPR1000-0545, I therefore consider that the containment nodalisation developed by the RP is appropriate to capture the main thermal-hydraulic phenomena occurring in the containment during a severe accident as well as to identify the main bounding scenarios for the hydrogen risk.

468. The IVR tank, injection lines, ERVC channel and recirculation pipes have been modelled using the CESAR module. The RP claims that the requirements (for example flow rates, filling times etc.) have been confirmed by the REVECT-II facility (Ref. 92). These are relatively simple requirements to confirm, and I have not sampled these experiments.

469. Based on the above, and my assessment of the deterministic analysis which shows a clear link between the design and performance of systems, I am satisfied that the RP's ASTEC model of UK HPR1000 is reflective of the actual design, and that my expectations for AV.3 have been met.

4.6.1.3 IVR Sensitivity Analyses

470. The RP has performed sensitivity analysis to account for the largest uncertainties in the code which affect IVR. Ref. 46 provides sensitivity analyses, using the LB-LOCA, for a range of phenomena. In this section I summarise my assessment of whether the sensitivity analysis provided for IVR meets my expectations for AV.6. My assessment has been carried out in coordination with the Chemistry inspector (Ref. 7) and informed by the TSC that has been commissioned by the Chemistry inspector (Ref. 95) to review the sensitivity analyses, and also my TSC's review of the computer codes.

471. The RP has performed sensitivity analyses for all phenomena recommended for investigation in the In Vessel Melt Retention (IVMR) 2020 project (Ref. 112), except for the transient establishment of heat transfers and correlation of heat transfer in the upper metal layer. The IVMR 2020 project is a multinational collaboration aimed at developing understanding and modelling of phenomena associated with IVR, and harmonising techniques to establish good practice in the area of deterministic analysis of IVR. Regarding the omissions in sensitivity analysis, my TSC has confirmed that these cannot be performed by the RP due to a limitation of the ASTEC code (Ref. 20), which is not in the gift of the RP to resolve. Whilst this appears to be a shortfall, my TSC has also noted that the phenomena are most important for the focussing effect. However, the metallic layer is predicted to be quite large in the RP's analysis such that the heat flux associated with the layer is spread out and the focussing effect is weak

(see sub-section 4.5). Because of this, I judge that even if it were possible to provide sensitivity analysis related to the focussing effect, this will not have a large impact on whether IVR is successful, and I therefore judge that the omission of these sensitivity analyses is acceptable.

472. For every phenomenon analysed by the RP, I judge that the RP provides an adequate explanation of the impact of the key parameters on the results. My TSC has confirmed that the ranges of values adopted for the input parameters are consistent and the calculation produces expected outputs (Ref. 20).

473. The results of the sensitivity analyses show that the predicted vessel minimum residual thickness is between 3 cm and 5.5 cm and the heat flux exceeds the CHF only in one case for a brief period of time (Ref. 46). RPV failure is predicted for only one case where 100% decay heat is relocated to the lower plenum, which is deemed very unlikely by my TSC (Ref. 20) and by the Chemistry inspector's TSC who has reviewed the IVR sensitivity analysis (Ref. 95). The inclusion of unfavourable results is encouraging, and is indicative that the RP has provided a balanced view, meeting my expectations for SAP SC.5 (Ref. 2).

474. With regards to the melting temperature of the fuel, the RP presents analysis of a range between 2450 and 3050 K. The melt temperature impacts the thermal load and the timing of relocation. The analysis shows that the most limiting condition is when the melting temperature is lowest because it has a significant impact on the timing of the relocation to the lower head. I judge that the sensitivity studies support the RP's arguments that the lower liquidus and solidus temperatures, which are recommended by IRSN in the code user manuals, should be used in the analysis.

475. Some experiments (e.g. MASCA (Ref. 80) have shown that some of the lighter metals that reside at the top of a corium pool, can undergo complex interactions with heavier metals (such as uranium) in the oxide pool and sink to the bottom due to the larger density of the mixture (Ref 80). After a relatively short period of time this layer consisting of heavy metals and light metals, breaks up and the light metals rise to the top of the corium pool. This process is sometimes referred to as layer inversion, and models that simulate this behaviour are sometimes referred to as the three layer model. The resulting postulated mix is not as simplistic as a purely metallic and purely oxidic layer. Using models to simulate this behaviour results in periods during this process in which the metallic layer is much thinner than that predicted by the more simplistic two-layer model. However, it is worth noting that there is still large uncertainty associated with this process, research is still going on in the area, and that there is not international consensus on how corium behaviour should be modelled.

476. Instead, the RP has used the simple phase separation model (sometimes referred to as a "two-layer model") for the majority of its analysis. However, as it recognises that some experiments suggest that layer inversion could occur, the RP has also performed analysis using the thermo-chemical equilibrium phase separation model (which allows for layer inversion) (Ref. 46). The results show that the retention of fission products (and therefore heat) within the metallic layer have the largest effect on the analysis. In comparison to the two-layer model, the maximum heat load is therefore at a higher azimuthal angle (higher up, because the metallic layer stratifies at the top of the corium pool). In addition to the additional decay heat in the metallic layer, it has also been observed in the IVMR2020 project (Ref. 20), that the transient effects (discussed above) can lead to a thinner metallic layer and an enhanced focussing effect. However, the RP has demonstrated that this transient effect does not enhance the heat focussing effect in its analysis when using the thermo-chemical equilibrium phase separation model (Ref. 46). Using the thermo-chemical equilibrium model, the RPV thickness is reduced to 3.5 cm, which is smaller than the base case (4.15 cm). Nevertheless, the minimum thickness is greater than the "cold-layer" thickness used in

the finite element analysis, and the RP concludes that no RPV failure is expected. In its arguments, the RP highlights that there is no international consensus regarding which models to use and that further research is ongoing (Ref. 3). Based on this, and the results from the sensitivity analysis, I consider that the use of the simple phase separation model for the base cases in the severe accident analyses is acceptable. These arguments have also been assessed by the Chemistry inspector who has come to the same conclusion (Ref. 7).

477. The sensitivity studies have only been performed on one parameter at a time. I judge that whilst more limiting cases would be discovered using sensitivities across a combination of parameters, the RP has already demonstrated that there are large margins in its current sensitivity studies and that any such sensitivity studies would be unlikely to impact the design. Moreover, my TSC, as part of its confirmatory analysis work (Ref. 15), performed uncertainty analysis which showed combinations of variations of similar parameters did not lead to cliff-edge effects. The independent analysis also shows that the parameters chosen by the RP were indeed the ones that led to the largest variations in heat flux, which provides me with additional confidence that the correct parameters have been chosen by the RP for sensitivity studies.

478. Based on my TSC's review of the RP's sensitivity analysis, I am satisfied that the RP has performed sensitivity analysis on the correct parameters, has demonstrated that there are no cliff-edge effects associated with those uncertainties and that the expectations of SAP AV.6 have been met.

4.6.1.4 Hydrogen management sensitivity analysis

479. The RP has performed sensitivity analyses on the most limiting fault, the IB-LOCA, to investigate the impact of the ASTEC input parameters on the hydrogen behaviour inside the containment (Ref. 47). As the ASTEC analysis is used to generate a hydrogen mass and energy release for the GASFLOW-MPI analysis, the uncertainties are promulgated. Therefore, the uncertainties here also are related to uncertainties for the GASFLOW-MPI analysis of the local effects.

480. The key phenomena investigated by the RP are widely recognised as areas that result in large uncertainties (IAEA-TECDOC-1661, Ref. 6). The RP has also provided sensitivity analyses for partial non-functionality of the PARs and spurious activation of the containment spray.

481. My TSC (Ref. 20) observed that the analysis shows the amount of hydrogen generated is sensitive to the following:

- The zirconium oxidation model – The ASTEC code is capable of applying different models that simulate oxidation of the zirconium cladding. The analysis demonstrates that the zirconium oxidation default model (BEST-FIT) used by the RP actually provides the most conservative results for the hydrogen cumulative mass generated compared to other models (e.g. RATER, CATHCART).
- The liquidus and solidus temperatures input by the user – As stated previously, the user can manually enter the liquidus and solidus temperatures of the fuel. The RP's analysis demonstrates that the most challenging scenarios are the ones related to artificially increasing these temperatures. This is because the rise of the melting temperature allows the core to remain for a longer time in a rod-like geometry, leading to a higher hydrogen cumulative mass generated (around an additional 30%).
- Efficiency of the PARs - the RP presents partial failure or reduced efficiency of the PARs (down to a reduction of 50% hydrogen removal rate). The analysis results show that this does not affect the hydrogen maximum local

concentration, but leads to a higher hydrogen average concentration in the containment, throughout the accident. This is because the reduced recombination rate of the PARs affects only the time necessary for the hydrogen to reach a state in which the PARs are recombining as much hydrogen as is being generated.

- Containment spray – As stated previously, containment spray condenses steam in the containment and has the potential to increase the relative concentration of hydrogen. The RP has also provided sensitivity analysis of spurious activations of the containment sprays at different times during the accident. The RP has demonstrated that this has a limited effect on the local maximum concentrations and the maximum average hydrogen concentration calculated in the open compartment. The RP demonstrates that out of all of the cases analysed the maximum average hydrogen concentration remains below 7% and that the conditions for flame acceleration are avoided.

482. Out of all of the sensitivity analyses performed, the maximum hydrogen mass generated in the RPV predicted by the ASTEC code varies between 445 kg and 621 kg; this higher value would lead to a local concentration in the pressuriser compartment above the 13.3 % hydrogen by volume as found for the reference case. However, as noted previously, the RP has applied a conservative assumption that all zirconium cladding is oxidised when analysing the local effects. This means that although the ASTEC analysis of the base case IB-LOCA predicts that a total of 445 kg of hydrogen is generated, when conservatively scaled up to 100% oxidation for the GASFLOW-MPI analysis, the assumed hydrogen generation is > 900 kg. In my opinion the 100% oxidation assumption used in the GASFLOW-MPI analysis is bounding of all of the uncertainties in the ASTEC analysis. I am therefore satisfied that the uncertainties promulgated to the GASFLOW-MPI analysis are adequately accounted for.

483. I am satisfied that the RP has performed sensitivity analysis on the correct parameters, has demonstrated that there are no cliff-edge effects associated with those uncertainties and that the expectations of SAP AV.6 have been met.

4.6.1.5 User Proficiency

484. At Ref. 113, as part of a technical meeting with the RP in China, I reviewed the RP's ASTEC user proficiency. I found that adequate arrangements for management of training, delivery of classroom and on-the-job training, training materials, assessment and keeping of records were in place to ensure that users of the ASTEC code were suitably qualified and experienced to perform severe accident analyses. I also recognise that the RP has been supported by the code developer, IRSN, to ensure that the calculations performed have used the appropriate models and recommended input parameters. I am, therefore, satisfied that the arrangements in place are well aligned with those described in NS-TAST-GD-042 (Ref. 4).

4.6.1.6 Conclusions

485. I commissioned my TSC to perform a review of the ASTEC code. My TSC's review found that whilst the ASTEC code was clearly applicable for use for the UK HPR1000 severe accident analysis, the analysis should be supplemented by additional sensitivity studies to account for significant uncertainties. As described the RP has provided the necessary uncertainty analyses.

486. I conclude that the validation of the ASTEC code is extensive, the sensitivity studies provided by the RP are comprehensive, and the arrangements in place for user proficiency are adequate. The identification of the areas of uncertainty meet my expectations of a balanced safety case and satisfy SAP SC.5 (Ref. 2).

487. I therefore consider that my expectations for SAPs AV.1, AV.2, AV.3, AV.5 and AV.6 (Ref. 2) and NS-TAST-GD-042 (Ref. 4) have been met and I have confidence that the ASTEC code is suitable for use in the UK HPR1000 Severe Accident Analysis safety case.

4.6.2 GASFLOW-MPI

488. The GASFLOW-MPI code is a well-established CFD / field code developed by Karlsruhe Institute of Technology (KIT). The GASFLOW-MPI code is a best-estimate code for predicting the transport, mixing and combustion of gases in nuclear reactor containments. The GASFLOW-MPI code is a development of the earlier GASFLOW code and now incorporates the ability to simulate combustion to assess the risk of flame acceleration and DDT and the pressure loads from combustion on containment structures. The GASFLOW code, (i.e. not GASFLOW-MPI), was used for combustible gas risk assessment in the UK EPR GDA. GASFLOW does not include the combustion models and was only used to assess the risk of combustion.

489. It is my expectation that adequate documentation is provided to support the use of the codes used in GDA and to facilitate review of the adequacy of the analytical models and data. The RP has submitted verification and validation documentation for the GASFLOW-MPI code (Ref. 43), which has been reviewed by my TSC (Ref. 21).

490. The information provided fulfils the majority of ONR's expectations for documentation to be submitted to support the use of a code. However, my TSC found that the quantification of uncertainty had not been supplied in the verification and validation documentation, and made a recommendation for the RP to quantify uncertainties for the UK HPR1000 containment model. This is a shortfall against the expectations of AV.5 and NS-TAST-GD-042, that the uncertainties should be quantified. However, my TSC also pointed out that there are large conservatisms related to the mass and energy release (derived in ASTEC) which will likely cover any uncertainty (Ref. 21). My expectations for the level of confidence required for severe accident codes are lower than what I would expect for codes that support more safety significant arguments (e.g. for codes that inform the design basis). This is because there are much larger uncertainties, limited by both human knowledge, computing power, and the inherent uncertainties and because the significance in risk is much lower (severe accidents are far less likely to occur).

491. Based on this, and the assurance from my TSC that the uncertainties in the boundary conditions generated by ASTEC and used in GASFLOW-MPI are large, I judge that it would be disproportionate to request that the RP also perform uncertainty analysis using the GASFLOW-MPI code. Moreover, the RP has used a very conservative assumption that 100% of the zirconium cladding is oxidised. It is my judgement that requesting additional documentary evidence of the quantification of uncertainty in GASFLOW-MPI will have limited impact on my overall conclusions on the adequacy of UK HPR1000 design and supporting safety case for hydrogen combustion. On that basis, I am satisfied that the RP has provided adequate documentation for the code for me to conduct a review against the expectations of SAP AV.5. However I have identified this as a minor shortfall against my expectations that details of uncertainty should be provided as the safety case does not provide reasons for why it is not necessary.

492. I have not assessed the user proficiency in detail but I take confidence from my assessment of the ASTEC code that adequate arrangements are in place to ensure staff are proficient for the use of the GASFLOW-MPI code for severe accident analysis.

493. My TSC's review of the GASFLOW-MPI code (Ref. 21) found that the code is widely used in the nuclear industry for hydrogen analysis in reactors and is also applicable for

the assessment of the UK HPR1000. In addition, my TSC has found that the GASFLOW-MPI code is similar in its approach and capabilities to equivalent CFD codes (for example ANSYS CFX). Moreover, my TSC considers that the meshing is appropriate and adequately reflects the UK HPR1000 containment. I am therefore satisfied that the expectations of SAP AV.1 has been met.

494. My TSC found that the verification and validation report clearly identified limitations of the code, had presented adequate comparisons of analytical solutions and experimental data, and had a complete validation base for GASFLOW-MPI (Ref. 21). I am therefore satisfied that the expectations of SAPs AV.2 and AV.3 have been met.

495. In terms of shortfalls in validation, my TSC identified that there is a known bias related to wall functions within the GASFLOW-MPI code, which do not adequately model condensation on the walls in near stagnant flow conditions, and that mesh sensitivity should be systematically performed to quantify the related bias (Ref. 21). Encouragingly, the RP had already recognised this bias and provided mesh sensitivity analysis at Ref. 90 which demonstrated that calculations were not sensitive to mesh size. In my opinion, this, and the assumption of 100% zirconium-steam reaction in the local effects analysis (Ref. 90), demonstrates that there are no cliff edge effects associated with the varying of the most sensitive parameters. This meets my expectation for AV.6.

496. To summarise, based on my TSC's review of the GASFLOW-MPI code, I am satisfied that the appropriate expectations of AV.1 – AV.3, AV.5 and AV.6 and NS-TAST-GD-042 have been met, and have confidence that the code is appropriate for its use in the Severe Accident Analysis safety case.

4.6.3 Other codes

4.6.3.1 MOPOL

497. The MOPOL code is a Chinese code, developed by Shanghai Jiao Tong University, which has been used in safety justifications for the IVR strategy for licensing purposes in China by the RP.

498. The code has a similar methodology to that employed by Westinghouse for the safety justification of IVR in the AP600 and AP1000 (Ref. 94) reactor designs. The RP claims that the MOPOL calculations are used as a supplementary argument to support claims that CHF will not be reached during the worst set of conditions during IVR.

499. My TSC's review (Ref. 17) of the MOPOL code confirmed that the most important parameters are varied in order to maximise the heat flux in a steady state calculation, and that the methodology was akin to that used in the safety justification for AP600/AP1000.

500. However, my TSC considered that because the code only performs steady state calculations, it does not account for potential transient effects in the separation of metals and oxides after relocation. As stated, there is still no international consensus on the physicality of this transient period, however, it has been found that it has the potential to lead to the most challenging heat fluxes in the IVMR2020 project (Ref. 111). To account for my concerns related to the transient effects, the RP has performed calculations using the thermo-chemical equilibrium phase separation model within ASTEC which captures the transient effects (see sub-section 4.6.1).

501. As the main safety justification has been made through the ASTEC code and the finite element analysis, and as the RP has submitted additional analyses to account for the transient effects not captured by MOPOL, I have chosen not to perform an in-depth

review of the MOPOL code and I am satisfied with the application of MOPOL in the RP's safety case.

4.6.3.2 JMCT

502. The JMCT code is a particle transport code using a Monte-Carlo method developed by China Academy of Engineering Physics. It can be used in neutron transport, photon transport and neutron or photon coupling transport mode. As described in sub-section 4.5, the RP has used the JMCT code to perform re-criticality analyses of a degraded core.

503. As part of ONR's Radiological Protection assessment (Ref. 110), a TSC was employed to review the use of the JMCT code for modelling criticality in the SFP. Although some of the critical masses appeared to be overestimated in spherical configurations, the review found that the JMCT code was validated for its use in the SFP. Whilst the validation is clearly geometry and model dependent, I take confidence from this review that the relatively simple geometries used in the severe accident analysis could be modelled. I judge that the significance of the effects associated with re-criticality is small in comparison to that associated with other claims made in the Severe Accident Analysis safety case (SRS No. 56 (Ref. 6)); on this basis I have not chosen to perform any further detailed assessment of the code for the purpose of the severe accident analysis.

4.6.3.3 MC3D

504. MC3D is a code developed by IRSN, which is used to analyse impulses from steam explosions. The RP has used the MC3D code to analyse the potential impulses related to ex-vessel steam explosions to demonstrate that it understands how severe accidents progress (Ref. 91).

505. Importantly, the RP has not used the MC3D code to demonstrate that the containment can withstand the impulses from ex-vessel steam explosions as it considers that there are very large uncertainties associated with this phenomenon and that the sequences that could lead to conditions in which a steam explosion occurs should be practically eliminated through implementation of the IVR strategy. Nor has the code been used to support the Level 2 PSA.

506. The validation documentation for the code was submitted by the RP (Ref. 44) and reviewed at a high-level by my TSC (Ref. 18). Whilst my TSC considered that the code was state of the art for evaluation of steam explosions, it noted some shortfalls in its validation. However, given that the UK HPR1000's main strategy for protecting the integrity of the containment (and therefore to practically eliminate early or large releases) is through IVR, the claims made on the tolerability of the plant to ex-vessel steam explosions are extremely limited, I judged that seeking further improvements to the submitted validation evidence for this internationally recognised code would not be proportionate. On that basis, informed by my TSC's review, I am satisfied that the code and how it has been applied by the RP is adequate for GDA.

4.6.4 Experimental Facilities

507. In Ref. 92 the RP has presented details of experiments that have been used to substantiate the design of the IVR strategy and the CHF correlation. This covers three experiments related to:

- optimisation of the IVR ERVC channel in the ACPR1000+ design;
- verification of the IVR systems and measurements of the lower head CHF at multiple angles along the lower head; and

- a downward facing heated plate experiment to investigate effects of nano-coating, debris and boron presence in the ERVC coolant and heat transfer surface roughness.

508. Through the downward facing heated plated experiment, the RP claims that there is limited benefit to applying surface coating or additional roughness to the RPV external surface. I have not assessed in detail the RP's claims related to the downward facing heated plate experiment in detail. This is because I judge that the largest contribution to maximise the CHF is to optimise the ERVC channel. However, in my judgement, the RP's claims appear reasonable.

509. In my opinion, the most important of these experiments in relation to optimising the design of the UK HPR1000 IVR strategy are those that support the design requirements of the UK HPR1000 IVR systems and measurements of the CHF (REVECT-II facility). A description of REVECT-II and the CHF correlation derived from the experiments is presented in Ref. 92. Some additional information on how the CHF curve accounts for measurement errors is presented in Ref. 35.

510. The REVECT-II facility is a two-dimensional facility with a full height circulation loop and 1:1 radial scaled test section of an RPV. It allows for reproduction of an effective full-scale simulation of the reactor axisymmetric geometry. The RP claims that this detailed 1:1 slice is necessary because the exact level of CHF which may be reached depends on the geometry of the outer wall of the RPV and the dimensions of the ERVC channel (for example, a very thin ERVC channel may result in low flow and low heat removal, and a very large ERVC may result in cooling more akin to that from a pool of water rather than convective flow).

511. The REVECT-II facility appears to be similar to the ULPU (I-II-III-IV) facilities (Ref. 94) which were used to calculate the CHF for the AP600 and AP1000 reactors at the University of California, and similar methodologies were utilised to conduct the experiments. The RP states that the REVECT-II facility geometry can reproduce with high level of reliability the IVR phenomena occurring in a UK HPR1000. The test measurements have allowed the determination of a polynomial correlation between the CHF and the angular position along the mock-up of the lower head (sub-section 4.5 provides an example of the shape of this polynomial curve). The RP states that to be conservative the CHF equation was fitted using lower values of the test data in every local zone.

512. The CHF correlation obtained during the tests is similar to that one calculated in the ULPU III-IV experiments and implemented in several severe accidents codes (Ref. 20). However, in my opinion, the RP has not provided enough information related to the experimental facilities to determine whether the REVECT-II facility adequately represents the UK HPR1000 design, and whether the measurements are applicable to the UK HPR1000. There is limited information related to the facility, the measurement methodologies, the limitations, assumptions or a discussion of the results. For example, it is unclear whether potential deformation of the cooling channel is accounted for in the errors. Whilst I have confidence that the RP will be able to provide further evidence to substantiate the CHF measurements, the lack of evidence is a shortfall against my expectations for AV.3.

513. Optimisation of the ERVC channel is an important strand in demonstrating that the risks related to IVR have been reduced ALARP. However, the experimental data related to optimisation of the ERVC channel to maximise the CHF values has not been provided. The process of optimisation is not novel and is a relatively simple procedure based on empirical results. Therefore, whilst I have no reason to believe that the channel design has not been optimised, the RP's safety case provides limited evidence to demonstrate that. I therefore consider that the licensee should demonstrate that the

ERVC channel of the UK HPR1000 has been optimised during detailed design to optimise the margin to CHF, and therefore reduce associated risks ALARP.

514. Demonstration of the optimisation of the UK HPR1000 ERVC channel and applicability of the CHF curves requires detailed design of the IVR system, which is not available in GDA. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0082 – The licensee shall, as part of detailed design of the external reactor vessel cooling channel and in-vessel retention subsystem, substantiate the lower head critical heat flux curve used in the severe accident analysis, and provide evidence that the geometry of the external reactor vessel coolant channel has been optimised to maximise the value of critical heat flux.

4.6.5 Strengths

515. The GASFLOW-MPI and ASTEC codes are well established codes used internationally for severe accident analysis (Refs 20 and 21).

516. The RP has provided appropriate third-party verification and validation documentation for these codes and has also described how the codes are applicable to the UK HPR1000.

517. The RP has performed comprehensive sensitivity analyses, which demonstrate there are no cliff-edge effects associated with any parameters or model changes in ASTEC. The RP has demonstrated that assumptions made in the GASFLOW-MPI model are bounding of the largest uncertainties in the model.

518. The RP has demonstrated that the codes align well with the expectations of the SAPs AV series and NS-TAST-GD-042.

4.6.6 Outcomes

519. I have raised one minor shortfall related to uncertainties in the GASFLOW-MPI code.

520. I have raised the assessment finding AF-UKHPR1000-0082 as I consider that the RP has provided insufficient evidence to substantiate the CHF measurements, or the claim that the ERVC channel has been optimised for CHF.

4.6.7 Conclusion

521. I am satisfied that the RP has provided sufficient evidence that the codes used to support the UK HPR1000 severe accident safety case are adequately validated for their use in GDA.

522. Where large uncertainties exist, the RP has performed adequate sensitivity analyses to demonstrate that these uncertainties do not result in cliff-edge effects, and that even when incorporating these uncertainties that the IVR and hydrogen management strategies are effective.

523. Although I judge that the RP has not provided sufficient evidence that the ERVC channel has been optimised, the CHF curve appears to be reasonable, and I have confidence that this evidence can be provided. This evidence should be provided by the licensee.

4.7 Assessment of Engineering Requirements

524. In this section I present my assessment of the adequacy of the engineering requirements of the severe accident safety features and the associated supporting SSCs (such as those providing electrical supplies, cooling and C&I).

525. Refs 48 to 75 contain details of the engineering requirements for the main UK HPR1000 severe accident safety features. These reports contain information related to categorisation and classification, independence and reliability, and environmental conditions for SSCs. The following sections present my assessment of these aspects in turn.

526. For my assessment I have applied the expectations of SAPs EKP.3, ECS.1, ECS.2, EQU.1, AM.1, ECV.2 and ECV.3 (Ref. 2). In the following sections, I have explained how I have applied these where appropriate.

4.7.1 Categorisation and Classification

527. It is my expectation that the safety functions identified (see sub-section 4.3) are categorised, and that the SSCs which carry out those safety functions are classified with respect to importance to safety. In my assessment, I have applied the general expectations of SAPs ECS.1 and ECS.2 (Ref. 2).

528. The RP has categorised safety functions and classified SSCs in accordance with its safety case rules described in Chapter 4 of the PCSR (Ref. 114). The RP's approach to categorisation and classification has been assessed as part of a cross-cutting topic and is reported in ONR's Fault Studies assessment report (Ref. 10). For the purpose of this report, it can be summarised that the RP uses a three-tiered approach which is closely aligned with SSG-30 (Ref. 6) and ONR's expectations for categorisation and classification in ECS.1 and ECS.2 of the SAPs (Ref. 2) and NS-TAST-GD-094 (Ref. 4). In a slight deviation to ONR's approach, the RP has adopted the terminology FC1, FC2 and FC3 for safety function categorisation (FC1 being the most safety significant) and F-SC1, F-SC2, and F-SC3 for SSC classification (F-SC1 being the most safety significant). I now consider how the approach has been applied to SSCs which have a role to play in severe accidents.

529. The majority of the safety functions for severe accident mitigation are FC3 and the SSCs that provide those safety functions are designated as F-SC3. The failure of most severe accident safety features does not result in a high (or any) consequences during normal operations and the likelihood of the safety functions being called upon is low, therefore the categorisation and classification is usually low. This is aligned with ONR's expectations, described in NS-TAST-GD-094 (Ref. 4) and I am satisfied the majority of safety functions are FC3, and that the relevant SSCs are F-SC3.

530. IAEA SSG-53 paragraph 3.75 (Ref. 6) states that the systems necessary for the control of pressure build-up inside the containment following a design basis fault should be safety class 1 (equivalent to F-SC1) and specifically cites containment spray as such a system. It goes on to state that backup systems for design extension conditions should be assigned at least safety class 2 (equivalent to F-SC2). In response to RQ-UKHPR1000-1597 [81], the RP has provided a justification for why it is appropriate that the EHR [CHRS] is assigned safety F-SC3. The RP points out that the EHR [CHRS] only provides a diverse means of heat removal when there has been a failure to deliver FC2 safety functions for DBC fault conditions, and is only the primary means of heat removal for accidents with core melting. A safety class 3 designation in these circumstances is consistent with my expectations and subsequent statements in SSG-53 paragraph 3.75 (Ref. 6) for systems which preserve containment integrity, and

therefore I am satisfied with both the RQ response and the EHR [CHRS] safety classification.

531. An exception in the RP's classification of severe accident safety features as F-SC3 is the classification of the first set of valves on the SADVs. These gate valves deliver a FC1 safety function and therefore are assigned as F-SC1. This is because they form a barrier to the primary circuit and their failure would result in a fault sequence similar to a large break loss of coolant accident. Whilst the gate valves are F-SC1, they are controlled by the F-SC3 KDA [SA I&C] system. Based on guidance in NS-TAST-GD-094 (Ref. 4), I challenged the RP on this as I judged that the lower classification of the actuating system could undermine the high classification of the valve (i.e. a less reliable system could defeat a high reliability system). However, in response to RQ-UKHPR1000-0078 (Ref. 81), the RP has clarified that the valves are usually electrically isolated and require to be de-isolated using the Emergency Control Panel (ECP) prior to actuation from the KDA [SA I&C]. With this in mind, I am satisfied that the classification of the KDA [SA I&C] does not undermine that of the SADV. I am also satisfied that the valves of the SADVs have been appropriately classified.

532. In addition, two of the PARs in the EUH [CCGCS] are also credited during DBC fault conditions and designated as F-SC2 SSCs. In this case, the F-SC2 classification for a DBC fault is aligned with the RP's methodology for categorisation and classification (Ref. 114) because they only provide safety functions to return the plant to a safe state (rather than to the controlled state). Consistent with its design rules, the RP has applied the single failure criterion in deterministic analysis to demonstrate that one of these two PARs alone is sufficient to reduce the hydrogen concentration to safe levels during DBCs (Ref. 103). However, other than their location, these two PARs are physically no different to the F-SC3 PARs. The DEC-B analysis to demonstrate the effectiveness of the majority of the PARs to deliver their severe accident functionality has not been undertaken on the same conservative basis. However, this is consistent with my expectations and I judge that the designation of F-SC3 to the remaining PARs is sufficient. For these reasons, I am satisfied that the classification of all of the PARs in the EUH [CCGCS] to be appropriate.

533. The ECS and KDA [SA I&C] system are both F-SC3 systems, which I am satisfied is appropriate. However, during GDA the RP has upgraded the 24-hour UPS and SBO generators (which power these systems) to F-SC2. This is because they provide power not only for severe accident management, but also provide the diverse means of delivering several FC1 safety functions. The higher classification exceeds that expected for equipment required for severe accident management, but I am content with the classification.

534. The RP's approach to seismic classification is decoupled from its safety categorisation of safety functions and classification of equipment (Ref. 114). This is because although lower safety classification (e.g. F-SC3) equipment are less safety significant than higher classification equipment (e.g. F-SC1), they should still be shown to able to carry out their safety functions when required. This is important for severe accident equipment (safety features and other equipment used for severe accident management) as the initiating event which leads to a severe accident may have been caused by seismic activity. The RP has therefore assigned all severe accident safety features, including the supporting C&I and ECS, the highest seismic classification. As a seismic event is an external hazard which has the potential to lead to severe accident conditions, I consider that highest seismic classification is appropriate.

535. In summary, I am satisfied that the safety functions associated with Severe Accident Analysis have been appropriately categorised and the SSCs appropriately classified, meeting my expectations for SAPs ECS.1 and ECS.2 (Ref. 2) and NS-TAST-GD-094 (Ref. 4).

4.7.2 Independence

536. A key tenant of the defence in depth principle as set out in SAP EKP.3 (Ref. 2) and Position 2 of WENRA Safety of new NPP designs (Ref. 12) is that severe accident safety features should be as independent as far as is practicable from other SSCs providing similar safety functions for more frequent faults.

537. In order to determine whether there is adequate independence between the levels of defence in depth, I have assessed two aspects. I have assessed whether there is equipment shared over multiple levels of defence in depth and whether inadvertent actuation of Level 4 defence in depth does not affect higher levels (e.g. Level 3). In this section I summarise my assessment of these two categories.

538. Power supplies, PARs (EUH [CCGCS]) and containment are the main SSCs which are shared across multiple levels of defence in depth. I am satisfied with the RP's position for the following reasons:

- For the power supplies: the EDGs, SBO generators, UPS' and diesel generators power are identified as both design basis safety measures and equipment for severe accident mitigation. This is designed this way because failure of one power supply, say the EDGs, does not lead to irrecoverable failure of all levels of defence in depth. Providing complete independence between the power supplies would limit the flexibility of providing power when necessary. As there are severe accidents that can be initiated by things unrelated to the power supply, I consider that not crediting the other levels of defence in depth (in terms of power supply) would be disproportionate. I therefore consider it acceptable that there is not complete independence between the power supplies for the different levels of defence in depth.
- For the PARs: the most likely way that a severe accident arises is because of an initiating event that is so severe that the Level 3 defence in depth is defeated, or that an initiating event occurs and the Level 3 defence in depth fails on demand. For these cases, it is expected that an independent level of defence in depth will mitigate the consequence. In the case of the PARs, failure of the two F-SC2 PARs during any initiating event fault will not be the cause of a core melt scenario. I therefore judge that it is appropriate to credit the F-SC2 PARs for both Level 3 defence in depth and Level 4 defence in depth.
- For the containment: the same reasoning for the PARs applies to the containment. Failure or success of the containment does not affect whether an initiating event progresses into a core melt scenario. I am therefore content that it is credited for both Level 3 and Level 4 defence in depth.

539. The SADVs are connected directly to the pressuriser with a dedicated line independent to the upstream discharge lines of the PSVs, are actuated using the KDA [SA I&C], and are powered by the 24-hour UPS. I am satisfied that they provide adequate independence to the PSVs in order to depressurise the primary circuit in a severe accident. As stated previously, however, the SADVs present a challenge to independence of defence in depth as inadvertent operation could result in a depressurisation of the primary circuit and similar consequences to a LB-LOCA. To account for this, the RP has made the gate valves F-SC1 and set the administrative requirement that the valves are electrically isolated. I am therefore satisfied that these measures ensure adequate independence of the SADVs from the other levels of defence in depth (Ref. 86).

540. In terms of IVR, the inadvertent actuation of the IVR system with the reactor at power has the potential to result in thermal shock and failure of the RPV. In response to RO-UKHPR1000-0032 (Ref. 100), the RP has demonstrated that that RPV would be tolerant of such faults and that the initiating event frequencies are very low due to

electrical isolation of the EHR [CHRS] valves. With this in mind, I consider that there is adequate independence between the IVR system and the other levels of defence in depth.

541. ONR's assessment of the IVR strategy and the associated C&I has led to a design modification to remove the 650 °C COT C&I interlock from the IVR strategy. This required signal processing from the Safety Automation System (SAS) which provides protection against design basis accidents (at Level 3 defence in depth). Prior to this design change, I considered that this arrangement presented a shortfall against my expectations for independence of levels of defence in depth. I judged that a failure of the SAS C&I platform would have the potential to result in a severe accident scenario and that this should not be credited for short term severe accident management. Moreover, I judged that it did not appear appropriate to rely on the survivability of the COT signals for the success of IVR. The RP performed optioneering and implemented design modification M63 (Ref. 93) and M89 (Ref. 115). These design modifications remove the C&I interlock and replace it with an administrative interlock. The design now also incorporates a key switch to prevent a single operator from operating the IVR system. When the COT signal is received via a hardwired connection, the operator seeks permission from the shift supervision who holds the key. In cooperation with the Human Factors assessor (Ref. 116) I am satisfied that the design modification is equally as robust in preventing inadvertent operation and has reduced the risks associated with failure of the 650 °C COT interlock to ALARP.

542. In addition, the RP has also identified a shortfall in independence between the KDA [SA I&C] and C&I systems for other levels of defence in depth. The RP has therefore implemented design modification M89, which removes the communication between the KDA [SA I&C] and other C&I platforms providing protection at other levels of defence in depth. ONR's C&I inspector has assessed the high-level design modification and is content that the modification improves independence (Ref. 117), however, ONR's C&I inspector has raised AF-UKHPR1000-0024, 0034 and 0035 which relate to a demonstration of derivation of the C&I requirements and a demonstration that the risks have been reduced ALARP.

543. To summarise my assessment related to independence, I am satisfied the RP has sufficiently demonstrated that the UK HPR1000 incorporates adequate independence between the levels of defence in depth and meets the expectations of SAP EKP.3 Ref. 2) and Position 2 of WENRA safety of new NNP designs (Ref. 12).

4.7.3 Redundancy

544. ONR's expectation is that sufficient redundancy is provided in safety systems such that they achieve the intended reliability (Ref. 2). Unlike design basis safety measures, which normally incorporate the single failure criterion and take account of maintenance requirements, there is no explicit guidance on how sufficient redundancy is to be achieved for severe accidents safety features. For redundancy with severe accident safety features, I have therefore judged the systems on a case by case basis to determine whether the risks have been reduced ALARP.

545. Since I consider redundancy in the Severe Accident Analysis topic area is related to the requirement to demonstrate risks have been reduced ALARP, I have provided a summary of my assessment related to redundancy against the ALARP principle in sub-section 4.10.

4.7.4 Environmental Conditions for Equipment

546. It is my expectation that the severe accident analysis is used to identify equipment required for severe accident management, and that the equipment is qualified for the

environmental conditions experienced during severe accidents. This equipment includes the severe accident safety features, but may also include equipment shared over multiple levels of defence in depth and which is not specifically identified in the DEC-B analysis for GDA (for example, the containment radiation monitoring system). My general expectations for equipment qualification for severe accidents are informed by SAPs EQU.1 and AM.1 (Ref. 2).

547. In addition, it is my expectation that the severe accident analysis is used to inform the requirements of the containment in accordance with SAPs EVC.2 and EVC.3 (Ref 2). The RP has chosen to use the same analysis of environmental conditions to inform its requirements for the containment. In this section, I summarise my assessment against both aspects.

548. The assessment of the overall methodology for equipment qualification is reported in ONR's Mechanical Engineering assessment report (Ref. 118). However, my assessment has focused on how the environmental conditions that occur during a severe accident have been calculated, and how equipment requiring qualification has been identified.

549. The RP has derived the environmental conditions for severe accidents using the ASTEC code (Ref. 119). The environmental conditions include the pressure, temperature and radiation field. Ref. 119 explains that the environmental conditions have been derived by the augmentation of conditions from the SBO, ATWS, LB-LOCA and SB-LOCA. Ref. 119 provides the plots for the containment pressures and dew point temperatures derived from these accidents. I am satisfied that Ref. 119 provides a reasonable basis for the RP's assumed bounding envelope for the conditions which could occur following a range of severe accidents (with the exception of the localised effects from the impingement of hot gases which require separate arguments – see sub-section 4.5 on hydrogen management).

550. In response to RQ-UKHPR1000-0876 (Ref. 81), the RP provided a preliminary list of equipment that would experience harsh conditions during a severe accident and also a list of equipment that is credited in severe accidents but does not experience harsh conditions. The RP has explained (Ref. 120) that the equipment was largely chosen based on whether the SSCs were expected to be in contact with primary coolant during its expected operation during a severe accident. For instance, the RP has included equipment in the containment and the annulus (because of containment leakage) but has not included components on the steam side or in safeguard buildings. I challenged the RP on this as I considered that equipment in the secondary side or safeguard buildings could be exposed to primary coolant due to a break, or exposed to radiation. However, the RP has highlighted that the full scope of the equipment qualification for these areas has not been performed during GDA and will need to be performed by the licensee. This position has been assessed in the Mechanical Engineering (Ref. 118) assessment. The full equipment list will depend on the SAMGs, which will be developed by a future licensee and are out of scope of GDA. For the purposes of Severe Accident Analysis in GDA, I therefore consider this position to be reasonable.

551. An important parameter which indicates the UK HPR1000 has entered a severe accident plant condition is the COT reaching 650 °C. This prompts the operators to start following the procedures set out in the SAMGs and represents an important assumption in the DEC-B analysis. It is therefore necessary for the equipment which measures this value to still be functioning when called upon. Survivability cannot be demonstrated during GDA as the technology has not been identified and should be demonstrated by a licensee as part of normal business. However it should be noted that by removing the COT interlock from the KDA [SA I&C]/SAS design the survivability becomes less crucial for the implementation of IVR as severe accidents can be diagnosed using multiple signals (e.g. containment radiation).

552. ONR's Mechanical Engineering inspector has sampled the equipment qualification requirements of the SADVs (Ref. 118). The RP has presented a qualification schedule, which links the environmental conditions derived (Ref. 119) to the design specification of the equipment. The Mechanical Engineering inspector is satisfied with the link between the safety analysis and the equipment specification (Ref. 118).

553. The DEC-B analysis has been used as an input to containment performance analysis. This analysis is in the scope of the PSA (Ref. 9) and Civil Engineering (Ref. 8) topic areas. However, since the environmental conditions used as an input to the containment analysis are the same as those used for the equipment qualification, I have assessed whether the analysis is appropriate for use for the containment analysis. The analysis uses a combination of the worst conditions analysed in the DEC-B analysis (Ref. 119). I consider that this is an appropriate basis for use in the containment analysis, and that my expectations for ECV.2 and ECV.3 have been met, from a severe accident point of view.

554. In my opinion, the RP has demonstrated that the environmental conditions for equipment qualification have been considered. Furthermore, based on ONR's Mechanical Engineering assessment (Ref. 118) I am satisfied that the RP has provided an auditable link to the design specification of the equipment. I am therefore satisfied that the RP has met my expectations for equipment qualification in EQU.1 and robustness of equipment for accident management in SAP AM.1 (paragraph 780) (Ref. 2).

4.7.5 Strengths

555. The RP has categorised safety functions and classified SSCs. The assignments related to severe accidents are well aligned with the expectations of ECS.1 and ECS.2, and NS-TAST-GD-094.

556. In general, there is adequate independence between levels of defence in depth, and the UK HPR1000 aligns with WENRA Position 2 Safety of new NPP designs and SAP EKP.3. Where the RP has identified deficiencies, the RP has implemented design modifications.

557. Although not required by its safety case rules, the RP has implemented redundancy where it deems appropriate. I consider this approach to be adequate for severe accident safety features.

558. The link between the severe accident analysis and the equipment qualification and containment design basis curves is clear and meets my expectations for SAPs EQU.1, ECV.2, ECV.3 and AM.1 (Ref. 2).

4.7.6 Outcomes

559. No assessment findings or minor shortfalls have been identified.

4.7.7 Conclusion

560. Based on my assessment of the engineering requirements I have found that in general, the RP has demonstrated an adequate link between the severe accident analysis and the engineering requirements.

4.8 Other Aspects of Severe Accident Management

561. In my opinion, the most important aspect of severe accident management for GDA is the design of the safety features which mitigate potential severe accidents scenarios. The substantiation for the design of the safety features is mainly provided by the RP's

DEC-B deterministic analysis, which I have already covered in sub-section 4.5. However, there are other aspects related to severe accident management which are within the scope of the Severe Accident topic area which should be covered during GDA.

562. In this section, I summarise my assessment of these other main aspects. These aspects are:

- The supporting systems to the safety features – here, I refer specifically to the permanent equipment used to support the severe accident safety features, such as the C&I, electrical supplies and the cooling chain.
- Basis for SAMGs – Although SAMGs are site specific, and should be developed by a licensee as part normal business, the severe accident analysis forms the basis for the future SAMGs.
- Human Actions and Post-Accident Accessibility – During a severe accident, operators may receive elevated doses whilst performing necessary actions for severe accident management. The most important actions are those which are required to enable the correct performance of the safety features, and therefore can be identified during GDA.
- Mobile equipment – although the safety features IVR, EHR [CHRS], EUH [CCGCS] and SADVs are not reliant on mobile equipment to bring the severe accident to a stable state, mobile equipment may in reality be used to prevent escalation to a severe accident and to support the safety features during a severe accident in the long term if off-site power cannot be restored.

563. In my assessment I have applied the expectations of the SAPs AM.1, ESS.3, EES.1, EES.9, FA.16, EHF.3 and SSG-2. I explain how I have applied these expectations in the following subsections.

4.8.1 Supporting systems - C&I, Electrical and Cooling Chain

564. In this section I present my assessment of the adequacy of the supporting systems that support severe accident safety features.

4.8.1.1 Instrumentation and Control

565. The main C&I systems of the UK HPR1000 are (Ref. 121):

- RPS [PS] – the F-SC1 system which brings the plant to a controlled state during DBC-2, DBC-3 and DBC-4 faults.
- SAS – the F-SC2 safety automated system, which brings the plant to a safe state in DBC-2, DBC-3 and DBC-4 faults. The SAS also provides monitoring data and performs some safety functions during DEC-A and severe accidents.
- Plant Standard Automation System (PSAS) – this performs FC3 and non-safety classified functions. The PSAS controls and monitors the plant in normal (DBC-1) and abnormal operations before a fault.
- Diverse actuation system (KDS [DAS]) – provides FC2 safety functions when the RPS [PS] and SAS have failed during design basis faults.
- KDA [SA I&C] – the KDA [SA I&C] performs FC3 control and monitoring functions in severe accidents.
- The Plant Computer Information and Control System (KIC [PCICS]) – the KIC [PCICS] performs FC3 and non-safety categorised monitoring and control functions.

566. The KDA [SA I&C] provides the instrumentation and control for short term severe accident management. The KDA [SA I&C] is a mainly hardwired F-SC3 system which has two divisions, A and B. Each division is situated in safeguard buildings A and B.

The KDA [SA I&C] can be powered by the EDGs, SBO generators, 24-hour batteries (UPS) and mobile diesel generators.

567. Along with ONR's Control & Instrumentation inspector, I have assessed the safety functions assigned to the KDA [SA I&C]. The scope of my assessment is only on a safety function level; a more detailed assessment of the architecture and system requirements of the KDA [SA I&C] is reported in ONR's C&I assessment report (Ref. 117).

568. Ref. 29 states that the KDA [SA I&C] controls the SADVs, IVR valves, EHR [CHRS] pumps and the EDE [AVS]. Importantly, however, Ref. 29 states that the KDA [SA I&C] does not control the EHR [CHRS] spray valves or the ECS SSCs. Ref. 29 assigns these functions, and associated monitoring functions to the F-SC2 SAS which is used mainly for Level 3 defence in depth measures. The RP explains that because the EHR [CHRS] and ECS systems require an Alternating Current (AC) power source, there is no advantage to assigning associated functions to the KDA [SA I&C], as AC power would need to be restored and the SAS would be available. The RP's reasoning for assigning the controls of the EHR [CHRS] to the SAS appears similar to that for other reactors. Initially, this appears to be a shortfall against independence as failure of the SAS is potentially the reason why there is a severe accident scenario. However, whilst not stated explicitly, it is usual that the associated pumps and the valves are capable of manual local actuation should the SAS not be restored. In my opinion, the RP's safety case for assigning the control of the EHR [CHRS] and the associated supporting functions to the SAS is not clear without wider knowledge of the safety case. I am confident, however, that this is just an omission in the safety case explanation and have only identified this as a minor shortfall.

569. In addition, the actuation of the EUF [CFES] is not controlled by the KDA [SA I&C]. This instead is performed locally. I consider that this is acceptable since the grace time is long, and the RP has provided substantiation for the "post-accident accessibility" of the relevant rooms (the RP refers to access required to mitigate accidents as post-accident accessibility). In general, ONR's Radiation Protection inspector considers that methodology for calculating the doses associated with these actions is reasonable (Ref. 110).

570. Other than actions related to the EUF [CFES] and EHR [CHRS], I am satisfied that the appropriate safety functions required for severe accident mitigation (i.e. those related to controlling the safety features and containment) have been assigned to the KDA [SA I&C].

571. The RP lists twenty monitoring functions perform by the KDA [SA I&C] (Ref. 29). These relate to:

- determining whether the severe accident safety features are working correctly;
- providing situational awareness and inform the operator on when to take action in both the reactor and the SFP;
- measuring parameters outside of the inner containment to confirm that the radiation levels that potentially leak from the containment are low; and
- confirming that the filtration system which further reduces leakages (EDE [AVS]) is working adequately.

572. I am satisfied that the parameters chosen should enable the operator to understand whether IVR, SADVs, and EUH [CCGCS], EHR [CHRS] and EUF [CFES] have been actuated and whether these are effective (Ref. 29). For example, the RCP [RCS] pressure and containment pressure can be measured using the KDA [SA I&C]. Rather than simply relying on C&I of the SADVs to provide the state of the valves, this information can be used to determine whether the valves have actually opened.

573. Regarding releases of radioactivity through venting of the containment (where the EHR [CHRS] has failed), the RP has identified several functions to determine the levels of radiation in the containment and the containment pressure (Ref. 29). This information can be used to determine whether venting is required and if so to balance the risks and benefits. Related to the filtering of any releases, the RP has also identified parameters which can inform whether the filters are working successfully. I am satisfied that this allows for decision making for closing or replenishing filtration systems.

574. The SFP includes C&I functions that support the prevention of accidents in the SFP to escalate to a severe accident, but also to determine if severe accident conditions have been reached. These accidents are either due to a loss of cooling or loss of inventory. In either case, fuel melt only occurs when the fuel is uncovered. The monitored parameters include water level, the SFP building pressure and SFP water temperature. The SFP water level gauge is measured by several different range detectors. The instrumentation measures the water level from just below the top of the spent fuel storage rack [redacted] to above the normal water level of the SFP [redacted]. For accidents that occur in the SFP, the operator may potentially need to open a vent in the SFP building in order to prevent an overpressure of the SFP building. This decision to open the SFP building vent is linked to the SFP temperature, as boiling results in a relatively fast increase in building pressure.

575. In my opinion, an extended range below the top of the fuel rack may be beneficial for situational awareness during a severe accident. In response to RQ-UKHPR1000-0622 (Ref. 81), the RP has explored options for increasing the range of the water level to below the top of the storage rack. However, the RP concluded that there are no reasonably practicable options available and it would not change the course of action in severe accident management, which is to add as much water to the pool as possible to regain control of the water level. Moreover, the RP has argued that accidents leading to fuel uncovery in the SFP are practically eliminated. My assessment of whether accidents in the SFP have been practically eliminated is summarised in sub-section 4.9. This includes arguments related to the withstand of the SFP wall to catastrophic failure, and that sequences that lead to fuel uncovery in the SFP are practically eliminated. It is important to note that the UK HPR1000 includes a large tank of water, which can feed the SFP for several days via gravity if cooling is lost or if there is a loss of inventory fault. This is an advantage that the UK HPR1000 has over some other comparable reactor designs. Given the above, although an extended water level measurement may be beneficial for situational awareness during severe accidents, I am satisfied with the RP's reasoning that the severe accident management would be unaltered and that the RP has adequately demonstrated that it would be grossly disproportionate to extend the level measurement.

576. I am satisfied that the RP has identified the appropriate parameters to monitor the SFP and SFP building, which can be used to prevent severe accidents in the spent fuel pool, and to manage challenges to the SFP building if an accident were to occur.

577. To summarise, I am satisfied that the RP has appropriately identified parameters that should be monitored during a severe accident to confirm the success of safety functions and to monitor the progression of accidents, which meets my expectations for paragraph 778 of SAP AM.1 and SAP ESS.3 (Ref. 2). In addition, the KDA [SA I&C] monitoring parameters are available to the operator within the MCR to enable severe accident management; this meets my expectations for SAP ESR.1 (Ref. 2).

4.8.1.2 Electrical Supplies

578. EES.1 sets the expectation that essential services should be provided to ensure the maintenance of a safe plant in accident conditions. In addition, EES.9 (SAPs paragraph 442) sets the expectation that severe accident analysis should be used to

show that the site's emergency arrangements would be sufficient to manage a severe accident event. For the UK HPR1000 GDA, I interpret this as demonstrating that there is sufficient electrical power supplies to power the severe accident safety features, and that back-up power supplies exist and can be implemented in time.

579. Together with ONR's Electrical Engineering inspector, I have assessed the adequacy of the allocation of the loads to the various power supplies, and the capacity of these power supplies (i.e. length of time in which they can operate).

580. There are two types of power supply required for severe accident mitigation in the UK HPR1000: AC power and Direct Current (DC) power. AC power sources are used to charge batteries and to power large equipment (e.g. pumps). The following are of importance for severe accident mitigation:

- EDGs – three EDGs can power the design basis and severe accident loads. Sufficient stocks of fuel and consumables are available for at least one week.
- SBO generators – two SBO generators can provide power when the EDGs are unavailable for both design basis and severe accident loads for several days.
- Mobile diesel generators – two mobile generators can provide power for design basis protection and for severe accident mitigation.
- 24-hour UPS – this can power relevant C&I and some mechanical equipment (e.g. valves) during severe accidents.

581. A summary of my assessment of the claims on mobile equipment are presented in section 4.8.4.

582. Below I have summarised the power supplies for each safety feature and supporting system (Ref 48 to 75):

- KDA [SA I&C] – the KDA [SA I&C] is powered by the 24-hour UPS.
- ECS – the pumps of the ECS require an AC power source (EDGs, SBO generator or mobile generator).
- IVR – for the passive filling phases, this only requires valves to be opened, and can be powered by the 24-hour UPS. For the active phase, the pumps require an AC power source (EDGs, SBO generators, mobile generators).
- EUH [CCGCS] – the PARs are not powered. The hydrogen monitors require power from the 24-hour UPS.
- EHR [CHRS] – as stated previously, this requires the SAS for initiation. Both these functions of the SAS and the spray (and IVR pumps mentioned above) require an AC power source (EDGs, SBO generators, mobile generators).
- SADVs – these valves are powered by the 24-hour UPS.
- EUF [CFES] – this requires local manual actuation, but has some monitoring functions associated with it, which are powered by the 24-hour UPS.

583. The 24-hour UPS battery is powered by the AC power sources whilst the loads are online and so all loads that are supplied by the 24-hour UPS can also be supplied by all AC power sources.

584. In a severe accident, if the EDGs and SBO generators are lost, the RP has identified that mobile generators are required after a certain length of time to provide power to SSCs required in the longer term (e.g. pumps). The RP's own safety requirements (Ref. 107) state that "no site based mobile light equipment shall be required in less than 12 hours from accident initiation, for containment performance assurance in DEC". This requirement is also derived from the EURs (Ref. 106) related to "autonomy objectives in respect of non-permanent equipment". This implies that the plant should be capable of performing safety functions in an SBO (in which the EDGs and SBO generators are lost) for at least 12 hours before AC power is required. For SBO events,

where the EDGs, SBO generators and ASP [SPHRS] are assumed to have failed, the analysis demonstrates that approximately 13 hours are available before AC power is required to be restored, through the repair of the permanent AC power sources or connection of the mobile diesel generators. The RP therefore demonstrates that this requirement is met. Moreover, the RP has demonstrated that even in the LB-LOCA (in which the EDGs and SBO generators are likely to be available) that 11 hours is available before AC power is required.

585. Regarding the capacity of the 24-hour batteries, the reference design of the UK HPR1000 (FCG3) only included batteries with a capacity of 12 hours. During a review of the UK HPR1000 against RGP, the RP recognised that it was good practice to extend the battery capacity to reflect learning from the Fukushima Daiichi accident, and that other UK plants had a larger capacity. An ALARP assessment was performed by the RP (Ref. 122), which made the recommendation to upgrade the UPS duration to 24-hours. For reactors which are reliant on passive means of heat removal during severe accidents (e.g. the AP1000) it is normal that the battery lasts as long as the passive heat removal can be ensured (usually around 72 hours). This is because there is no reliance on active systems, such as pumps. However, I judge that the upgrade of the UK HPR1000 brings the battery duration in line with that of other comparable new reactors which are reliant on active heat removal (e.g. the UK EPR). Given this, and taking assurance from ONR's Electrical Engineering assessment (Ref. 123), I therefore am satisfied that the design modification is an appropriate ALARP measure.

586. Regarding independence of the levels of defence in depth, ONR's External Hazards inspector has provided me with assurance that the 24-hour UPS is located above the design basis flooding level (Ref. 124), and that an external hazard leading to flooding of the site should not impede the functionality of the 24-hour UPS.

587. I judge that it is reasonable to assign the loads of the equipment requiring AC power to the AC power sources, with backup permanent equipment. In addition, I judge that for GDA it is reasonable to assume that mobile generators will be available after 12 hours. I also judge that the assignment of the majority of the loads from control and monitoring to the 24-hour UPS is appropriate. In cooperation with ONR's Electrical Engineering inspector, I am satisfied that the RP has identified the relevant loads for severe accident management, and has assigned them to appropriate power supplies.

588. Moreover, I am satisfied that the design of the electrical supplies should enable severe accident management for a length of time comparable to other new reactors, allowing time for recovery of longer-term AC power. From a severe accidents point of view, this meets my expectations for EES.1 and EES.9.

4.8.1.3 Cooling Chain

589. The heat loads generated by the plant (e.g. pumps) and decay heat generated by the core and SFP, are normally removed via a secondary cooling chain. This is normally performed by a combination of the steam generators and heat exchangers cooled by the Component Cooling Water System (RRI [CCWS]). After an initial removal of heat by the SGs, all of the heat is removed by the RRI [CCWS] which is cooled by seawater. However, there are scenarios which can lead to a severe accident by a loss of this cooling chain. The UK HPR1000, therefore, includes a diverse cooling chain to the CCWS/seawater, called the ECS, which removes heat using a separate system of pipes to the CCWS and cools its water using a cooling tower rather than sea water. The water sprayed by the EHR [CHRS] is collected in the IRWST and pumped through a heat exchanger which is cooled by the ECS.

590. The ECS can be powered by the EDG, SBO generators and mobile generators. The ECS make-up tank has a capacity to provide water for up to 24 hours, and following that it can be made up via multiple water sources.

591. I have not targeted the ECS during my assessment. However, I note that the capacity is consistent with other mission times, such as the capacity of the SBO diesel generators, and is not the limiting factor. Whilst I have not targeted the ECS, I am satisfied that the capacity will enable adequate severe accident management consistent with the mission times of other support systems and I am also content from my other samples that the performance requirements are consistent with the deterministic analysis.

4.8.2 Basis for SAMGs

592. In Refs 125 and 126, the RP sets out the high-level principles for developing SAMGs. Development of SAMGs will be the responsibility of a future licensee. Although I have not assessed these principles in detail, the high-level principles within Ref. 125 and 126 cover all operating modes and appear to align with the high-level expectations in IAEA SSG-54 (Ref. 6).

593. In accordance with FA.16 of the SAPs, it is my expectation that the severe accident analysis be used to inform the SAMGs. I raised RQ-UKHPR1000-1261 (Ref. 81) because I considered that it was unclear how the analysis presented in GDA enables the development of SAMGs. The RP has stated that currently submitted documents provide only background information to identify plant specific vulnerabilities, the nature and importance of potential challenges to the boundaries, timings, parameters which can be used as symptoms, potential strategies to manage the accident and in general to understand the plant specific response to accident situations. The RP has stated that the licensee should analyse more scenarios, different assumptions and various delay times; strategies can then be calculated to support development of SAMGs.

594. In my opinion, the RP's strategy for GDA is appropriate, and provides a basis for the main actions to be taken during severe accident mitigation (e.g. initiating IVR, opening SADVs), and demonstrates that the actions are effective. However, it means that the analysis provided during GDA is limited. For example, as stated in Ref. 126, the RP claims that the SAMGs should highlight actions to prevent further degradation of the core. However, once the SADVs have opened they cannot be closed and opening can actually exacerbate core degradation in certain circumstances. For instance, during an SBO, it may be beneficial to delay RCP [RCS] depressurisation if it is believed that power can be restored and core melt can be avoided. I judge that since the RP's analysis is focussed on the bounding case for IVR, it does not provide insights to later depressurisation or core reflooding.

595. There are also other examples where the bounding approach means that more supporting analysis may need to be performed for development of SAMGs (e.g. to determine opening / closing criteria for the EUF [CFES]).

596. Since the SAMGs are a matter for development by the licensee, I do not consider these observations to meet the criteria for GDA assessment findings or minor shortfalls. I anticipate that the licensee's SAMGs will be subject to appropriate ONR regulatory attention as part of future routine permissioning activities.

597. In summary, I consider that the analysis provided by the RP can be used to provide some insights for SAMGs. However, a future licensee will need to develop SAMGs, which may require further development and refinement of the supporting analyses. Notwithstanding this limitation, I am satisfied that for GDA the RP's analysis forms a

basis for accident management and is aligned, so far as possible at this stage, with the expectations of FA.16.

4.8.3 Human Actions and Post-Accident Accessibility

598. The human based safety claims (Ref. 127) associated with severe accidents management of the DEC-B accidents analysed have been assessed by the ONR's Human Factors inspector. This is limited to the actions required for demonstrating the effectiveness of the DEC-B safety features. To support this assessment, I have reviewed these claims and I judge that the appropriate human actions have been captured.

599. Of these claims, in cooperation with the Human Factors and PSA inspectors, I targeted human actions related to the initiation of IVR. The reference design (FCG3) included the requirement for local electrical de-isolation of IVR valves to prevent spurious initiation of the IVR valves. Due to the speed of the LB-LOCA progression, and the distance between the electrical isolation cabinets (in safeguards buildings A and B), the RP's Human Reliability Assessment (HRA) found that there was insufficient time to perform the actions. The RP has since implemented design modification M63, which moves the actions for de-isolation to the MCR. In cooperation with the PSA (Ref. 9) and Human Factors (Ref. 116) assessments, I judge that this is sufficient for GDA. However, I anticipate that this will require further justification when the details of the human machine interface are known. I consider that this is normal business as the design develops.

600. In general, ONR's PSA and Human Factors assessments (Refs 9 and 116) have found that the RP's methodology for performing HRA in the severe accidents area to be fit for purpose for GDA. Together with Human Factors and PSA inspectors, I judge that all human actions required in the DEC-B analysis are identified and achievable in the given time. As the appropriate actions have been identified this meets my expectations for SAP EHF.3 (Ref. 2).

601. The RP has provided a summary of whether the actions required for design basis faults and severe accidents are achievable given the environmental conditions that may be present at the time. The RP terms this "post-accident accessibility" assessment (Ref. 109). This is intended to cover all actions required after the initiating event.

602. Together with ONR's Radiological Protection and PSA inspector, I have assessed whether the RP's post-accident accessibility assessment (Ref. 109) has identified the relevant local actions for severe accidents management which are credited in the RP's DEC-B analysis. As most actions are performed from the MCR, the list of these actions is small. These actions are listed in Ref. 109 as: activating KRT [PRMS] prior to opening the EUF [CFES], opening and closing the EUF [CFES] and the de-isolation of the active part of the IVR system (i.e. after 10 hrs). However, as noted in paragraph 599 these no longer include the de-isolation of the passive part of the IVR system which will be carried out from the MCR. The doses predicted are for the actions associated with opening the EUF [CFES] (including activating the KRT [PRMS]) resulting in approximately 200 mSv to the field operator carrying out each action. The doses for each action exceed the annual legal limits for employees working with ionising radiation (see Numerical Target 1 of ONR's SAPs (Ref. 2)). However, ONR's PSA and Radiological Protection inspectors have provided me with confidence that the doses are conservatively calculated (both the source term and the length of time needed to complete the actions (Ref. 110)).

603. Importantly, the actions identified are only necessary for opening the EUF [CFES] in the unlikely event that the EHR [CHRS] fails. The sequence frequency is predicted by the RP to be approximately 8×10^{-9} pa (Ref. 102). The usage of the EUF [CFES] is

only included in the design as a last resort to prevent catastrophic failure of the containment. Whilst, as noted above, that the doses associated with each action exceed the annual legal limit for employees working with ionising radiation, I note that Regulation 19 of REPPIR19 (Ref. 101) does allow for the disapplication of dose limits for emergency workers in order to mitigate the consequences of a radiation emergency. ONR's Radiological Protection inspector has judged that the associated doses are below the reference levels that apply for emergency workers to prevent the development of catastrophic conditions quoted in REPPIR19 and its Approved Code of Practice (Ref. 101) and are acceptable for GDA. However, ONR's Radiological Protection inspector has judged that the RP has not demonstrated that internal exposures to radiation from local interventions during severe accidents have been reduced to ALARP, and has therefore raised AF-UKHPR1000-0105, such that a licensee provides this demonstration (Ref. 110). Notwithstanding this Assessment Finding, I am satisfied that the ability to open the EUF [CFES] is a credible action during a very unlikely event for which in GDA both the radiological benefits and consequences have been identified to inform future severe accident management guidance and plans.

604. Regarding the habitability of the MCR, in response to RQ-UKHPR1000-1713 (Ref. 81) the RP explains that it has calculated the doses for an MCR worker for two release categories calculated in the Level 2 PSA (Ref. 102):

- Release Category RC101 – LB-LOCA with successful IVR, SADVs, EUH [CCGCS], and EHR [CHRS]
- Release Category RC501 – LB-LOCA with successful IVR, SADVs, EUH [CCGCS], but with failure of EHR [CHRS] sprays and heat removal and success of EUF [CFES].

605. The RP claims that the LB-LOCA accidents result in the largest source terms due to the over-pressurisation of the containment and therefore largest leakage rate. This claim has been subject to scrutiny by the PSA inspector as the LB-LOCA has been used to bound many faults (Ref. 9). However, for the purposes of calculating the dose uptake in the MCR, I consider that the arguments made appear sensible.

606. The RP has also provided dose calculations which have been performed using the same methodologies as used for its design basis analysis. The Radiation Protection inspector has found that this shows that the calculated doses accumulated over 30 days is 37 mSv (Ref. 110), which is well below the BSO of ONR's Numerical Targets 5 and 6. The RP claims that the high efficiency particulate absorbing filters installed in the MCR Heating Ventilation and Air Conditioning (HVAC) system, the thick containment walls, radiation monitors on the HVAC intake and radiation monitoring of the staff provide protection against radiological consequences in the MCR and all contribute to reducing risks of exposure to an operator in the MCR to ALARP. Based on ONR's Radiation Protection (Ref. 110) and PSA assessments (Ref. 9) I am satisfied that the methodologies for the calculation of the dose are adequately conservative, and I am satisfied that the RP has adequately demonstrated that the MCR will remain habitable for the time required to perform relevant severe accident human actions (e.g. opening the IVR valves, opening the SADVs, starting EHR [CHRS], and monitoring severe accident conditions), meeting my expectations for SAP ESS.3 (Ref. 2) and paragraph 7.60 of IAEA SSG-2 (Ref. 6).

4.8.4 Mobile Equipment

607. It is my expectation for GDA, that the requirements for on-site mobile equipment during severe accidents are adequately identified, including the requirements related to the connection points for the reactor and SFP. In this section, I summarise my assessment of the availability of mobile equipment for either prevention of escalation to a severe

accident or to support mitigation of a severe accident. Whilst many decisions associated with the storage, movement and deployment of mobile equipment will be site specific, and therefore cannot be determined during GDA, some design choices related to mobile equipment are within the scope of GDA. Together with the External Hazards inspector, I have assessed the RP's claims related to mobile equipment.

608. The majority of the DEC-B analysis is not reliant on mobile equipment, and only credits permanent equipment. There are two main reasons for this: the initiating event may be independent of availability of power sources (e.g. LB-LOCA) and there is a large grace time provided by the passive IVR tank in order to restore power if necessary. The RP claims that for severe accidents on-site mobile equipment is not necessary for at least 12 hours following an initiating event (Ref. 107).

609. For power supplies, the DEC-B analysis simply assumes power is restored when AC power is required (>13 hours for the SBO) regardless of whether it is from permanent equipment or mobile equipment. In the low frequency case in which the severe accident feature EHR [CHRS] fails, the RP assumes that a mobile water source is available for injection from an external connection, powered by a mobile diesel generator at 10 hours after initiation of the passive injection. This means that there appears to be a discrepancy between deterministic analysis (Ref. 39) and the RP's own general safety requirements (Ref. 107). Nevertheless, it is only a shortfall in my expectations for consistency in a safety case, and therefore I consider it a minor shortfall.

610. Mobile equipment can also be used to prevent escalation to a severe accident in the unlikely scenario that permanent equipment is lost. For example, in the scenario in which a loss of offsite power occurs and the EDGs and the SBO generators fail to start, mobile diesel generators can support heat removal from the reactor using the ASP [SPHRS] or ECS for several days, and mobile pumps can be used to top up the SFP as necessary. The analysis which supports substantiation of these claims has been covered by the Fault Studies assessment (Ref. 10).

611. A description of the mobile equipment, design substantiation and connection points available for severe accident management are described in Refs 128 to 130. The main mobile equipment for pumping water includes a vehicle mounted pump, portable pumps and submersible pumps available in different areas. The UK HPR1000 also includes two mobile diesel generators of different ratings.

612. The RP has identified connection points for both water sources (Ref. 129) and power sources (Ref. 130). The RP has provided high level arguments related to the safe storage of equipment, ease of transport to connection points and ease of access to the connection points. Importantly, the RP claims that the UK HPR1000 is resilient to severe external hazards, and therefore an external hazard will not lead to a core melt scenario. This means that the RP claims that a scenario in which a severe external hazard and a core melt scenario occur simultaneously are of extremely low frequency, such that the need for mobile equipment during severe external hazards does not arise as the permanent equipment will be available to cope with the core melt scenario. Based on this the RP claims that the requirement for connecting mobile equipment in 12 hours is achievable, as the site will be free from external hazards. However, ONR's External Hazards inspector considers that the RP has not provided sufficient justification that the plant is resilient to some beyond design basis flooding events, albeit very unlikely ones, which would defeat both the EDG and SBO generator sets, and simultaneously cause mass disruption on the site. With this in mind, ONR's External Hazards inspector considers that further justification should be provided for the claim that mobile generators can be connected within the 12 hours. As the details are site specific matters, the External Hazards inspector has therefore raised AF-UKHPR1000-087 to capture this concern.

613. Ref. 129 also provides details of the various configurations for supplying water under different conditions. For example, the number of pumps and connection points required for injection to the primary circuit is described. The RP provides reasoning for the required water sources and the equipment that would be needed to supply the water. The requirements are based on multiple plant states and are broken down into requirements as time progresses. I have not assessed the requirements in detail, but the arguments presented appear to be aligned with my understanding of the requirements from the deterministic analysis, and appear reasonable.

614. Ref. 130 provides details related to mobile diesel generators. Two mobile diesel generators are described, one with a 690 V rating and one with a 380 V rating. Whilst the information is limited, the RP states that mobile generators provide power to the 24-hour batteries (which in turn powers the KDA [SA I&C] and various valves and monitoring equipment), EHR [CHRS] (including IVR) and ECS. The loads account for all those required in the DEC-B analysis. I am therefore satisfied that the appropriate loads for severe accident mitigation have been identified.

615. As emergency arrangements are not in the scope of GDA, I have not assessed the information in detail. However, I judge from the information provided that the provisions included in the design to supply water and power via external connections are comparable to other new reactors. I anticipate a licensee's emergency arrangements will be appropriately assessed by ONR in the future and I am satisfied that my expectations for GDA have been appropriately met.

4.8.5 Strengths

616. The C&I, electrical power and cooling chain requirements identified by the RP meet the relevant expectations for SAPs AM.1, ESS.3, ESR.1, EES.1 and EES.9 (Ref. 2).

617. Whilst more detailed analysis will need to be performed by a future licensee, the DEC-B analyses submitted serves as a basis for SAMGs. This meets my expectations for FA.16 for GDA.

618. The RP has identified the severe accident human based safety claims related to emergency management and carried out HRA for these, meeting my expectations for SAP EHF.3 (Ref. 2).

619. The RP has identified the local emergency actions and performed dose assessment for those actions. The RP has also performed a dose assessment for the MCR and demonstrated that it remains habitable during a severe accident, meeting my expectations for SAP ESS.3 (Ref. 2) and paragraph 7.60 of IAEA SSG-2 (Ref. 6).

620. The RP has provided information related to mobile equipment and connection points. At this stage (in GDA) the provisions are adequate and clearly thought through.

4.8.6 Outcomes

621. I have raised two minor shortfalls related to the justification for placing safety functions related to the EHR [CHRS] and ECS on the SAS, instead of the KDA [SA I&C] (see sub-section 4.8.1) and claims related to inconsistencies between the RP's own requirements and the claims in the deterministic analysis of the EUF [CFES].

4.8.7 Conclusion

622. I consider that the UK HPR1000 design should enable severe accident management and that the safety case serves as a basis for the development of more detailed severe accident management guidelines by the future licensee.

4.9 Assessment of Claims Related to Practical Elimination of Early or Large Releases

623. Aligned with IAEA SSR 2/1, Requirement 20 (Ref. 6), it is my expectation for a new reactor design that it is demonstrated through an appropriate consideration of design extension conditions (as part of a broader demonstration of defence in depth), that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'. IAEA SSR 2/1 (Ref. 6) also states that:

- An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time; and
- A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

624. Ref. 78 provides a summary of the RP's arguments as to why it considers that accidents leading to early or large releases are practically eliminated through the UK HPR1000 design.

625. The RP's approach to practical elimination is to use a probabilistic and deterministic approach. The probabilistic approach uses numbers derived from its Level 1, 2 and 3 PSA and draws comparisons to probabilistic targets. The deterministic approach relates to a demonstration that the SSCs are adequately designed to prevent, protect and mitigate accidents that would lead to an early or large release.

626. In this section, I present my assessment of the RP's arguments related to practical elimination against the expectations of IAEA SSR 2/1, SSG-2 (Ref. 6) and WENRA 'Practical Elimination Applied to New NPP Designs – Key Elements and Expectations' (Ref. 12).

4.9.1 Definitions for Practical Elimination of Early or Large Releases of Radioactivity

627. The RP considers that scenarios which can lead to an early or large release are practically eliminated if it is either physically impossible for the accident or sequence to occur, or if the accident sequence can be considered with a high degree of confidence to be extremely unlikely to arise (Ref. 78). This approach aligns with that in IAEA SSR 2/1 (Ref. 6).

628. The RP does not provide a definition for "large" or "early" within Ref. 78. In response to RQ-UKHPR1000-1754 (Ref. 81), the RP provided a qualitative description of what constitutes an early release. The RP considers that an early failure is one that occurs a significant time before RPV failure or at the time of RPV failure. In terms of "large" the RP has explained that it links "large" to the state of the containment during a severe accident, rather than an exact radiological release. The RP has not attempted to link the definitions of large and early to any potential off-site responses. Instead, Ref. 81 lists the following sequences or phenomena that could lead to an early or large release:

- MCCI;
- DCH;
- high energy hydrogen combustion modes;
- steam explosion;
- containment over-pressure;
- rupture of a large component in the RCP [RCS];
- large reactivity insertion;

- containment isolation failure;
- containment bypass;
- severe accidents with an open containment; and
- fuel failure in the SFP.

629. The list aligns well with that provided in paragraph 3.56 of SSG-2 (Ref. 6) and covers the whole spectrum of early to late containment failures. Importantly, the RP has also recognised that severe accidents during shutdown states with open containment should be practically eliminated (IAEA SSG-53 (Ref. 6)). Moreover, the above list also aligns well with the different types of accidents identified in WENRA guidance (Ref. 12).

630. The RP has claimed in response to RQ-UKHPR1000-1754 (Ref. 81) that if the above sequences or phenomena are practically eliminated, then no off-site measures are required during a severe accident. This represents a reasonable design objective which is consistent with IAEA expectations for practical elimination. However, this does not necessarily mean there is no requirement for off-site planning including some practical measures; the requirements for emergency planning for a future licensed plant would need to be considered in accordance with REPPIR19 legislation (Ref. 101). Notwithstanding this, the radiological consequences predicted in the Level 3 PSA (Ref. 77) for release category RC101 (LB-LOCA with the SADV, IVR, EHR [CHRS] and EUH [CCGCS] effective, and therefore no use of EUF [CFES]) at 1 km, over the course of a year, is less than 5 mSv. It is therefore possible that the doses in the nearest residential area (assuming a distance of about 1 km) would be lower than the ERL's recommended by UK Health Security Agency (Ref. 131).

631. Aligned with paragraph 7.72 of IAEA SSG-2 (Ref. 6), claims of physical impossibility are seldom used throughout Ref. 78. The RP only claims that reactor core melt whilst the core is unloaded is physically impossible; in my opinion, this is clearly true as no fuel is within the reactor. For claims that releases are "extremely unlikely with a high degree of confidence", Ref. 78 provides both probabilistic and deterministic arguments.

632. For probabilistic arguments, the RP uses a target that:

- the total sum of frequencies of accident sequences that can lead to an early or large release is lower than 10^{-6} pa;
- an individual sequence has a frequency lower than 10^{-7} pa; and
- the numerical targets in the RP's general requirements are met (Ref. 107).

633. For the probabilistic part of the demonstration of practical elimination, WENRA guidance (Ref. 12) states that targets can be specified for both individual sequences and an overall target for practical elimination of early or large releases. ONR does not have any specific expectations with regards to numerical targets for the purpose of demonstrating practical elimination. However, I consider that ONR's numerical targets (SAP NT.1 (Ref. 2)) provide relevant benchmarks. For example:

- The RP's target related to the total sum of the frequencies of accident sequences that can lead to an early or large release equates ($< 10^{-6}$ pa) is similar to the frequency targets for (but not directly comparable to) Numerical Target 8 (Ref. 2).
- Although ONR does not have a directly comparable target for a single sequence leading to an early or large release, the RP's approach to defining a limit on a single sequence being one decade less than the total ($< 10^{-7}$ pa) is similar to ONR's guidance related to frequency of individual sequences which make up a dose band (see paragraph 749 of ONR's SAPs (Ref. 2).
- The RP has also used numerical targets, described in Ref. 107, that are directly comparable to ONR's Numerical Targets 7, 8 and 9.

634. With this in mind, I consider that the RP's numerical targets are appropriate to support the probabilistic part of its arguments, and I therefore consider that the RP's approach is aligned with expectations set out in WENRA guidance. In my assessment I have therefore used the RP's targets related to the frequency of individual sequences and sum of the frequency of sequences.

635. The RP recognises that deterministic arguments are an important strand of practical elimination and the majority of Ref. 78 focusses on these arguments. This approach aligns with the expectations set out in WENRA 'Practical Elimination Applied to New NPP Designs' (Ref. 12).

4.9.2 Assessment of Deterministic and Probabilistic Arguments

636. The RP recognises that all of the levels of defence in depth are important for demonstrating that early or large releases have been practically eliminated.

637. For each of the items listed in paragraph 628, the RP has presented both deterministic and probabilistic arguments as appropriate to provide an overall argument that sequences that lead to early or large releases have been practically eliminated.

638. In this section, I present my assessment of the RP's probabilistic and deterministic arguments related to each of these aspects. However, since the majority of this report is focused on the deterministic analysis of DEC-B safety features I have not repeated my assessment of the deterministic arguments in detail here. I have therefore grouped the arguments related to practical elimination of early or large releases due to phenomena which are prevented by the DEC-B safety features. Based on the RP's safety case, I have therefore structured sections 4.9.2.1 to 4.9.2.7 in the following manner:

- MCCI, steam explosions, high energy hydrogen combustion, DCH and containment overpressure
- Rupture of a large component in the RCP [RCS]
- Large reactivity insertion
- Containment isolation failure
- Containment bypass
- Severe accidents with open containment
- Severe accidents in the SFP

639. For each category above, the RP has provided a comparison of the frequency of the sequences which lead to an early or large release due to the phenomena in question to its own sequence frequency target of 10^{-7} pa. The RP uses the Level 1 PSA (Ref. 24) and Level 2 PSA (Ref. 102) to identify the sequence frequency as appropriate. For some cases, the Level 1 PSA can be used directly to derive a large release frequency as the core damage state results in a direct release to the environment (e.g. severe accidents during open containment). The RP has presented the predicted point estimate frequency in units of occurrence per reactor year (pry). Simply put, this is the most likely value in a probability distribution of the occurrence during the time a demand may be placed on it. Since this number is always larger than the frequency per annum (pa) (which accounts for time at risk) then I judge that the comparison of the numbers is valid. Within Ref. 78, the RP has consistently provided 'the point estimate frequency' and the '95th percentile frequency'. The purpose is to provide an indication of uncertainty associated with predicted frequency. For the purposes of this report, I have only used the point estimate frequency as it is the mean value.

640. In addition to my assessment of whether the sequence frequency is lower than the RP's target of 10^{-7} pa, I have also considered whether the summed frequency of large

releases is greater than its acceptance criteria of 10^{-6} pa, and whether ONR's targets 7, 8 and 9 have been met. I summarise my assessment of this in sub-section 4.9.2.8.

641. In addition to the Level 1 (Ref. 24) and Level 2 PSA (Ref. 102) considered for the individual sequence, the RP has used results from the Level 3 PSA (Ref. 77) to demonstrate that numerical targets 7, 8 and 9 have been met. The assessment of the Level 1, 2 and 3 PSA has been performed by ONR's PSA inspector. In general, the assessment has found that the PSA is adequate for GDA (Ref. 9). My assessment has only, therefore, looked at the way the output of the PSA has been used for arguments of practical elimination.

4.9.2.1 MCCI, Steam Explosions, High Energy Hydrogen Combustion, DCH and Containment Overpressure

642. For accidents in which there is a closed containment, the RP has argued that sequences that lead to an early or large release due to MCCI, steam explosions, high energy hydrogen combustion, DCH and containment overpressure are practically eliminated.

643. For accidents that occur during when the RCP [RCS] is closed (POS A, B and most of C) the RP argues that the design basis measures, DEC-A and DEC-B safety features prevent the conditions in which the above phenomena could occur.

644. The RP recognises that a key aspect for the demonstration of practical elimination is the concept of defence in depth. Ref. 78 provides an overview of the main safety systems which prevent design basis accidents escalating to severe accidents in which the phenomena have the potential to occur. The RP states that diverse protection has been provided for all frequent faults and that DEC-A analysis has been performed. Importantly, the RP highlights that the F-SC3 ASP [SPHRS] provides an additional line of defence against loss of cooling chain / power faults. ONR's assessment of the adequacy of the protection available for design basis faults (termed DBCs by the RP) and DEC-A faults is within the scope of the Fault Studies assessment (Ref. 10), which has found that the RP's fault identification process is comprehensive and that adequate protection is provided for all faults identified, with large margins to acceptance criteria for most faults.

645. As stated previously in sub-section 4.4, the RP has used the Level 1 PSA (Ref. 24) to determine DEC-B scenarios in which there is escalation of an initiating event to a core damage state.

646. For GDA, a key part of the demonstration of practical elimination of early or large releases is the demonstration that the safety features which mitigate the DEC-B scenarios are effective, such that conditions that could lead to phenomena which could challenge the containment are prevented. Ref. 78 summarises how MCCI, DCH, high energy hydrogen combustion (those which may challenge the containment), steam explosions and containment overpressure are practically eliminated. The arguments are largely based on the deterministic analysis. The RP argues that the IVR strategy has been demonstrated to be effective for the bounding case (LB-LOCA), such that MCCI and ex-vessel steam explosions are prevented. In addition, the RP argues that the EHR [CHRS] and EUF [CFES] prevent containment overpressure sequences, therefore conditions resulting in overpressure are prevented. In addition, the RP argues that the SADVs are effective in reducing the pressure of the RCP [RCS] to a low enough pressure to avoid HPME and DCH. In addition, the RP has provided arguments for why in-vessel steam explosions are extremely unlikely. I have presented my assessment of the evidence that supports these claims in sub-sections 4.2 and 4.5 of this report and have found that the RP has presented adequate evidence that the

severe accident safety features are adequately designed to prevent these phenomena in the DEC-B scenarios analysed.

647. Besides in-vessel steam explosions, the relevant phenomena could occur if the associated safety features fail or are ineffective. For each of the phenomena, the RP has provided a sequence frequency in Ref. 78 that could lead to that phenomenon and therefore, on a conservative basis, would lead to an early or large release. The RP applies the probabilistic argument that the sequences are less than the 10^{-7} pa frequency that it has defined as demonstrating practical elimination. Below I have summarised the RP's arguments related to the severe accident phenomena:

- MCCI – MCCI is prevented by the Level 3 defence in depth safety measures and by IVR. The point estimate large release frequency caused by MCCI is predicted to be 2.73 x 10^{-8} pry in the level 2 PSA (Ref. 102), which is less than the 10^{-7} pa target set by the RP.
- DCH – DCH is prevented the Level 3 defence in depth and by the SADVs. The point estimate large release frequency caused by DCH is predicted to be 1.13 x 10^{-10} pry, in the level 2 PSA (Ref. 102) which is less than the 10^{-7} pa target set by the RP.
- High energy hydrogen combustion – Accidents leading to this are prevented by Level 3 defence in depth and by the EUH [CCGCS]. The point estimate large release frequency caused by hydrogen related phenomena is predicted to be 4.68 x 10^{-10} pry in the level 2 PSA which is less than the 10^{-7} pa target set by the RP.
- Containment overpressure – Containment overpressure is prevented by the Level 3 defence in depth, and both the EHR [CHRS] and EUF [CFES]. The point estimate frequency of large release due to containment overpressure is 8.47 x 10^{-9} pry.
- Ex-vessel steam explosions - The point estimate frequency of large release due to ex-vessel steam explosion phenomena predicted in the level 2 PSA (Ref. 102) is 5.81 x 10^{-9} pry which is less than the 10^{-7} pa target set by the RP.
- In-vessel steam explosions - The frequency of large release due to in-vessel steam explosion phenomena predicted in the level 2 PSA is lower than 10^{-13} pry which is less than the 10^{-7} pa target set by the RP. This number is very low because it is based on theoretical upper limits of both the occurrence of the steam explosion and the damage it causes the RPV.

648. Based on the PSA assessment of the Level 1 and Level 2 PSA (Ref. 9), I am satisfied that these numbers are appropriate for use in the demonstration of practical elimination.

649. Based on the Fault Studies assessment (Ref. 10), my assessment of the effectiveness of the severe accident safety features, and the RP's probabilistic arguments (Ref. 9) I am satisfied that the RP has provided adequate arguments that the severe accident phenomena MCCI, steam explosions, high energy hydrogen combustion, containment overpressure and DCH have been practically eliminated.

4.9.2.2 Rupture of a Large Component in the RCP [RCS]

650. There are specific reactor faults which can either lead to a severe accident or potentially directly to failure of containment with a severe accident. For these, the majority of the RP's effort for safety justification is on prevention of occurrence of the faults. The RP categorises certain components as 'Highest Integrity Component' (HIC), with the objective of preventing their failure.

651. Ref. 78 lists the large components of the RCP [RCS] as the RPV, the pressuriser and the SGs and provides a high-level summary of the HIC arguments associated with

each. ONR's Structural Integrity inspector has sampled and assessed the RP's arrangements for developing and implementing HIC safety cases, the details of which are presented within the Structural Integrity report (Ref. 98). In general, the Structural Integrity inspector is broadly satisfied that the RP understands ONR's regulatory expectations related to the Structural Integrity topic area, and has developed an adequate methodology to construct robust HIC Structural Integrity safety cases (Ref. 98). It is noted however, that a number of assessment findings have been raised regarding the evidence provided within GDA to demonstrate that this methodology has been implemented for the full range of HICs identified in accordance with the RP's own requirements. Whilst these assessment findings are important, the Structural Integrity inspector considers overall 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. I am therefore satisfied that the RP has demonstrated an adequate approach for Structural Integrity HIC safety claims within GDA, which support deterministic arguments related to practical elimination.

652. In terms of probabilistic arguments, the RP claims that it has grouped these accidents into two types:

- Failure leading to a severe accident which can be mitigated by severe accident safety features – this includes failure of the SGs and failure of the pressuriser. The RP claims that the consequences of these are bounded by the LB-LOCA, and that the contribution of frequency of the LB-LOCA takes failure of these into account.
- Failure leading directly to containment failure –the only component in this category is the RPV.

653. For the first category, Ref. 78 claims that failures of these components are therefore taken into account in the sequence frequencies discussed in sub-section 4.9.2.1 as they are grouped within existing initiating events in the PSA, and the frequencies are within the RP's target for demonstrating practical elimination of sequences.

654. For the second category, the RP states that RPV failure has a point estimate frequency of 1.25×10^{-8} pry (Ref. 78), which is less than the RP's target for demonstrating practical elimination of sequences.

655. Based on the above, and supported by the ONR's Structural Integrity (Ref. 98) and PSA (Ref. 9) assessments, I am satisfied that the RP has provided adequate arguments that sequences involving failures of large components of the RCP [RCS] that would lead to an early or large release have been practically eliminated.

4.9.2.3 Large Reactivity Insertion

656. In this context, the RP defines large reactivity insertion faults as those which may result in early releases of radioactivity. In Ref. 78, the RP summarises which faults can lead to a large reactivity insertion. These are: beyond design basis SLBs and boron dilution faults. The RP has summarised the safety case for prevention and protection of boron dilution faults in Ref. 78.

657. Heterogenous boron dilution refers to the faults in which a 'slug' of unboronated water can form undetected and is transported to the core causing an uncontrolled reactivity excursion. The prevention of heterogeneous boron dilution is reliant on start-up procedures and administrative lockout of SSCs. Deterministic claims related to the prevention of these faults have been assessed by ONR's Fault Studies inspector (Ref. 10). As a result of GDA, the RP has upgraded some procedures related to start-up of RCPs to F-SC1.

658. Within Ref. 78, the RP has not addressed inherent boron dilution faults, which the RP defines as ones which can occur due to accident conditions, such as the condensate reflux phenomenon which can occur during LOCAs and can lead to a formation of unboronated water in the cross-over leg. This is because the RP claims that this does not have the potential to lead to an early or large release. These claims are assessed within the Fault Studies report (Ref. 10) and I consider the omission of this acceptable for the purposes of Ref. 78.

659. Homogenous boron dilution refers to accidents in which the majority of the coolant within the RCP [RCS] is diluted uniformly. It can occur due to faults in systems which regulate the RCP [RCS] chemistry. For homogenous boron dilution, the protection is provided mainly by the ex-core flux detectors (which detect power excursions), reactor trip and isolation of the dilution source. ONR's Fault Studies inspector has assessed the RP's claims that adequate protection is provided against these faults and considers them acceptable for GDA (Ref. 10).

660. Although there are multiple Assessment Findings associated with boron dilution faults the Fault Studies inspector considers that the RP has provided a sufficient deterministic safety case for boron dilution faults (Ref. 10).

661. A double ended guillotine SLB with ATWS, or double ended guillotine SLB with failure of the MSIVs would result in an uncontrolled reactivity addition fault. The deterministic arguments have not been provided in Ref. 78, but relate to assignment of the MSL as a highest integrity component, and that adequate protection is provided via the F-SC1 RPS [PS], F-SC1 MSIVs and F-SC2 KDS [DAS] even if the SLB were to occur. Because of this, I consider the omission of the deterministic arguments is only a minor shortfall in Ref. 78 and not the design.

662. Related to the probabilistic arguments, the RP has argued that the fault sequences which lead to a reactivity insertion have a point estimate frequency determined by the Level 1 PSA of 1.09×10^{-8} pry (Ref. 78). This is less than the RP's target for demonstrating practical elimination of sequences, and is comparable to both failure of the RPV and the sequence frequencies which result in phenomena arising from severe accidents which can challenge the containment.

663. Based on the Fault Studies assessment (Ref. 10) which found that the deterministic arguments related to boron dilution faults were adequate for GDA, and that adequate protection is provided against SLBs, and the RP's probabilistic arguments which are underpinned by an adequate PSA (Ref. 9) I am satisfied with the RP's arguments that reactivity accidents that result in early or large releases have been practically eliminated.

4.9.2.4 Containment Isolation Failure

664. The RP's safety case makes claims on containment isolation for some design basis faults, some DEC-A sequences and all the reactor DEC-B sequences it has analysed. The RP claims that failure of containment isolation during these faults can result in an early or large release.

665. In Ref. 78, the RP provides an overview of the claims related to containment isolation failure. Containment isolation is provided by a "functional group", which is not assigned to a single system. Any penetration to the containment is accompanied by two isolation valves in series, and these valves are part of the system to which the pipework belongs to.

666. In most cases, these valves are active valves which can be controlled automatically or manually by the F-SC1 RPS [PS], F-SC2 KDS [DAS] and F-SC3 KDA [SA I&C].

However, some valves include non-return valves, instead of active valves, in order to allow operation during design extension conditions (e.g. as is the case for one of the valves on the EHR [CHRS]).

667. The arrangements of valves, and diversity of the valves has been assessed by the Mechanical Engineering inspector (Ref. 118). Although an Assessment Finding was raised related to the qualification of the ASG [EFWS] isolation valve, the assessment has found that adequate justification of the design of the containment isolation had been provided for GDA.

668. In relation to probabilistic arguments, Ref. 78 states that the point estimate frequency of sequences that lead to a large release by containment isolation failure is 2.89×10^{-9} pry, which is less than the RP's target for demonstrating practical elimination of sequences (10^{-7} pa).

669. Supported by ONR's Mechanical Engineering assessment (Ref. 118), and ONR's PSA assessment (Ref. 9), I am satisfied with the deterministic and probabilistic arguments provided by the RP that sequences involving failure of the containment isolation have been practically eliminated.

4.9.2.5 Containment Bypass

670. The RP identifies that a SLB (with an induced SGTR) and interfacing LOCA has the potential to lead to severe accidents with containment bypass (Ref. 78).

671. The protection measures for both SGTR and SLB have been assessed by the Fault Studies inspector (Ref. 10) and it has been found that adequate protection exist against both individual accidents. The RP has performed deterministic analysis of the SGTR as a consequence of the SLB as part of its DEC-A analysis. The DEC-A analysis has been assessed by ONR's Fault Studies inspector, who has found that adequate protection is available for DEC-A faults. Importantly, Ref. 78 states that neither SGTR alone, or in coincidence with the SLB can result in an early or large release if the accident does not escalate to a core melt scenario. Although the Fault Studies assessment has found that the SGTR does result in radiological consequences higher than the Basic Safety Level (BSL) of Target 4 (Ref. 2), the assessment has also found that the radiological consequence analysis is overly conservative and that when more appropriate conservatisms are used the BSL can be met (Ref. 10). Nevertheless, I judge that the offsite consequences associated with an SGTR without core melt do not constitute an early or large release of radioactivity using the RP's definition. Based on the Fault Studies assessment (Ref. 10), I am satisfied that adequate design basis safety measures are in place to prevent escalation to a severe accident for both the SLB and SGTR taken independently and the SGTR as a consequence of the SLB.

672. An interfacing LOCA is one in which a pipe connected to the primary circuit (e.g. one used in the nuclear sampling line or for residual heat removal) breaks outside of the containment. In Ref. 78, the RP also summarises the deterministic arguments related to an interfacing LOCA. Claims related to adequate protection for interfacing LOCAs have been assessed by the Fault Studies inspector (Ref. 10), who has found that adequate protection is available to prevent escalation of the fault to a severe accident. The protection is similar to that for a LOCA within the containment, however the additional action of isolating the line with the break is required. An interfacing LOCA alone without escalation to a severe accident (which would require failure of the MHSI and LHSI) does not result in an early or large release.

673. The RP has not included within Ref. 78 information related to containment bypass due to creep failure of the SG tubes during severe accidents. As discussed in sub-section

4.5, the RP has provided evidence that actuation of the SADVs avoids creep rupture of the SG tubes during severe accidents. I judge that this is simply an omission of the document, which I judge to be a minor shortfall and I have not taken this further.

674. In relation to probabilistic arguments, Ref. 78 states that the point estimate frequency of sequences that lead to a large release by containment bypass is 8.00 x 10^{-9} pry, which is less than the RP's target for demonstrating practical elimination of sequences (10^{-7} pa).

675. Supported by ONR's Fault Studies assessment (Ref. 10) of the deterministic arguments, and ONR's PSA assessment (Ref. 9), I am satisfied with the deterministic and probabilistic arguments provided by the RP that sequences involving containment bypass have been practically eliminated.

4.9.2.6 Severe Accident with an Open Containment

676. In Ref. 78, the RP describes states in which the containment may be opened to transport equipment in and out, such as the Multi-Stud Tensioning Machine (MSTM), which is used to open and close the RPV head for refuelling or maintenance. This only occurs during shutdown conditions. If an accident were to occur during this time which then progressed to a core melt scenario, the radioactivity released from the core would be directly released from the containment and result in both an early (and large) release.

677. The RP states that the equipment hatch can be opened in POS C, D, E and F (Ref. 78). The states are when the reactor is shutdown and encompass operations related to maintenance and core unloading.

678. The operation to remove the studs that hold down the RPV head occurs in POS C and D. This time is referred to by the RP as Maintenance Cold Shutdown (MCS). During this time, no water level exists above the RPV, and the water in the RPV is drained to a level slightly lower than the RPV head flange. Following removal of the studs, the reactor pool is filled and the RPV head is lifted and moved so that fuel can be removed from the core. The fuel is removed during POS E and is fully unloaded at POS F.

679. During MCS the water level is at approximately ¾ loop level (which is the level ¾ the height of the hot and cold leg nozzles). This is much lower than the water level when at POS E and F (approximately 11 meters lower). The worst time for an accident of this nature to occur is during ¾ loop level.

680. The Fault Studies assessment (Ref. 10) has found that the RP has considered all appropriate initiating events that occur during shutdown, and that the RP has used MCS as the initial condition for the deterministic analysis (i.e. the worst time). The protection is provided through the F-SC1 RIS [SIS], the F-SC1 RPS [PS], the F-SC2 KDS [DAS], the F-SC2 SAS, and the F-SC3 EHR [CHRS]. The Fault Studies assessment (Ref. 10) has found that these protective safety measures are sufficient to prevent core uncovery and therefore prevent core damage and a potential release.

681. In Ref. 78, the RP argues that for POS E and F, if an accident were to occur which led to a reduction in water level, and that the design basis and DEC-A measures failed, there is sufficient time to perform further actions that have been identified in the design basis analysis. For example, during POS E, Ref. 78 claims that there is approximately 80 hours between an initiating event and the core uncovering, allowing for time for the containment to be sealed back up in the worst case scenario.

682. However, for ¾ loop level operations, if an accident were to occur which led to a reduction in water level, and that the design basis and DEC-A measures failed, the RP claims that only 2 to 3 hours would be available until a core melt scenario was

reached. The RP states, therefore, that insufficient time is available to close the containment. The RP states, however, that the operations have been optimised to minimise the number of times in which the containment needs to be opened during ¾ loop level operations. In response to RQ-UKHPR1000-1695, I judge that the RP has provided convincing arguments related to the optimisation of these operations. However, this is a matter for a licensee and it will need to provide an adequate safety case, cognisant of how it plans to undertake operations.

683. In relation to probabilistic arguments, Ref. 78 states that the point estimate frequency of sequences that lead to a large release by severe accidents during open containment bypass is 1.55 x 10^{-8} pry, which is less than the RP's target for demonstrating practical elimination of sequences (10^{-7} pa).

684. Supported by ONR's Fault Studies assessment (Ref. 10), and ONR's PSA assessment (Ref. 9) I am satisfied with the deterministic and probabilistic arguments provided by the RP that sequences involving severe accidents during times in which the containment is open have been practically eliminated.

4.9.2.7 Fuel Failure in the Spent Fuel Pool

685. The UK HPR1000 SFP is used to store and transfer new and irradiated fuel under boronated water. The SFP provides a boronated storage rack with the capacity for 1,020 irradiated fuel assemblies. The SFP is made from reinforced concrete, with a leak-tight steel liner.

686. The RP's arguments related to practical elimination of severe accidents in the SFP are based on avoidance of fuel damage by preventing fuel uncovery. In my opinion, the arguments can be summarised as follows:

- The RP has analysed severe accidents scenarios in the SFP, and determined that no further mitigation can be provided following fuel uncovery which would prevent an early or large release. The RP has therefore concluded that it is necessary for it to demonstrate that the design practically eliminates fuel melt caused by fuel uncovery.
- One train of the F-SC2 PTR [FPCTS] provides normal cooling to the SFP during power operations, and two trains provide cooling during refuelling.
- The PTR [FPCTS] is normally cooled by the F-SC1 RRI [CCWS].
- The UK HPR1000 includes a diverse ultimate heat sink for the PTR [FPCTS], which is provided by the F-SC3 ECS.
- The PTR [FPCTS] is equipped with siphon breakers, and segregation between the suction lines prevents common cause failure of the trains of PTR [FPCTS].
- If the PTR [FPCTS] pumps are lost, or if an unisolable break occurs in the connecting piping to the SFP, then the ASP [SPHRS] provides a FC-2 makeup function to the SFP which is sufficient to prevent fuel damage for several days. This is an important advantage that the UK HPR1000 has regarding additional defence in depth for the SFP.
- Design basis and DEC-A analysis has been performed on all faults associated with the SFP, and adequate protection is provided against those faults.

687. The RP's safety case for the SFP has presented design basis and DEC-A analyses for faults related to connecting pipe breaks, loss of heat removal, and dropped fuel. The RP has screened out the following from the design basis and DEC-A analysis:

- SFP gate failure
- Pipeline connected to the reactor pool break
- Fuel transfer tube (FTT) break
- Spurious drainage of SFP

- SFP structure damage (including pool liner)

688. The stated reason for screening out the first four is that the faults are self-limiting or bounded by other initiating events which have been taken forward. The Fault Studies assessment (Ref. 10) (supported by the Structural Integrity (Ref. 98) and Civil Engineering assessments (Ref. 8)) considers that the substantiation of these decisions for design basis and DEC-A purposes is reasonable, and on that basis I am content that they do not need a practical elimination demonstration.

689. The performance of the spent fuel building and SFP structure and liner has been assessed in some detail in the ONR Civil Engineering assessment (Ref. 8) considering the static and dynamic loads induced by a seismic event (excluding dropped loads) up to the design basis earthquake and judged to be adequate for GDA. The RP's claims related to beyond design basis loads and the absence of cliff-edge effects have also been judged to be adequate for GDA (Ref. 8). However, for both design basis and beyond design basis loads, ONR's Civil Engineering inspector considers that there are site-specific issues that should be addressed by the licensee, either through normal business or Assessment Findings.

690. ONR's Civil Engineering has also assessed the RP's claims that the SFP concrete and liner can withstand the design basis dropped loads (Ref. 8). Whilst ONR's Civil Engineering inspector found that further work was required at the site-specific stage, the analysis to demonstrate the SFP's withstand was adequate for GDA. I note, however, that the RP has only considered a dropped fuel assembly as the design basis dropped load. In my opinion there are potentially larger loads that could drop onto the SFP, such as buildings or cranes, which have not been considered in the RP's design basis analysis or in Ref. 78. These could result from a beyond design basis seismic event which cause structural failure of buildings, structures and/or large equipment, such as cranes. The risks from loads larger than those considered in the design basis are something that could be assessed in the PSA. However, it was agreed between ONR and the RP that a UK HPR1000 seismic PSA would not be submitted during GDA. Instead, insights from the FCG3 reference plant seismic PSA would be utilised, ahead of a site-specific seismic PSA being developed at a point in the future.

691. The outstanding matters from the civil engineering assessment (and the agreed PSA scope) limit the extent to which it can be argued that severe accidents as a result of SFP structure damage can be shown to be practically eliminated in GDA. However, my specialist colleagues have not identified any specific concerns that claims made on the robustness of the SFP structure in GDA will not be demonstratable in later design phases, and on that basis I judged there to be little benefit in pursuing, in my practical elimination assessment, additional justifications that other specialist areas are confident can be provided later as part of normal business.

692. In terms of the protection available for design basis and DEC-A loss of coolant or cooling faults considered by the RP, ONR's Fault Studies inspector considers that the redundancy in the PTR [FPCTS] and the diverse heat sink (ECS) are sufficient to prevent boiling in the SFP (which is the design basis acceptance criterion for accidents in the SFP). If these systems fail additional defence in depth provided by the ASP [SPHRS] (which can provide make-up water for over 120 hours via gravity) can account for the water lost by boiling (Ref. 10).

693. In addition to the design basis and DEC-A analysis, as stated previously, the RP has performed severe accident analysis on the SFP in which melting of the whole inventory of the SFP is modelled using the ASTEC code (Ref. 132). The RP concludes that the consequences would exceed any radiological targets and that no mitigation is achievable; therefore, accidents in the SFP should be practically eliminated. I judge

that this approach is reasonable and aligns with IAEA and WENRA guidance (Refs 6 and 8), and is consistent with the approach taken by other requesting parties.

694. In Ref. 132, the RP demonstrates that for the most onerous fault condition (i.e. the one with the least time available), the available time to implement safety actions is 30.9 hours. For this scenario, a local action is required to align valves from the ASP [SPHRS] to the SFP, which is a F-SC2 design basis safety measure. Whilst the RP argues that successful implementation of the ASP [SPHRS] sufficiently demonstrates that severe accidents due to breaks in the SFP have been practically eliminated, Ref. 132 also identifies additional water sources that could be used to make up the SFP (e.g. the extra cooling system, the Firefighting Water Production System (JAC [FWPS]), sources from the conventional island and mobile equipment).

695. Supported by ONR's Fault Studies assessment (Ref. 10) of the deterministic analysis, which has concluded that sufficient protection is available for accidents in the SFP, and the additional deterministic arguments relating to the time available and the additional water sources available, I am content that the RP has provided adequate deterministic arguments that accident sequences in the SFP that would lead to fuel uncovery are prevented by the design of the UK HPR1000.

696. In terms of the probabilistic arguments, the RP argues that the total sequence frequency of faults resulting in fuel uncovery and therefore fuel melt in the SFP is 6.64 x 10^{-9} pry, which is below the RP's target for demonstrating practical elimination of sequences (10^{-7} pa) (Ref. 78). Given that the highest probability for sequences leading to a large release for the reactor is predicted to be 2.73 x 10^{-8} pry (related to sequences leading to MCCI) and the lowest is 1.13 x 10^{-10} pry (for DCH), I judge that the predicted sequence frequencies are reasonably comparable. I have not used the frequency of in-vessel steam explosions in my comparison (10^{-13} pry) as it is based largely on theoretical upper limit predictions.

697. To summarise, I judge that, for GDA, the RP has provided adequate deterministic and probabilistic arguments to demonstrate that accident sequences in the SFP which could lead to an early or large release are practically eliminated by the UK HPR1000 design. However, a future licensee will need to consider how the external hazards PSA affects the arguments related to practical elimination of accidents in the SFP (see paragraph 689 to 691).

4.9.2.8 Overall Assessment of PSA Arguments to Support Practical Elimination

698. As stated in the previous sections (4.9.2.1 to 4.9.2.7), for each sequence or phenomena, Ref. 78 has presented the large release frequency derived from the Level 1 and 2 PSA and has demonstrated that its sequence frequency target of 10^{-7} pa is met. The sequence frequencies all lie within the 10^{-7} to 10^{-10} pry range, which appears reasonable.

699. In Ref. 78 the RP has stated that the point estimate value of the total large release frequency is 8.78 x 10^{-8} per reactor year, which satisfies one of its targets for practical elimination of early or large releases (10^{-6} per reactor year, see paragraph 632).

700. Ref. 78 includes a brief summary of the Level 3 PSA (Ref. 77) and comparisons against the RP's targets, which are the same as ONR's Numerical Targets 7, 8 and 9 described in the SAPs (Ref. 2). The RP states that the Level 3 PSA (Ref. 77) demonstrates the BSO for Targets 7 and 8 are met, and that although the BSO of Target 9 is not met, it is only exceeded marginally; so much so that the total risk is only 2% of the BSL for Target 9. In the Level 3 PSA report (Ref. 77), it can be seen that the dominant risk contribution for Target 9 comes from the dropped fuel cask accident within the SFP building, which contains 32 fuel assemblies. The RP claims that no

credit for decontamination by the SFP water is considered, no impact limiters are considered, and a generic non-conservative source term is applied (Ref. 9).Through collaboration with the PSA inspector, I have gained confidence that the analysis associated with the cask drop accident is conservative, and that removal of these conservatisms would decrease the overall risk to below the BSO for ONR's Target 9. I am therefore satisfied that the small exceedance of the BSO is acceptable and not a concern for the purpose of demonstrating practical elimination in the SFP.

701. To summarise, the RP has compared the PSA risks with its own probabilistic criteria for demonstrating practical elimination and demonstrates that these are met. Whilst ONR does not set criteria for this purpose, I am satisfied that when compared with ONR's numerical targets as benchmarks, the risks are extremely low. Complimented by the RP's deterministic arguments across levels of defence in depth, I am satisfied that the probabilistic arguments support the position that early or large releases of radioactivity are extremely unlikely with a high degree of confidence. I am content that this overall approach to probabilistic considerations is aligned with the expectations of IAEA SSG-2 (Ref. 6) and WENRA guidance for practical elimination (Ref. 12).

4.9.3 Strengths

702. The RP has identified all relevant scenarios and phenomena that have the potential to lead to an early or large release. These align well with the expectations of SSG-2 and WENRA guidance for practical elimination.

703. The RP has recognised that all levels of defence in depth are important for the demonstration of practical elimination, which is aligned with the expectations of 'Practical Elimination Applied to New NPP Designs' (Ref. 12). The RP has demonstrated through deterministic analysis that there are safety measures which prevent escalation to severe accidents.

704. The RP has derived its own targets for demonstrating the practical elimination of sequences that lead to early or large releases which appear reasonable.

705. Ref. 78 summarises how, taken together, the deterministic and probabilistic arguments support claims that early or large releases have been practically eliminated, with the majority of the arguments being deterministic. This is aligned with the expectations described in 'Practical Elimination Applied to New NPP Designs' (Ref. 12).

706. Ref. 78 also summarises arguments that demonstrate that the UK HPR1000 includes adequate mitigation for severe accident scenarios and phenomena that have the potential to lead to early or large releases.

707. The RP has demonstrated that its probabilistic targets are met. Judging these against ONR's targets (NT.1) in the SAPs, the RP has demonstrated that the BSO of Targets 7 and 8 are met, and that the BSO of Target 9 is only slightly exceeded, with likely further reductions in risk due to proposed modifications to the SFP crane. This satisfies my expectations for NT.1.

708. The approach taken for practical elimination aligns well with the expectations of IAEA SSR-2/1, SSG-2 (Ref. 6), and WENRA guidance for practical elimination (Ref. 12).

4.9.4 Outcomes

709. I have identified two minor shortfalls which are related to completeness of the RP's submission summarising the arguments related to practical elimination of early or large releases.

4.9.5 Conclusion

710. The RP's approach to demonstrate that the early or large releases have been practically eliminated by the UK HPR1000 is aligned with international expectations.

711. I consider that for GDA, the RP has made an adequate case that UK HPR1000 is designed such that early or large releases of radioactivity are practically eliminated.

4.10 Demonstration that Relevant Risks Have Been Reduced to ALARP

712. The demonstration that risks have been reduced to ALARP is a fundamental requirement of UK law and it is ONR's expectation that the RP provides an ALARP demonstration as part of GDA. The RP presents the general application of its ALARP methodology in Chapter 33 of the PCSR (Ref. 133). On a holistic level, the RP's Severe Accident Analysis and the Level 4 defence in depth provides a key element of the demonstration that risks associated with operation of the UK HPR1000 will be reduced to ALARP. In this section, I only address the aspects of ALARP associated with the Severe Accident Analysis topic area.

713. For Severe Accident Analysis, the demonstration of ALARP is provided in the main by the design of the safety features and the deterministic analysis which informs this design. The RP has summarised the aspects of ALARP related to the Severe Accident Analysis topic area in Ref. 79.

714. ONR's guidance for ALARP, NS-TAST-GD-005 (Ref. 4), states that meeting RGP is a strong indication that the requirements for demonstrating ALARP have been satisfied. However, NS-TAST-GD-005 (Ref. 4) also states that where RGP and associated guidance is not clear cut then the onus is on the RP to demonstrate that the risks are ALARP. For severe accidents, RGP comes in the form of standards, guidance, and the approach taken to meet these standards and guidance for other reactors.

715. Specific standards and guidance related to the provision of severe accident safety features are limited and are often high-level. There are often multiple ways to achieve the same objectives. However, what is common to all PWRs is the requirement to prevent or mitigate the risk from severe accident phenomena that can result in containment failure. These have been identified by the RP as: combustion of flammable gases, MCCI and basemat melt through, containment overpressure, HPME and DCH, steam explosions and containment bypass.

716. For each phenomenon, the RP in Ref. 79 provides a short summary of the different aspects to provide an overall argument that risks associated with the Severe Accident Analysis topic area have been reduced to ALARP, including:

- how the UK HPR1000 meets relevant standards and guidance;
- the severe accident management strategy provided (which is the subject of the majority of my report);
- how the strategies have evolved from previous designs to become those implemented in the UK HPR1000 design; and
- a comparison of the relevant aspects of other modern reactor designs (the AP1000 and EPR).

717. In the following sections (4.10.1 to 4.10.8) I present my assessment of the RP's ALARP demonstration, based on Ref. 79 and considerations of the wider safety case. Whilst Ref. 79 provides a holistic view, there are some specific cases in which the ALARP position is less clear and has required special attention during GDA. These are addressed specifically in Ref. 79 and also in my assessment.

718. I have applied the expectations of NS-TAST-GD-005 throughout my assessment. My assessment of whether the standards and guidance have been met for the design is presented throughout this report. In general, I judge that the RP's design has met the relevant standards and guidance. Therefore in sub-sections 4.10.2 to 4.10.8, I focus my assessment on whether the RP has reduced risks to ALARP.

4.10.1 Relevant Standards and Guidance

719. In relation to GDA, Annex 2 of NS-TAST-GD-005 states that the RP must set out the standards and codes used and justify them to the extent that ONR can 'deem' them RGP when viewed against ONR's SAPs. A comparison with other international/ national standards is one way in which this can be demonstrated. Throughout my assessment, I have made judgements against RGP. This subsection (4.10.1) considers whether a clear comparison to RGP is made by the RP in relation to severe accidents; it is not an overall judgement as to whether RGP has been met for the design as a whole.

720. In Ref. 79 the RP simply provides a list of IAEA standards, IAEA safety reports and WENRA guidance which it claims the design of the UK HPR1000 meets. I note that the RP lists 'Design of Reactor Containment Systems for Nuclear Power Plants', IAEA NS-G-1.10, 2004 (Ref. 134) as RGP. Whilst this document has been superseded by IAEA SSG-53 (Ref. 6), the expectations applicable for my assessment have not significantly changed. In addition, the RP has made a comparison to international standards and guidance (Ref. 135) and confirms that the UK HPR1000 design meets all of the relevant guidance. I judge that the RP has correctly identified the most important standards and guidance for severe accidents.

721. Separately the RP has performed a "gap analysis" against ONR's NS-TAST-GD-007 (Ref. 136). Ref. 136 identified that there were potential gaps in the definition of severe accidents, the expectation that ALARP is demonstrated, and the expectation that "uncertainty analysis" is performed. As a result, work was carried out early in GDA and the RP provided deliverables to meet ONR's expectations.

722. I am satisfied that the RP has identified appropriate RGP, and has performed a gap analysis with ONR's expectations. This approach aligns with the expectations of NS-TAST-GD-005 (Ref. 4). In the remainder of this section I consider the RP's arguments that the design of the key severe accident features of the UK HPR1000 meet RGP.

4.10.2 Corium Retention

723. The UK HPR1000 adopts the IVR strategy in order to prevent MCCI and ex-vessel steam explosions. The RP's reasons for choosing IVR over ex-vessel corium spreading and cooling are discussed below.

724. Ref. 79 describes the evolution of the IVR strategy from the M310, CPR1000 and ACPR1000 designs to the UK HPR1000. The RP states that the M310 had no dedicated IVR strategy, that an external water source was back fitted to the CPR1000+ plant to flood the reactor pit, and that a dedicated and optimised IVR strategy was implemented in the ACPR1000 onwards.

725. The RP makes high-level comparisons of its approach with the EPR and AP1000 designs. The RP provides sensible reasoning for why the corium spreading strategy may be more appropriate for larger reactors, but why the IVR strategy is appropriate for the UK HPR1000. Amongst these reasons is the operational experienced gained in the evolution of the Chinese fleet of reactors.

726. I agree that the RP's design of its IVR strategy is comparable to that for other reactor designs which adopt IVR and meets the expectations of IAEA SSG-2 (Ref. 81) such

that sequences that lead to MCCI and ex-vessel steam explosions are practically eliminated. In addition, the RP has provided arguments as to why further improvements would not be reasonably practicable. Specifically, I have challenged the RP on improving the time in which passive cooling is available, redundancy and delaying corium relocation.

727. In response to RQ-UKHPR1000-1695 (Ref. 81), the RP states that the IVR strategy already meets its own requirements related to passive filling of the reactor pit, as power supplies for active plant is considered to be available after 12 hours, and that in the limiting scenario (the SBO) the AC power is only required after 12 hours. As stated previously, this is inconsistent with the RP's analysis of the EUF [CFES] which requires the mobile generators to be in place by 11 hours. However, I note that this is only the case when the first line of Level 4 defence in depth (the EHR [CHRS]) has failed during the LB-LOCA. In addition to the arguments related to sufficient time being available to restore AC power, the RP provides reasoning related to the compact containment layout design as to why further improvements to the capacity of the passive flooding would be grossly disproportionate.

728. An additional connection between the ASP [SPHRS] and the reactor pit would extend the length of time that water could be passively fed to the reactor pit. However, the RP states that at the point that active reactor pit filling is required, the containment spray is also required, therefore there is no advantage for passive filling. Whilst I judge that there would be an advantage when the EUF [CFES] is in use (i.e. to replace water lost from evaporative losses through the EUF [CFES]), the RP also points out that this would introduce a new potential containment bypass, a risk of inadvertent flooding of the reactor pit and a new risk of boron dilution (the water in the ASP [SPHRS] tank is not boronated). I consider that the RP's arguments are reasonable, and that the capacity of the IVR system (i.e. 10 hours of passive feed) reduces relevant risks to ALARP.

729. Whilst the IVR system does not include redundancy in the passive filling line, the RP has pointed out that the active filling could be used if the passive line failed. In my opinion this is a reasonable ALARP approach.

730. In terms of grace times, the RP has made design modifications for the UK HPR1000 to reduce the time required to implement IVR. This modification removes the requirement for local action, allowing de-isolation of the IVR valves from the MCR with a key switch provided by the shift supervisor. In my opinion, the improvement in the design outweighs the negative impact (e.g. slight increase in risk of inadvertent flooding) and therefore contributes to reducing the risks to ALARP.

731. In addition, the RP has removed C&I interlocks that prevent implementation of passive and active IVR if the COT is less than 650 °C. The RP has also implemented further hardwired technology (see Ref. 117) which reduces the risk of malfunction of the COT reading. In my opinion, the increase in independence of the levels of defence in depth by removal of the interlock is a simple and effective measure to increase the reliability of IVR. I therefore consider the design modification to reduce the relevant risks to be a suitable ALARP measure.

732. For the purposes of GDA, I consider that the RP has demonstrated that the IVR strategy is effective, is comparable to other Generation-III reactor designs, meets RGP and that in the event of core melt the design reduces associated risks to ALARP.

4.10.3 Primary Depressurisation

733. As stated previously, the UK HPR1000 includes SADVs primarily to prevent HPME and DCH (Ref. 3).

734. Ref. 79 provides a description of the evolution of the plant design in relation to depressurisation of the plant in severe accident conditions, noting that for older plants the depressurisation was caried out by the PSVs. Recognising the need for independence of levels of defence in depth, the RP states that the ACPR1000 and UK HPR1000 include dedicated depressurisation valves, each train with the capacity of all of the three PSVs.

735. The RP makes comparisons to the EPR and AP1000, which also have dedicated depressurisation for severe accidents with similar levels of redundancy. The RP has stated in response to RQ-UKHPR1000-1695 (Ref. 81) that redundancy is included in severe accident systems where possible, and is addressed on a case by case basis. In this case, the RP states that the increase in reliability outweighs the negative aspects (additional piping, cost, risk of inadvertent opening). Whilst the risk of inadvertent opening has not been quantified by the RP, it can be seen from the other reactors that a similar logic has been applied. In my opinion redundancy in the SADVs is beneficial to severe accident management.

736. The RP's analysis, discussed in sub-section 4.5, demonstrates that a single SADV has the capacity to reduce primary circuit pressure well below the safety criterion and therefore HPME (and DCH) is avoided. Even when a 30 minute delay in operator action is applied, large margins are seen in primary pressure.

737. The RP has therefore demonstrated that the SADVs are effective, that redundancy has been included to increase the reliability, and that the means of depressurisation is comparable to other Generation-III reactors. I therefore consider that the RP has demonstrated that the design reflects RGP and that the relevant risks are reduced to ALARP.

4.10.4 Hydrogen Management

738. As discussed in previous sections, combustible gases pose various challenges to the containment and equipment. The EUH [CCGCS] has been designed to mitigate the potential for these challenges.

739. Ref. 79 provides a description of how the EUH [CCGCS] has evolved with the development of the Chinese fleet of reactors. The RP describes how mobile PARs are included for design basis accidents in the M310, and how the necessity for severe accident dedicated PARs has evolved over time. The RP points out that the number of PARs required is dependent on the size of the reactor and the layout of the containment. Whilst the number of PARs in the UK HPR1000 (29) is lower than that of the CPR1000 and ACPR1000 (33), the RP claims that the containment is larger and therefore the overall hydrogen concentration by volume is generally lower.

740. The RP points out in Ref. 79 that the AP1000 design incorporates a different strategy incorporating ignitors to burn the hydrogen quickly. Akin to the UK HPR1000 design, the EPR incorporates only PARs and, whilst achieved in slightly different ways, has also designed its containment to promote mixing and circulation during severe accidents. Whilst both strategies may be valid, the RP points out that no power is required for the use of PARs, and that the effectiveness of the EUH [CCGCS] has been demonstrated using conservative assumptions.

741. Whilst not mentioned in the ALARP report (Ref. 79), the RP has stated in response to RQ-UKHPR1000-1325 (Ref. 81) that the UK HPR1000 design uses siliceous concrete for the basemat, which reduces the amount of carbon monoxide generated due to MCCI. Whilst the RP considers that MCCI is practically eliminated (due to its IVR strategy), I consider this to be an additional ALARP measure which further reduces risk of combustion and overpressure.

742. I am satisfied that these aspects demonstrate that the design of the EUH [CCGCS] and containment have reduced risk associated with combustible gases to ALARP.

4.10.5 Containment Overpressure – Containment Heat Removal System

743. Long term containment overpressure can occur if heat is not removed from the containment. The EHR [CHRS] is designed to remove sufficient heat to prevent overpressure.

744. Ref. 79 describes how the containment heat removal system has evolved through the Chinese fleet of reactors. The RP notes that for the M310 design and CPR1000 the containment spray was only designed to cope with design basis accidents. For ACPR1000 and UK HPR1000, a dedicated severe accident spray system was incorporated into the design. In addition, the RP states that the extra cooling chain (the ECS) has been incorporated into the UK HPR1000 as a post-Fukushima learning improvement.

745. Ref. 79 notes that two active trains of containment spray and heat removal, and a diverse cooling chain are also available in the EPR. The AP1000 applies passive heat removal. In my opinion, both approaches (active and passive) represent credible examples of RGP. The RP's approach is similar to the EPR and so in my opinion reflects RGP.

746. IAEA SSG-53 (Ref. 6) sets the expectation that the containment spray and nozzles be designed to optimise both retention of radionuclides and heat removal. In response to RQ-UKHPR1000-1597 (Ref. 81), the RP has provided justification of how the design has good coverage of the upper containment space (> 80%) and that the nozzle holes are greater than the maximum allowable size of debris in the EHR [CHRS]. The RP points out that the heat removal is the most important aspect of the EHR [CHRS] design. I agree with the RP's justification that the UK HPR1000 large and open containment design is beneficial for heat removal in severe accidents.

747. In my opinion, the UK HPR1000 provides comparable means of heat removal to other Generation-III reactors. Redundancy and an additional diverse heat sink is incorporated in the design and the deterministic analysis demonstrates the effectiveness of the EHR [CHRS] (even with a 12-hour grace time). However, a view of whether risks related to overpressure have been reduced ALARP also needs to consider the EUF [CFES], which is discussed in the following section.

4.10.6 Containment Overpressure – Containment Filtration and Exhaust System

748. The EUF [CFES] has been incorporated into the design in order to mitigate the risk of containment overpressure in sequences where the EHR [CHRS] has failed.

749. The Fukushima accident highlighted the importance of the ability to control containment pressure when all other ability to remove heat is lost. As previously stated, currently, there is no international consensus or expectation for the inclusion of a containment venting system. The inclusion is often dependent on country specific regulatory requirements or expectations (Ref. 108). ONR does not set an overarching expectation that a containment vent should be included in the design of new reactors, but sets the expectation that it is demonstrated that the risks are reduced to ALARP. On this basis, the inclusion of a vent in the design is assessed on a case by case basis.

750. In this section, I focus on whether inclusion of a containment vent reduces the relevant risks to ALARP.

751. Position 4 of 'WENRA Safety of New NPP designs' set the expectation that if a containment venting system is included in the design to reduce the containment pressure in a core melt accident, it shall have a filtering capability. The EUF [CFES] does include a filtered capability. The details of the filter, and the chemical effects on the progression of accidents when the filter is depleted have been assessed by ONR's Chemistry Inspector which has found that sufficient filtration capacity is available (Ref. 7).

752. The RP claims that the EUF [CFES] is included in the design of the UK HPR1000 to supplement defence in depth and would only be called upon if the EHR [CHRS] failed. The RP has demonstrated in Ref. 39 that the EUF [CFES] would only be required more than 60 hours after a LB-LOCA with failure of the EHR [CHRS].

753. Ref. 137 provides justification for inclusion of the EUF [CFES] in the UK HPR1000. The RP claims that as the UK HPR1000 is a design evolution of the CPR1000 and ACPR1000, which include a filtered vent. Moreover the reference design, FCG3, includes the EUF [CFES].

754. Ref. 137 presents an evaluation of the negative aspects of including the EUF [CFES] in the design. The main negative aspects are as follows:

- hydrogen combustion in the vent system;
- inadvertent operation;
- potential for negative pressures in the containment; and
- radiation exposure to operators during actuation.

755. The RP's main argument is that the inclusion of an EUF [CFES] is beneficial to severe accident management as it allows for a means of managing containment pressure and preventing uncontrolled releases through failure of the containment. Not including a EUF [CFES] could risk containment rupture and an uncontrolled release if the EHR [CHRS] failed. The RP has not provided an analysis of the hydrogen combustion in the vent system, but has made the argument that the analysis (Ref. 39) demonstrates that the EUF [CFES] is only required to operate after 60 hours. The RP argues that by this time, even if the conservative assumption is made that all the steam is condensed, the hydrogen is well mixed and the maximum concentration would be 1.5%. The RP therefore considers that the negative aspects are acceptable and that the benefits to nuclear safety outweigh any of the negative aspects.

756. In addition, the RP presents a summary of the Level 3 PSA in response to RQ-UKHPR1000-1695 (Ref. 81). The RP compares doses and conditional risk for both a severe accident with correct operation of the EUF [CFES] and with failure of the EUF [CFES] (and therefore rupture of the containment). The results show that whilst doses to the public would be significantly reduced by several orders of magnitude, the actual difference in risk is low. I judge that this is because the sequence frequency for the demand of the EUF [CFES] is approximately 3.5×10^{-9} per reactor year. However, the RP still concludes that the inclusion of the EUF [CFES] is supported by the Level 3 PSA.

757. The RP also presents an evaluation of benefits and disbenefits with regards to cost, technical maturity, and the environment. The RP concludes that the cost is low, that technical maturity is high, and the benefits to the environment and nuclear safety are clear.

758. Consistent with guidance provided in NS-TAST-GD-007 (Ref. 4), I consider that the design of the UK HPR1000 should be considered on its own merits and not be overly prejudiced by previous GDAs. I judge that the RP has made a clear case in favour of

the inclusion of the EUF [CFES] in the HPR1000 design, and that its inclusion reduces the relevant risks to ALARP.

4.10.7 Spent Fuel Pool

759. The RP claims that severe accidents in the SFP have been practically eliminated. This claim is based on the ability to monitor temperature and water level, redundant PTR [FPCTS] trains in stand-by, diversity in the cooling of the PTR [FPCTS] pumps, a diverse heat cooling chain, the emergency diesel generator and the SBO generator, back-up C&I, the robustness of the SFP, the relatively large grace times associated with SFP loss of cooling/coolant accidents and the F-SC2 gravity fed ASP [SPHRS] make-up water which can ensure fuel remains covered for five days.

760. In addition to the above, the RP has also identified several other water sources that could be used to make up the SFP. The RP claims that water from ECS, JAC [FWPS], CI Demineralised Water Distribution System (SER [DWDS (CI)], NI Demineralised Water Distribution System (SED [DWDS (NI)]) and Potable Water System (SEP [PWS (NI)]) could be transferred to the SFP through the emergency make-up line by mobile equipment.

761. ONR has no specific conditions for mission times for keeping fuel covered in the SFP until normal duty systems are restored, consumables can be restocked or a different system can provide longer term cooling. The capability of the ASP [SPHRS] to maintain coverage of the fuel for five days is a significant benefit to the UK HPR1000. Whilst the details are site specific, I judge that this is sufficient time to implement measures for longer term cooling. I therefore consider that the UK HPR1000 has met RGP in this area, and has reduced risks ALARP.

762. In ONR's report 'Japanese earthquake and tsunami: Implications for the UK Nuclear Industry Interim Report' (Ref. 11), the Chief Nuclear Inspector recommended that "The UK nuclear industry should ensure that the design of new spent fuel ponds close to reactors minimises the need for bottom penetrations and lines that are prone to siphoning faults. Any that are necessary should be as robust to faults as are the ponds themselves." The design of the UK HPR1000 eliminates all bottom penetrations and penetrations below the height of the spent fuel rack. Siphon breakers are included in trains A and B of the PTR [FPCTS]. In addition, train C of the PTR [FPCTS] is at a lower penetration to train's A and B such that if an unisolable break were to occur in either of these trains, train C, which is normally in stand-by, could be brought into service and still provide cooling. The UK HPR1000 has clearly incorporated the recommendation, and I consider that the design reduces risks ALARP.

763. In terms of monitoring the SFP water level, as stated previously (see sub-section 4.8), the RP claims that there are no reasonably practicable improvements that can be made (Ref. 81) to extending the range of the water level monitoring to below the fuel rack. I am satisfied with the RP's reasoning and consider the design reduces risks ALARP.

764. In the response to RQ-UKHPR1000-0622 (Ref. 81) the RP has also provided reasoning for not including PARs in the SFP building. The RP claims that in accidents leading to fuel uncovery, by the time hydrogen would be generated, the steam would fill the building and would reduce the potential for high energy combustion. Moreover, the RP claims that the mass of hydrogen generated would be such that it would not be practical to mitigate this using PARs. Most importantly, however, the RP claims that the radiological consequences from a severe accident alone mean that the sequences should be practically eliminated by preventing fuel uncovery. Therefore, arguments related to hydrogen management are less important. I note that no other PWRs considered in GDA have included PARs in the SFP building. I therefore consider the

RP's arguments to be reasonable and that not including PARs in the SFP reflects RGP.

765. I am satisfied that the RP has demonstrated that severe accidents in the SFP are practically eliminated. I am satisfied that the RP has identified a range of additional measures that would keep the fuel covered. In addition, I am satisfied that adequate monitoring capability is in place to enable situational awareness (pool temperature, pool level down to just below fuel rack level, radiation levels in fuel building). From a severe accidents point of view, I therefore judge that the RP has demonstrated that risks related to severe accidents in the SFP have been reduced to ALARP.

4.10.8 Grace Times

766. As stated previously, the RP has designed the UK HPR1000 with a set of requirements derived from the EURs (Ref. 106). These include requirements related to "autonomy", and prescribe lengths of times before certain actions should be required. Essentially, they result in grace times until permanent stocks deplete. These grace times relate to:

- Available time before off-site stocks (e.g. water and fuel oil) are required
- Available time before onsite mobile equipment is required
- Available time before operator actions are required

767. The UK HPR1000 is designed with these requirements in mind. In this section, I present my assessment of these aspects.

Time Available Prior to Requiring Off-site Support

768. The UK HPR1000 is designed to be resilient to loss of off-site power faults. The UK HPR1000 incorporates the EDGs and SBOs, and the fuel oil available onsite provides design basis power loads for over 10 days. Even after this point, mobile generators, the ASP [SPHRS], ECS and EHR [CHRS] are available to prevent escalation to a severe accident. In the case that a total loss of AC power occurs, the ASP [SPHRS] can be run by only using the UPS 24-hour battery, for 24 hours, until mobile generators are available. These aspects are out of scope of my assessment and are considered in the Fault Studies assessment (Ref. 10).

Time Available Prior to Requiring Onsite Non-Permanent Equipment

769. The EURs set the expectation that during a severe accident, no onsite mobile equipment should be credited within 12 hours of an initiating event leading to a severe accident.

770. A severe accident in the UK HPR1000 can be caused by a loss of offsite power, with the loss of the back-up AC power supplies. Because of this, the UK HPR1000 is designed to be able to cope with a severe accident without these AC power supplies, for an amount of time necessary until AC power is restored. In reality, even in a loss of AC power event, the ASP [SPHRS] is battery powered, and would prevent escalation to a severe accident whilst the battery power was still available. In consideration of independence of the levels of defence in depth, however, the ASP [SPHRS] is not credited in designing severe accidents safety features, and is assumed to be lost at the same time that AC power is lost.

771. The RP claims that for severe accidents, there is a 12-hour grace time in the design before AC power is required. This assertion assumes that AC power supplies would not be lost during faster acting severe accidents, such as the LB-LOCA. As stated sub-section 4.8, I consider this assumption to be appropriate, as a total loss of AC power supply (LOOP, EDG failure, SBO failure) in coincidence with an independent LB-LOCA has an extremely low sequence frequency. Moreover, even in this scenario, there is

approximately 11 hours grace time until an AC power supply is required for active reactor pit injection.

772. As discussed in sub-section 4.8, the RP has extended the duration of the UPS [LAP/LAQ] power supplies from 12 to 24 hours during GDA. The batteries supply power for lighting, monitoring (via the KDA [SA I&C] and parts of the SAS) and control of valves. This means that situational awareness is significantly improved in the event that AC power is not restored within 12 hours. This improvement is aligned with post-Fukushima learning, and I, along with the Electrical Engineering inspector (Ref. 123), consider this to be an ALARP improvement which aligns with RGP.

773. In my opinion, the amount of grace time available until AC power (either through restoration of the EDGs, SBO, or mobile generators) is comparable to other Generation-III plants with active heat removal for severe accidents (e.g. the EPR) and is in broad agreement with the EURs (Ref. 106). Moreover, the ASP [SPHRS] is a beneficial feature of the UK HPR1000, which has the ability to remove heat for several days if the control and monitoring is available, which would prevent a severe accident (Ref. 10).

774. The deterministic analysis related to the SADVs, IVR, EUH [CCGCS] and EHR [CHRS] support the RP's assertion that the severe accident mitigation can be performed without the need for mobile equipment for 12 hours (or restoration of EDGs or SBO generators). The EUF [CFES] is an exception to this rule, but as stated previously, this analysis is based on the LB-LOCA with the assumption that the EHR [CHRS] has failed and this is a very low frequency sequence.

Grace Times Related to Operator Actions

775. My assessment has considered the amount of time available for operators to complete actions.

776. For the SADV, EHR [CHRS] and EUF [CFES], the grace times are very long (several hours), and together with ONR's PSA and Human Factors inspectors I consider these times reasonable (Refs 37 to 39). The grace times for EUH [CCGCS] are not relevant, as the PARs start passively and automatically.

777. The shortest grace time, however, is associated with the initiation of passive reactor pit flooding during a LB-LOCA without LHSI and MHSI. Initiation is required within the first 40 minutes of the accident in order to ensure that the reactor pit is filled prior to corium relocation to the RPV lower head. As discussed previously, to facilitate this the RP has made design modifications so that the actions for opening IVR valves can be performed in the MCR only (see design modification, M63 (Ref. 93)). Whilst the timescales appear short, I judge that the LB-LOCA with failure of the MHSI and LHSI is an extremely unlikely sequence, and the confirmatory analysis shows that the requirement for filling the reactor pit prior to relocation is conservative. With this in mind, the operator is likely to have comparable times to design basis accidents to determine a course of action. Moreover, in comparison to other severe accident scenarios, it should be relatively simple to diagnose and determine the course of action for an accident similar to a LB-LOCA severe accident. The design modification removes significant delays in the implementation of IVR. I therefore consider that the design modification has reduced risks of failure to implement IVR to ALARP.

Conclusions Related to Grace Times

778. To summarise, the RP has demonstrated that the autonomy times of the UK HPR1000 are at least comparable to other reactor designs with active heat removal and in broad agreement with the EURs (Ref. 106). Moreover, the ASP [SPHRS] offers a benefit to

the capacity of heat removal for high pressure severe accidents. The RP has also demonstrated that whilst most grace times are long, short grace times associated with IVR actuation may be challenging. However, the RP has made design modifications during GDA to remove actions that cause significant delays and, in my opinion, has reduced risks associated with the IVR strategy to ALARP.

4.10.9 General Approach to ALARP

779. The RP's approach to ALARP, in aspects related to the Severe Accident Analysis topic area, is to demonstrate that the severe accident safety features are effective, even when using worst case assumptions, in mitigating the DEC-B scenarios that it has identified.

780. The RP has not provided ALARP justification for every aspect of its safety case, particularly where the design of the UK HPR100 clearly meets RGP. Instead, it has chosen specific aspects where the available RGP is less well defined in order to justify its design choices. I consider this approach to be reasonable, and aligns well with the expectations of NS-TAST-GD-005 (Ref. 4).

781. In cases where the RP has developed specific ALARP arguments, the RP has performed optioneering in varying levels of detail, ranging from high level conceptual optioneering (such as the case with the SFP monitoring) to more detailed design solutions (such as the case for the design modification related to the upgrade of the UPS from 12 to 24 hours). I consider that the RP's approach has been appropriately graded based on the associated risk and complexity of the topic in question.

782. In general, I consider that the RP's approach to demonstrating ALARP in the Severe Accidents Topic area is aligned with the expectations of NS-TAST-GD-005 (Ref. 4).

4.10.10 Strengths

783. The RP has submitted a dedicated report to demonstrate that risks have been reduced ALARP. The structure of the report is aligned with the expectations for demonstration of ALARP in GDA described in NS-TAST-GD-005.

784. Aligned with NS-TAST-GD-005, the RP has demonstrated that RGP is met and that no further improvements related to severe accident mitigation are reasonably practicable.

785. The RP has demonstrated that the SFP design meets RGP and the relevant risks have been reduced ALARP. Moreover, the RP has provided an adequate demonstration that severe accidents in the SFP have been practically eliminated in the design, which meets the expectation of SSG-2.

786. In addition, specific design modifications have been made which in my opinion reduce risks ALARP.

4.10.11 Outcomes

787. No Assessment Findings or minor shortfalls have been raised in this section.

4.10.12 Conclusion

788. For the purpose of GDA, the RP has demonstrated the design of the UK HPR1000 is adequately designed to mitigated severe accidents in the reactor, and to prevent severe accidents in the and meets RGP.

789. I consider that for the purposes of GDA the risks associated with severe accidents in the UK HPR1000 have been shown to be ALARP.

4.11 Consolidated Safety Case (Chapter 13)

790. My assessment is based on PCSR Version 1 (Ref. 3) and information exchanged in RQ and RO responses. In line with ONR's guidance to requesting parties (Ref. 1), the RP has since performed a review of its responses and updated the safety case documentation as necessary to include the relevant information.

791. In this section I present my assessment of whether the RP has consolidated RQ responses relevant to my assessment within PCSR Version 2 (Ref. 138). In doing so, I present my assessment of the PCSR Chapter 13 Version 2 as a whole against the expectations of NS-TAST-GD-051 (Ref. 4), SAP SC.4 (Ref. 2) and NS-TAST-GD-007 (Ref. 4).

4.11.1 Assessment

792. In Step 2 of GDA, I considered that the safety case fell short of the general expectations set out in NS-TAST-GD-051 and the specific expectations set out in FA.15, FA.16 and NS-TAST-GD-007 (Rev. 4). In general terms, I did not consider that there was a coherent safety case from identifying safety functions through to demonstrating the effectiveness of UK HPR1000 severe accidents safety features. I therefore raised RO-UKHPR1000-0003 (Ref. 100) which included actions related to providing a strategy and methodology for building a Severe Accident Analysis safety case.

793. Rather than relying of Version 2 of the PCSR to close out the RO, the RP provided Ref. 28, PCSR Version 1 and a review of Version 1 against ONR's expectations set out in NS-TAST-GD-051 (Ref. 139). The RP categorised what it considered shortfalls against the different themes of "overall qualities of a safety case" presented in NS-TAST-GD-051 and provided examples of how the safety case would be improved for Version 2. Based on several interactions and feedback from ONR, the RP's review (Ref. 139) found that:

- There was a consistent lack of context and cross-referencing to other parts of the safety case. In isolation, it was therefore difficult to understand what arguments the safety case was making.
- Referencing to background information from the international severe accidents community, or to previous learning from the RP, was limited and the safety case often assumed knowledge. This made the safety case less accessible to the reader.
- The PCSR contained several examples of outdated information that should be reviewed for PCSR Version 2.
- Parts of the safety case were incomplete. For example, the safety case for severe accidents during shutdown and refuelling, and the supporting arguments for practical elimination of severe accidents in the SFP, were not included.
- The safety case was not detailed enough and in some cases limited evidence had been provided to support arguments made.

794. Based on several examples provided in Ref. 139 and Version 1 of PCSR Chapter 13, I considered it appropriate to close RO-UKHPR1000-0003 (Ref. 140). I judge that the improvements identified in Ref. 108 have been made in Version 2 of the PCSR and that it is broadly aligned with the expectations of NS-TAST-GD-051 (Ref. 4) and SAP SC.4 (Ref. 2).

795. In addition, throughout GDA, the RP has continuously provided updates to relevant supporting documents. The RP has summarised these commitments in Ref. 23. In addition, I have sampled the RQs and found that only one commitment made was

omitted from the list provided in Ref. 23. I have sampled the majority of the 44 commitments made in RQ responses to update documentation and found that the safety case has been updated satisfactorily.

796. Moreover, for Severe Accident Analysis, the RP has performed a second review of all RQ responses (including those without commitments), information exchanged as part of confirmatory analysis, meeting records and actions, emails and design modifications to ensure that the appropriate information is captured in the safety case. I have sampled several RQs and found that the RP has indeed updated the relevant information in the safety case. For example, in response to RQ-UKHPR1000-0545 (Ref. 81), the RP did not make a commitment to include comparisons of the ASTEC and GASFLOW-MPI calculations. However, following a review, the RP has now updated the relevant documentation to include this evidence.

797. Overall, therefore, I am content that the RP has satisfactorily consolidated relevant information from GDA into the final PCSR and supporting references. These final revisions are consistent with my assessment in Section 4.

4.11.2 Strengths

798. Through RO-UKHPR1000-0003 (Ref. 100) the RP has improved its severe accidents analysis safety case. I consider that Version 2 of the PCSR broadly satisfies the expectations of SAP SC.4 (Ref. 2), NS-TAST-GD-051 and NS-TAST-GD-007 (Ref. 4).

799. The RP has performed a comprehensive review of all information exchanged during GDA and has updated the PCSR where appropriate.

4.11.3 Outcomes

800. I have identified no minor shortfalls or assessment findings.

4.11.4 Conclusion

801. I am satisfied that PCSR Chapter 13 Version 2 broadly meets the expectations of SC.4, NS-TAST-GD-051 and NS-TAST-GD-007.

802. I am content that the RP has satisfactorily consolidated relevant information from GDA into the final PCSR and supporting references. These final revisions are consistent with my assessment in Section 4.

4.12 Comparison with Standards, Guidance and Relevant Good Practice

803. In Section 2, I have identified the most relevant standards, guidance and other RGP. Throughout my assessment report I have described how I have applied these in my assessment. This section provides a summary of how the design of the UK HPR1000 and the safety case has met the key expectations.

804. The most relevant SAPs for my assessment are:

- Severe accidents: FA.1, FA.15, FA.16, FA.25 - The RP has performed severe accident analysis to demonstrate that the phenomena arising from severe accident scenarios are mitigated. The analysis has been performed on a best estimate basis, forms a basis for severe accident management, and serves as an input to the Level 2/3 PSAs.
- Computer codes and calculation methods: AV.1, AV.2, AV.3, AV.5 and AV.6 – The RP has provided adequate verification and validation documentation for the ASTEC, GASFLOW-MPI, MOPOL and MC3D codes which I chose to

sample. In addition, the RP has provided adequate sensitivity analyses to cover the areas of greatest uncertainty.

- Planning and preparedness: AM.1 – the RP has demonstrated that the most important plant parameters will be monitored during a severe accident, and the UK HPR1000 design enables accident management
- Numerical Targets: NT.1 – The RP has used ONR's Targets 7, 8 and 9 to support arguments related to practical elimination.

805. The most relevant TAGs applied in my assessment are:

- ONR-TAST-GD-007 - Severe Accident Analysis – The RP has identified severe accident phenomena, severe accident management strategies, analysed severe accident scenarios and demonstrated that the severe accident management strategies are effective.
- ONR-TAST-GD-042 - Validation of Computer Codes and Calculation Methods – In particular, I have applied the expectations for what should be included in verification and validation documentation and sensitivity analyses.
- ONR-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components – The RP has derived safety functions and categorised them appropriately. The RP has assigned the classification of the safety features appropriately.
- NS-TAST-GD-005 - ONR Guidance on the Demonstration of ALARP – For the purposes of GDA, the RP has provided adequate demonstration that the risks associated with the UK HPR1000, from a Severe Accident Analysis point of view, have been reduced ALARP.

806. The most relevant international standards and guidance are as follows:

- IAEA SSR-2/1 - Safety of Nuclear Power Plants: Design – The UK HPR1000 has been designed to cope with design extension conditions and the RP has demonstrated that early or large releases have been practically eliminated.
- IAEA SSG-2 - Deterministic Safety Analysis for Nuclear Power Plants – The RP's methodologies are aligned with the expectations of SSG-2. The RP has demonstrated that the UK HPR1000 design can mitigate phenomena that arise from severe accidents and bring the plant to a controlled stated.
- WENRA - Statement on Safety Objectives for New Nuclear Power Plants – The RP has performed analysis of design extension conditions and has demonstrated that early or large early or large releases are practically eliminated. For the purposes of GDA, the RP has demonstrated that there is adequate independence between the levels of defence in depth.
- WENRA - Safety of New NPP Designs – The RP has performed analysis of design extension conditions and demonstrated adequate independence of the levels of defence in depth.
- WENRA - Practical Elimination Applied to New NPP Designs – Key Elements and Expectations – The RP has demonstrated that scenarios that have the potential to lead to an early or large release are practically eliminated. The methodology to demonstrate this is aligned with WENRA expectations. In particular, the RP has provided a demonstration that early or large releases caused by accidents described in this guidance (referred to as Type I, II and III) have been practically eliminated in the UK HPR1000 design.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

807. This report presents the findings of my Severe Accident Analysis assessment of the generic UK HPR1000 design as part of the GDA process.

808. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- The RP has adequately identified severe accidents phenomena, severe accident scenarios and safety features used for severe accident management.
- The RP has demonstrated that the UK HPR1000 safety features for severe accident management are effective through deterministic analysis and has provided appropriate verification and validation evidence for the codes used.
- The RP has demonstrated that appropriate engineering requirements have been derived and assigned to structures, systems and components claimed for severe accident management.
- The RP has demonstrated that the UK HPR1000 supporting systems are adequate to support the safety features for severe accident management.
- The RP has demonstrated that early or large releases have been practically eliminated in the UK HPR1000 design.
- The RP's approach is aligned with both ONR and international expectations for severe accident analysis.
- For the purposes of GDA, the RP has demonstrated that the design of the UK HPR1000 has reduced the relevant risks to ALARP.
- Four Assessment Findings have been identified which should be resolved by the future Licensee.

809. 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 Severe Accident Analysis perspective.

5.2 Recommendations

810. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From a Severe Accident Analysis perspective, ONR should grant a DAC for the generic UK HPR1000 design.

- **Recommendation 2**: The four 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

2. *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 1, January 2020, ONR, http://www.onr.org.uk/saps/saps2014.pdf

3. *Pre-Construction Safety Report: Chapter 13: Design Extension Conditions and Severe Accident Analysis*, HPR/GDA/PCSR/0013, Rev. 001, 10 January 2021, GNSL, CM9 Ref. 2020/13935

4. Technical Assessment Guides

   Guidance on Mechanics of Assessment, NS-TAST-GD-096, Revision 0, April 2020

   Severe Accident Analysis, NS-TAST-GD-007, Revision 4, September 2017

   Guidance on the Demonstration of ALARP, NS-TAST-GD-005, Revision 11, November 2020

   The Purpose, Scope, and Content of Safety Cases, NS-TAST-GD-051, Revision 7, December 2019

   Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094, Revision 2, July 2021

   Validation of Computer Codes and Calculation Methods, NS-TAST-GD-042, Revision 5, March 2019

   http://www.onr.org.uk/operational/tech_asst_guides/index.htm

5. *GDA Step 4 Assessment Plan of Severe Accident Analysis topic for the UK HPR1000 Reactor*, ONR-GDA-UKHPR1000-AP-19-009, Revision 0, February 2020, ONR, CM9 Ref. 2020/33804

6. *International* Atomic Energy Agency Standards, Guidance and Reports

   Safety Assessment for Facilities and Activities. Safety Standards Series, No. GSR Part 4;

   Safety of Nuclear Power Plants: Design, Specific Safety Requirements, No. SSR 2/1. Rev. 1, February 2016

   Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide, No SSG-2. Rev. 1. 2019,

   Design of Reactor Containment Systems for Nuclear Power Plants. Specific Safety Guide, No. SSG-53, Rev 1, 2019

   Accident Management Programmes for Nuclear Power Plants, Specific Safety Guide, No. SSG-54, 2019

   Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants, Safety Reports Series, No. 56, 2008

   Consideration of the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, Rev. 0, 2016

   IAEA, Mitigation of Hydrogen Hazards in Severe Accidents in Nuclear Power Plants, IAEA-TECDOC-1661, 2011.

   www.iaea.org

7. *Step 4 Chemistry Assessment Report*, ONR-NR-AR-21-002, Rev 0, January 2022, ONR, CM9 Ref. 2021/41488

8. *UK HPR1000 Step 4 Civil Engineering Assessment Report*, ONR-NR-AR-21-018, Rev 0, January 2022, ONR, CM9 Ref. 2021/57205

9. *UK HPR1000 Step 4 PSA Assessment Report*, ONR-NR-AR-21-020, Rev 0, January 2022, ONR, CM9 Ref. 2021/49362

10. *UK HPR1000 Step 4 Fault Studies Assessment Report*, ONR-NR-AR-21-014, Rev 0, January 2022, ONR, CM9 Ref. 2021/44803

11. *Japanese earthquake and tsunami: Implications for the UK nuclear industry*, September 2011, ONR

12. Western European Nuclear Regulators' Association Reports

    WENRA statement on safety objectives for new nuclear power plant, Reactor Harmonization Working Group, November 2010

    Report on Safety of new NPP designs, Reactor Harmonization Working Group, 2013

    WENRA Reactor Reference Safety Levels, Reactor Harmonization Working Group, September 2014

    Safety of new NPP designs, Reactor Harmonization Working Group, March 2013

    Practical Elimination Applied to New NPP Designs: Key Elements and Expectations, Reactor Harmonization Working Group, September 2019

    www.wenra.eu

13. *COCOSYS Model for UK HPR1000*, Rev 1, June 2021, GRS, CM9 Ref. 2021/51182

14. *ATHLET CD Model for UK HPR1000*, Rev 1, June 2021, GRS, CM9 Ref. 2021/51181

15. *Confirmatory Analyses IVR Strategy for UK HPR1000*, Rev 1, June 2021, GRS, CM9 Ref. 2021/51184

16. *Phase 1: ASTEC Code Review for the UK HPR1000 Safety Case on behalf of ONR*, ONRTSF/4NT/0685035/000/01, February 2020, Tractebel, CM9 Ref. 2020/97056

17. *Phase 1: MOPOL Code Review for the UK HPR1000 Safety Case on behalf of ONR*, ONRTSF/4NT/0685038/000/02, June 2020, Tractebel, CM9 Ref. 2020/270473

18. *Phase 1: MC3D Code Review for the UK HPR1000 Safety Case on behalf of ONR*, ONRTSF/4NT/0685037/000/02, June 2020, Tractebel, CM9 Ref. 2020/270469

19. *Phase 1: GASFLOW Code Review for the UK HPR1000 Safety Case on behalf of ONR*, ONRTSF/4NT/0685036/000/02, June 2020, Tractebel, CM9 Ref. 2020/270467

20. *Phase 2: ASTEC Code Review for the UK HPR1000 Safety Case on behalf of ONR*, ONRTSF4NT073596000000, January 2021, Tractebel , CM9 Ref. 2021/11406

21. *Phase 2: GASFLOW-MPI Detailed Code Review for the UK HPR1000 Safety Case on behalf of ONR*, ONRTSF/4NT/0742960/000/01, March 2021, Tractebel, CM9 Ref. 2021/26112

22. HPR1000 Multi-National Design Evaluation Programme Working Group

    Hydrogen Control During Severe Accidents, TR-HPR1000WG-01, 2020

    Technical Report on Regulatory Requirements and Practices for Severe Accidents, TR-HPR1000WG-02, 2020

    Common Position Addressing Fukushima Daiichi NPP Accident-Related Issues, CP-HPR1000WG-01, 2020

https://www.oecd-nea.org/mdep/working-groups/hpr1000wg.html

23. *Production Strategy for Severe Accident Analysis,* GHX00100026KPGB03GN, Rev F, 28 April 2021, CGN, CM9 Ref. 2021/35423

24. *Internal Events Level 1 PSA*, GHX00650001DOZJ02GN, CGN, Rev B, April 2020, CM9 Ref. 2020/112233

25. *Methodology to Identify Severe Accident Sequences for UK HPR1000*, GHX00600137DRAF02TR, CGN, Rev. B, April 2018, CM9 Ref. 2018/112556

26. *Selection of Severe Accident Scenarios*, GHX00600058DRDG03GN, Rev E, June 2020, CGN, CM9 Ref. 2020/195856

27. *Overall Methodology of Severe Accident Analysis*, GHX00600007DRAF02GN, Rev B, November 2018, CGN, CM9 Ref. 2018/367425

28. *Topic Report on the Severe Accident Analysis of a Typical Sequence,* GHX00600255DRAF02GN, Rev B, 29 November 2019, CGN, CM9 Ref. 2019/359714

29. *Functional Requirements of Severe Accident I&C,* GHX00600324DRAF02GN, Rev B, November 2020, CGN, CM9 Ref. 2020/309793

30. *Safety Functional Requirements of IVR,* GHX000600327DRAF02GN, Rev B, November 2020, CGN, CM9 Ref. 2020/309792

31. *Safety Functional Requirements of Containment Combustible Gas Control System*, GHX00600326DRAF02GN, Rev A, May 2020, CGN, CM9 Ref. 2020/130916

32. *Safety Functional Requirements of Severe Accident Dedicated Valve [SADV],* GHX00600325DRAF02GN, Rev A, 28 March 2020, CGN, CM9 Ref. 2020/98072

33. *Safety Functional Requirements of EHR [CHRS]*, GHX00600328DRAF02GN, Rev A, 04 May 2020, CGN, CM9 Ref. 2020/130928

34. *Safety Functional Requirements of EUF [CFES]*, GHX00600329DRAF02GN, Rev A, 28 March 2020, CGN, CM9 Ref. 2020/98077

35. *Assessment of In-Vessel Retention Strategy*, GHX00600113DRAF02GN, Rev E, 15 December 2020, CGN, CM9 Ref. 2020/321351

36. *Assessment of Containment Combustible Gas Control System by Lumped Parameter Method*, GHX00600103DRAF02GN, Rev E, 27 November 2020, CGN, CM9 Ref. 2020/314645

37. *Depressurisation Capacity Analysis of Severe Accident Dedicated Valve*, GHX00600055DRAF02GN, Rev D, 3 December 2020, CGN, CM9 Ref. 2021/99

38. *Assessment of EHR [CHRS]*, GHX00600063DRAF02GN, Rev D, 3 October 2019- CM9 Ref. 2019/285719

39. *Assessment of EUF [CFES]*, GHX00600065DRAF02GN, Rev D, 3 October 2019, CGN, CM9 Ref. 2019/285731

40. *Applicability Assessment on Severe Accident Analysis Codes Used for UK HPR1000,* GHX00600257DRAF02GN, Rev B, 28 March 2020 – CM9 Ref. 2020/98068

41. *ASTEC V2.1 Final Validation Report*, *Volume 1*, IRSN2020-00437, 2020, IRSN, CM9 Ref. 2020/200194

42. *ASTEC V2.1 Final Validation Report, Volume II (Appendices)*, IRSN2020-00437, 2020, IRSN, CM9 Ref. 2020/200226

43. *GASFLOW-MPI : A Scalable Computational Fluid Dynamics Code for Gases, Aerosols and Combustion, Volume 3: Verification and Validation,* 10.5445/KSP/1000050393, Revision 1.0, KIT, J. Xiao et al, 2016, CM9 Ref. 2019/282524

44. *Version 3.5 of the Software MC3D Validation Report,* NT/DSR/SAGR/05-89, 2005, IRSN, CM9 Ref. 2019/31747

45. *Development and Verification Report of MOPOL,* GHX00600001DRAF03GN, Rev B, 30 July 2021, CGN, CM9 Ref. 2021/58684

46. *Sensitivity Studies on Key Parameters of IVR Analysis*, GHX00600303DRAF02GN, Rev A, 29 June 2020. CM9 Ref. 2020/195854

47. *Sensitivity studies on key parameters of hydrogen risk assessment*, GHX00600304DRAF02GN, Rev C, 31 January 2021 – CM9 Ref. 2021/8908

48. *EHR Containment Heat Removal System Design Manual Chapter 2 Brief Introduction to the System,* GHX17EHR002DNHX45GN, Rev A, 2 October 2018, CGN, CM9 Ref. 2018/318485

49. *EHR Containment Heat Removal System Design Manual, Chapter 3 System Functions & Design Bases,* GHX17EHR003DNHX45GN, Rev A, 2 October 2018, CGN, CM9 Ref. 2018/318484

50. *EHR Containment Heat Removal System Design Manual, Chapter 4 System & Component Design,* GHX17EHR004DNHX45GN, Rev A, 2 October 2018, CGN, CM9 Ref. 2018/318482

51. *EHR Containment Heat Removal System Design Manual, Chapter 5 Layout Requirements & Environment Condition,* GHX17EHR005DNHX45GN, Rev A, 2 October 2018, CGN, CM9 Ref. 2018/318481

52. *EHR Containment Heat Removal System Design Manual, Chapter 6 System Operation & Maintenance* B, 2 October 2018, CGN, CM9 Ref. 2018/318480

53. GHX17EHR009DNHX45GN, *EHR Containment Heat Removal System Design Manual, Chapter 9 Flow Diagrams,* GHX17EHR006DNHX45GN, Rev B, 2 October 2018, CGN, CM9 Ref. 2018/318479

54. *EUH-Containment Combustible Gas Control System Design Manual Chapter 2 Brief Introduction to the System*, GHX17EUH002DNHX45GN, Rev A, 1 October 2018, CGN, CM9 Ref. 2018/318525

55. *EUH-Containment Combustible Gas Control System Design Manual Chapter 3 System Functions and Design Bases*, GHX17EUH003DNHX45GN, Rev A, 1 October 2018, CGN, CM9 Ref. 2018/318522

56. *EUH-Containment Combustible Gas Control System Design Manual Chapter 4 System and Component Design*, GHX17EUH004DNHX45GN, Rev A, October 2018, CGN, CM9 Ref. 2018/318519

57. *EUH-Containment Combustible Gas Control System Design Manual Chapter 5 Layout Requirements and Environment Condition*, GHX17EUH005DNHX45GN, Rev A, October 2018, CGN, CM9 Ref. 2018/318518

58. *EUH-Containment Combustible Gas Control System Design Manual Chapter 6 System Operation and Maintenance*, GHX17EUH006DNHX45GN, Rev A, 1 October 2018, CGN, CM9 Ref. 2018/318516

59. *RCP [RCS] Design Manual, Chapter 2 Brief Introduction to the System,* GHX17RCP002DNHX45GN, Rev A, 09 November 2018, CGN, CM9 Ref. 2018/369176

60. *RCP [RCS] System Design Manual Chapter 3 System Functions and Design Bases,* GHX17RCP003DNHX45GN, Rev B, December 2019, CGN, CM9 Ref. 2019/372785

61. *RCP [RCS] System Design Manual Chapter 4 System and Component Design,* GHX17RCP004DNHX45GN, Rev C, December 2019, CGN, CM9 Ref. 2019/372789

62. *RCP [RCS] Design Manual Chapter 5 Layout Requirements and Environment Condition*, GHX17RCP005DNHX45GN, Rev C, December 2019, CGN, CM9 Ref. 2019/373158

63. *RCP [RCS] System Design Manual Chapter 6 System Operation and Maintenance*, GHX17RCP006DNHX45GN, Rev D, December 2019, CGN, CM9 Ref. 2019/373164

64. *RCP [RCS] System Design Manual Chapter 9 Flow Diagrams*, GHX17RCP009DNHX45GN, Rev D, December 2019, CGN, CM9 Ref. 2019/375630

65. *EUF-Containment Filtration and Exhaust System Design Manual Chapter 2 Brief Introduction to the System*, GHX17EUF002DNHX45GN, October 2018, CGN, CM9 Ref. 2018/318513

66. *EUF-Containment Filtration and Exhaust System Design Manual Chapter 3 System Function and Design Bases*, GHX17EUF003DNHX45GN, 1 October 2018, CGN, CM9 Ref. 2018/318512

67. *EUF-Containment Filtration and Exhaust System Design Manual Chapter 4 System and Component Design*, GHX17EUF004DNHX45GN, 1 October 2018, CGN, CM9 Ref. 2018/318510

68. *EUF-Containment Filtration and Exhaust System Design Manual Chapter 5 Layout Requirements and Environment Condition,* 1 October 2018, CGN, CM9 Ref. 2018/318509

69. GHX17EUF006DNHX45GN, *EUF-Containment Filtration and Exhaust System Design Manual Chapter 6 System Operation and Maintenance*, GHX17EUF005DNHX45GN, October 2018, CGN, CM9 Ref. 2018/318507

70. *KDA [SA I&C] Severe Accident I&C System Design Manual Chapter 2 Brief Introduction to the System*, GHX17KDA002DIYK45GN, Rev C, 30 March 2021, CGN, CM9 Ref. 2021/27282

71. *KDA [SA I&C] Severe Accident I&C System Design Manual Chapter 3 System Functions and Design Bases,* GHX17KDA003DIYK45GN, Rev D, 25 March 2021, CGN, CM9 Ref. 2021/26035

72. *KDA [SA I&C] Severe Accident I&C System Design Manual Chapter 4 System and Component Design,* GHX17KDA004DIYK45GN, Rev D, 30 March 2021, CGN, CM9 Ref. 2021/27287

73. KDA [SA I&C] *Severe Accident I&C System Design Manual Chapter 5 Layout Requirements and Environment Condition*, GHX17KDA005DIYK45GN, Rev E, March 2021, CGN, CM9 Ref. 2021/26042

74. *KDA [SA I&C] Severe Accident I&C System Design Manual Chapter 6 System Operation and Maintenance,* GHX17KDA006DIYK45GN, Rev C, March 2021, CGN, CM9 Ref. 2021/26039

75. *KDA [SA I&C] Severe Accident I&C System Design Manual Chapter 9 Flow Diagrams,* GHX17KDA009DIYK45GN, Rev D, March 2021, CGN, CM9 Ref. 2021/26033

76. *Severe Accident Source Terms Analysis,* GHX00600258DRAF02GN, Rev D, 29 November 2019, GCN, CM9 Ref. 2019/359722

77. *Level 3 PSA Report*, GHX00650002DOHB02GN, Rev A, 29 January 2021, CGN, CM9 Ref. 2021/8460

78. *Practically Eliminated Situations*, GHX00600127DRAF02GN, Rev G, July 2021, CGN, CM9 Ref. 2021/51728

79. *ALARP Demonstration Report for Severe Accident Analysis*, GHX00100056KPGB03GN, Rev D, January 2021, CGN, CM9 Ref. 2021/8505

80. *Nuclear Safety In Light Water Reactors, Severe Accident Phenomenology,* ISBN: 978-0-12-388446-6, 2012, Bel Raj Sehgal

81. *UK HPR1000 – Regulatory Query (RQ) Tracking Sheet*. ONR. CM9 Ref. 2017/407871

82. *SERG: A Reassessment of the Potential for an Alpha-Mode Containment Failure and a Review of the Current Understanding of Broader Fuel-Coolant Interaction Issues*, NUREG-1524, 1995, NRC

83. *SERENA Project Report: Summary and Conclusions,* NEA/CSNI/R(2014)15, February 2015, OECD

84. *Lower Head Integrity Under Steam Explosion Loads*, Nuclear Engineering and Design, 189, 7–57, 1999, T. G. Theofanous, *et* al.

85. *Assessment of Re-criticality*, GHX00600330DRAF02GN, Rev B, 18 December 2020 CM9 Ref. 2020/322709

86. *Severe Accident Engineered Measures Summary Report*, GHX00600256DRAF02GN, Rev A, 3 October 2019, CGN, CM9 Ref. 2019/285687

87. *KDA [SA I&C] System Requirements Specification*, GHX06002012DIYK03GN, Rev D, 25 March 2021, CGN, CM9 Ref. 2021/26037

88. *Design Specification of Severe Accident I&C System (KDA [SA I&C])*, GHX56100028GSNS44TR, Rev D, 30 March 2021, CGN, CM9 Ref. 2021/27285

89. *UK HPR1000 Step 4 Cross Cutting Assessment Report,* ONR-NR-AR-21-007, Rev 0, January 2022, ONR, CM9 Ref. 2021/47905

90. *Assessment of EUH [CCGCS] by CFD method*, GHX00600298DRAF02GN, Rev E, 22 January 2021, CGN, CM9 Ref. 2021/6697

91. *Ex-vessel Steam Explosion Analysis*, GHX00600331DRAF02GN, Rev A, 26 August 2020, CGN, CM9 Ref. 2020/256894

92. *Summary Report on RPV Lower Head CHF Experiment*, GHX00600001CRNS02GN, Rev B, 30 September 2020, CM9 Ref. 2020/290060

93. *The Delivery of UK HPR1000 GDA Design Modification-Cat2 "Modification for Operation Time Problem of IVR (M63-GHTCN000178-A)"*, HPR-GDA-LETT-0079, November 2020, GNSL, CM9 Ref. 2020/306204

94. *In-Vessel Coolability and Retention of a Core Melt Report*, Vol 1, DOE/ID-10460, 1996, Theofanous, T.G., et al.

95. *Chemistry for the Step 4 GDA of UK HPR1000: Part 1: Severe Accidents, In-Vessel Retention and Hydrogen Control*, March 2021, NNL, CM9 Ref. 2021/29076

96. *The Structural Integrity Assessment of RPV on In-Vessel Retention Condition,* GHX00100014DPLX44GN, Rev B, October 2020, CGN, CM9 Ref. 2020/303742

97. *The Thermal Shock Analysis of RPV While Inadvertent Flooding of Reactor Pit Condition*, GHX00100041DPLX44GN, Rev A, 15 July 2020, CGN, CM9 Ref. 2020/214799

98. *UK HPR1000 Step 4 Structural Integrity Assessment Report,* ONR-NR-AR-21-016, Rev. 0, January 2022, ONR, CM9 Ref. 2021/52300

99. *The Thermal Shock Analysis of RPV While Triggering IVR Condition*, GHX00100011DPLX44GN, Rev B, 29 April 2020, CGN, CM9 Ref. 2020/128280

100. *UK HPR1000 Regulatory Observation (RO) Tracking Sheet*. ONR. CM9 Ref. 2019/465031

101. *The Radiation (Emergency Preparedness and Public Information) Regulations 2019 Approved Code of Practice and Guidance*, ISBN 978 0 7176 6728 4, Second Edition, 2020, ONR

102. *Internal Events Level 2 PSA*, GHX00650002DOZJ02GN, Rev A, November 2018, CGN, CM9 Ref. 2018/378858

103. *DBC Hydrogen Generation and Control*, GHX00600282DRAF02GN, Rev B, 28 June 2019, CM9 Ref. 2019/185232

104. *State of the Art Report on Flame Acceleration and Deflagration-to-Detonation Transition in Nuclear Safety,* August 2000, OECD

105. *Reinforced Concrete Barrier Substantiation Report for BRX*, GHXREX10005DWJG42GN, Rev B, November 2020, CM9 Ref. 2020/309727

106. *European Utility Requirements*, *Volume 2,* Revision D, December 2016

107. *General Safety Requirements*, GHX00100017DOZJ03GN, Rev F, 9 December 2019 – CM9 Ref. 2019/367630

108. *Status Report on Filtered Containment Venting,* NEA/CSNI/R(2014)7, July 2014, OECD

109. *Post-accident Accessibility Analysis Topic Report*, GHX00100017DNFP03GN, Rev G, July 2021, CGN, CM9 Ref. 2021/58530

110. *UK HPR1000 Step 4 Radiological Protection Assessment Report,* ONR-NR-AR-21-022, January 2022, ONR, CM9 Ref. 2021/52054

111. *Elaboration of a Phenomena Identification Ranking Table (PIRT) for the modelling of In-Vessel Retention*, ANE 146: pp 1-12, 2020, Fichot, F. et al.

112. GHX00600305DRAF02GN, *Sensitivity Studies on Key Parameters of Severe Accident Source Term Analysis*, Rev B, 18 December 2020, CGN, CM9 Ref. 2020/322706

113. *UK HPR1000 Level 4 Severe Accidents Workshop,* ONR-NR-CR-18-820, 28 February, ONR, CM9 Ref. 2019/94570.

114. Pre-Construction Safety Report Chapter 4 *General Safety and Design Principles,* HPR/GDA/PCSR/004, Rev 2, October 2021, GNSL, CM9 Ref. 2021/72680

115. Modification Form Cat2 M89 - *"Design modification to Improve the Independence and Reliability of KDA [SA I&C] (M89-GHTCN000200-A)",* HPR-GDA-LETT-0109, April 2021, GNSL, CM9 Ref. 2021/30979

116. *UK HPR1000 Step 4 Human Factors Assessment Report,* ONR-NR-AR-21-013, Rev 0, January 2022, ONR, CM9 Ref. 2021/54151

117. *UK HPR1000 Step 4 Control and Instrumentation Assessment Report,* ONR-NR-AR-21-005, Rev 0, January 2022, ONR, CM9 Ref. 2021/57205

118. *UK HPR1000 Step 4 Mechanical Engineering Assessment Report,* ONR-NR-AR-21-004, Rev 0, January 2022, ONR, CM9 Ref. 2021/50021

119. *Severe Accident Environmental Conditions*, GHX00600299DRAF02GN, Rev B, 27 October 2020, CGN, CM9 Ref. 2020/303859

120. *UK HPR1000 Level 4 Severe Accidents Meeting*, ONR-NR-CR-20-736, November 2020, ONR, CM9 Ref. 2020/316186

121. *Pre-Construction Safety Report: Chapter 8: Instrumentation and Control*, Rev 002, October 2021, GNSL, CM9 Ref. 2021/72676

122. *Severe Accident Battery Duration Analysis Report*, GHX05000005DEDQ45GN, Rev E, September 2020, CGN, CM9 Ref. 2020/290071

123. *UK HPR1000, Step 4 Electrical Engineering Assessment* Report, ONR-NR-AR-21-011, Rev 0, January 2022, ONR, CM9 Ref. 2021/51507

124. *UK HPR1000, Step 4 External Hazards Assessment Report*, ONR-NR-AR-21-006, Rev 0, January 2022, ONR, CM9 Ref. 2021/54151

125. *Technical Scheme and Framework Development Report for Full-scope SAMG*. GHX00600122DRAF02GN, Rev D, November 2020, CGN, CM9 Ref. 2020/314876

126. *General Study Report for Full-scope SAMG,* GHX00600121DRAF02GN, Rev B. November 2018, CGN, CM9 Ref. 2018/367438

127. *Human Reliability Assessment for the Human Actions in Severe Accident Analysis*, GHX00100163DIKX03GN, Rev A, September 2020, CGN, CM9 Ref. 2020/2888

128. *Lessons Learnt from Fukushima*, GHX00100112DOZJ03GN, Rev A, November 2019, CGN, CM9 Ref. 2019/347028

129. *Mobile Water Supply Equipment Design Scheme*, GHX00100018DCHS03GN, Rev. A, March 2021, CGN, CM9 Ref. 2021/22359

130. *Mobile Diesel Generator Design Scheme*, GHX05000045DEDQ45GN, Rev. B, 27 April 2021, CGN, CM9 Ref. 2021/34978

131. *Public Health Protection in Radiation Emergencies,* PHE-CRCE-049, May 2019, Public Health England

132. *Severe Accident Analysis on Spent Fuel Pool*, GHX00600259DRAF02GN, Rev B, 29 September 2020, CGN, CM9 Ref. 2020/288789

133. *Pre-Construction Safety Report: Chapter 33: ALARP Evaluation,* HPR/GDA/PCSR/033, Rev 002, October 2021, GNSL, CM9 Ref. 2021/72615

134. *Design of Reactor Containment Systems for Nuclear Power Plants*, IAEA NS-G-1.10, 2004 (superseded)

135. *Suitability Analysis of Codes and Standards in Severe Accident Analysis*, GHX00800009DRAF02GN, Rev B, 9 July 2021, CGN, CM9 Ref. 2021/53932

136. *Gap Analysis with TAG-007*, GHX00600178DRAF02GN, Rev A, 15 June 2018, CGN, CM9 Ref. 2018/199797

137. GHX00100135DOZJ03GN, *Containment Filtration and Exhaust System Justification Report*, Rev B, 27 October 2020, CGN, CM9 Ref. 2020/303861

138. *Pre-Construction Safety Report: Chapter 13: Design Extension Conditions and Severe Accident Analysis,* Rev 002, 4 October 2021, GNSL, CM9 Ref. 2021/72671

139. *Severe Accident Analysis Safety Case Review and Improvement Strategy,* HPR/GDA/LETT-0061, GNSL-REG-0061N, 6 August 2020, GNSL, CM9 Ref. 2020/239124

140. *Assessment of the Response to RO-UKHPR1000-0003, Suitable and Sufficient Severe Accident Analysis Safety Case*, ONR-NR-AN-20-020, 22 February 2021, ONR, CM9 Ref. 2021/15947

Annex 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No	SAP Title	Description
SC.4	**The regulatory assessment of safety cases** Safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
SC.5	**The regulatory assessment of safety cases** 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.3	**Engineering principles: key principles** 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	**Engineering principles: key principles** Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.
EKP.5	**Engineering principles: key principles** Safety measures	Safety measures should be identified to deliver the required safety function(s).
ECS.1	**Engineering principles: safety classification and standards** 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 regard to safety.
ECS.2	**Engineering principles: safety classification and standards** 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.
EQU.1	**Engineering principles: equipment qualification** Qualification procedures	Qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.

SAP No	SAP Title	Description
ESS.3	**Engineering principles: safety systems** Monitoring of plant safety	Adequate provisions should be made to enable the monitoring of the facility state in relation to safety and to enable the taking of any necessary safety actions during normal operational, fault, accident and severe accident conditions.
ESR.1	**Engineering principles: control and instrumentation of safety-related systems** Provision in control rooms and other locations	Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations.
EES.1	**Engineering principles: essential services** Provision	Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and in fault and accident conditions.
EES.9	**Engineering principles: essential services** Simultaneous loss of service	Essential services should be designed so that the simultaneous loss of both normal and back-up services will not lead to unacceptable consequences.
EHF.3	**Engineering principles: human factors** Identification of actions impacting safety	A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents.
ECV.2	**Engineering principles: containment and ventilation: containment design** Minimisation of releases	Containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions.
ECV.3	**Engineering principles: containment and ventilation: containment design** Means of confinement	The primary means of confining radioactive materials should be through the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.
FA.1	**Fault analysis: general** 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.

SAP No	SAP Title	Description
FA.2	**Fault analysis: general** 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.
FA.3	**Fault analysis: general** Fault Sequences	Fault sequences should be developed from the initiating faults and their potential consequences analysed.
FA.15	**Fault analysis: severe accident analysis** Scope of severe accident analysis	Fault states, scenarios and sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.
FA.16	**Fault analysis: severe accident analysis** Use of Severe Accident Analysis	Severe accident analysis should be used in the consideration of further risk-reducing measures.
FA.25	**Fault analysis: severe accident analysis** Relationship to DBA and PSA	The severe accident analysis should be performed in a manner complementary to the DBA and PSA, so that each type of analysis informs the others in a mutually consistent manner within the facility's safety case.
AV.1	**Fault analysis: assurance of validity of data and models** Theoretical models	Theoretical models should adequately represent the facility and site.
AV.2	**Fault analysis: assurance of validity of data and models** Calculation methods	Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place.
AV.3	**Fault analysis: assurance of validity of data and models** 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.5	**Fault analysis: assurance of validity of data and models** Documentation	Documentation should be provided to facilitate review of the adequacy of the analytical models and data.
AV.6	**Fault analysis: assurance of validity of data and models** 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	**Numerical targets and legal limits** 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.
NT.2	**Numerical targets and legal limits** Time at risk	There should be sufficient control of radiological hazards at all times.
AM.1	**Accident management and emergency preparedness** Planning and preparedness	Strategies and plans should be in place to prepare for and manage accidents at the facility and/or site.

Annex 2

Assessment Findings

Number	Assessment Finding	Report Section
AF-UKHPR1000-0079	The licensee shall determine whether reflooding following corium pool formation will challenge the structural integrity of the reactor pressure vessel. The potential impact of reflooding should be accounted for in the severe accident management guidelines.	4.5.2
AF-UKHPR1000-0080	The licensee shall, as part of detailed design and as part of development of severe accident management guidelines, demonstrate that equipment used for severe accident management is not negatively impacted by the exhaust of the passive autocatalytic recombiners of the containment combustible gas control system.	4.5.3
AF-UKHPR1000-0081	The licensee shall, as part of detailed design and as part of development of severe accident management guidelines, determine the required stocks of consumables to replenish the containment filtration and exhaust system. If necessary, the requirement for replenishment should be included in the severe accident management guidelines.	4.5.6
AF-UKHPR1000-0082	The licensee shall, as part of detailed design of the external reactor vessel cooling channel and in-vessel retention subsystem, substantiate the lower head critical heat flux curve used in the severe accident analysis, and provide evidence that the geometry of the external reactor vessel coolant channel has been optimised to maximise the value of critical heat flux.	4.6.4

Annex 3

Plant Operating States

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	Plant Operating State
Reactor in power (RP)	Reactor in power	Closed	PZR level at setpoint	3	295≤T≤307	155	Critical boron concentration	Shutdown banks extracted Control banks auto or manual	1	A
	Hot standby	Closed	PZR 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	PZR 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	PZR 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	PZR 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	PZR 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	Plant Operating State
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