Office for
Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Probabilistic Safety Analysis for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-020
Revision 0
January 2022

Published 01/22

EXECUTIVE SUMMARY

This report presents the findings of my assessment of the Probabilistic Safety Analysis (PSA) 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 PSA perspective, on whether the generic UK HPR1000 reactor 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 PSA information contained within the PCSR and supporting documentation.

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

- methods used for PSA;
- completeness and scope of the PSA modelling;
- justification and quality of documentation;
- clarity of the substantiation of the PSA;
- technical review of Level 1 PSA;
- technical review of Level 2 PSA;
- technical review of Level 3 PSA;
- the overall design;
- the design insights from the PSA results;
- PSA input to design improvements; and
- demonstration of ALARP for PSA.

The conclusions from my assessment are:

- Based on my assessment, I have concluded that the UK HPR1000 PSA methods, scope, completeness, justification and quality of the documentation, and the clarity of the substantiation, broadly meets the expectations of ONR's PSA Technical Assessment Guide (TAG) and is adequate to support the PCSR.
- The UK HPR1000 PSA has a credible and defensible basis and allows for comparison against Targets 7, 8 and 9 contained in ONR's Safety Assessment Principles (SAPs). Comparison of the results of the UK HPR1000 PSA to Targets 7 and 8 show that the estimated level of risk is below the basic safety objective (BSO). Comparison of the results of the UK HPR1000 PSA to Target 9 shows that the estimated level of risk is well below the basic safety level (BSL). However, the level of risk is slightly above the BSO for Target 9.
- The core damage frequency for internal events Level 1 PSA is low ($3.85\text{x}10^{-7}$ /ry). The large release frequency for Level 2 PSA is also low ($6.05\text{x}10^{-8}$ /ry).
- From the PSA perspective, and for matters within the scope of PSA, the final design of the UK HPR1000 achieves a level of risk consistent with RGP for a modern plant and unless they are easily achievable, my expectation is that further modifications are likely to be grossly disproportionate.

- The PSA has been used adequately during GDA to ensure that risks are being managed towards an as low as reasonably practicable (ALARP) position as the design continues through GDA and into the site-specific stage. The PSA has been used to identify ALARP improvements which have been incorporated into the GDA design reference and to calculate the risk significance of these changes to the design. My assessment has not found any major areas of the plant design for which additional ALARP analysis was needed in GDA or where alternative design features were required.
- The scope and content of the PSA is adequate for GDA. However the PSA will need to be revised by the licensee to reflect the detailed design, address the Assessment Findings identified by my review, include site-specific characteristics and operational matters and to allow for these aspects to be risk informed.

These conclusions are based upon the following factors:

- A detailed and in-depth technical assessment, on a sampling basis, of the full scope Level 1, Level 2, and Level 3 PSA. The scope of my assessment included all of the technical areas of PSA following the guidance established in ONR's PSA TAG.
- Independent information, reviews, and analysis of key aspects of the PSA undertaken by a Technical Support Contractor (TSC).
- Detailed technical interactions on many occasions with the RP, alongside the assessment of the responses to the substantial number of PSA Regulatory Queries (RQs) and PSA 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 two 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 PSA perspective a DAC may be granted.

LIST OF ABBREVIATIONS

AAD [SSFS]	Startup and Shutdown Feedwater System
A/C	Air Conditioning
ALARP	As Low As Reasonably Practicable
APG [SGBS]	Steam Generator Blowdown System
ASEP	Accident Sequence Evaluation Program
ASG [EFWS]	Emergency Feedwater System
ASP [SPHRS]	Secondary Passive Heat Removal System
ATWS	Anticipated Transient without SCRAM
AOS	Abnormal Operating State
BFX	Fuel Building
BMS	Business Management System
BMX	Turbine Generator Building
BNX	Nuclear Auxiliary Building
BPW	Circulating Water Pumping Station
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
BWX	Radioactive Waste Treatment Building
C&I	Control and Instrumentation
CCF	Common Cause Failure
CCMC	Core Cooling Monitoring Cabinet
CCRDR	Chinese National Nuclear Reliability Database
CET	Containment Event Tree
CD	Core Damage
CDF	Core Damage Frequency
CFD	Computational Fluid Dynamics
CGN	China General Nuclear Power Corporation Ltd
CRF	Circulating Water System
DAC	Design Acceptance Confirmation
DCH	Direct Containment Heating
DCL [MCRACS]	Main Control Room Air Conditioning System
DEL [SCWS]	Safety Chilled Water System
DFM	Detailed Fire Modelling
DR	Design Reference
DVL [EDSBVS]	Electrical Division of Safeguard Building Ventilation System
DWDS (NI)	Nuclear Island Demineralised Water Distribution System
DWK [FBVS]	Fuel Building Ventilation System
DXS [ESWVS]	Essential Service Water Pumping Station Ventilation System

EDG	Emergency Diesel Generator
EHR	[CHRS] Containment Heat Removal System
EMIT	Examination. Maintenance, Inspection and Testing
EOP	Emergency Operating Procedure
ESFAS	Engineered Safety Features Actuation System
ET	Event Tree
EUF [CFES]	Containment Filtration and Exhaust System
EUH [CCGCS]	Containment Combustion Gas Control System
EVF	Containment Internal Filtration System
EVR	Containment Cooling and Ventilation System
F&B	Feed and Bleed
F&C	Fuel and Core
FCG	Fangchenggang
FDF-M	Fuel Damage Frequency - Mechanical
FDF-T	Fuel Damage Frequency - Thermal
FLB	Feedwater Line Break
FMEA	Failure Mode and Effect Analysis
FT	Fault Tree
FV	Fussell Vesely
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd.
GNSL	General Nuclear System Ltd.
HAZOP	Hazard and Operability
HBSC	Human Based Safety Claims
HELB	High Energy Line Break
HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Event
HLR	Hot Leg Rupture
HPME	High Pressure Melt Ejection
HRA	Human Reliability Analysis
HBSC	Human Based Safety Claims
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICRP	International Commission on Radiological Protection
IB-LOCA	Intermediate Break Loss of Coolant Accident
IE	Initiating Event
IEC	International Electrotechnical Commission
IEF	Initiating Event Frequency

IS-LOCA	Interfacing System Loss of Coolant Accident
IRWST	In-containment Refuelling Water Storage Tank
IVR	In-Vessel Retention
JPI [FW-NI]	Fire Water System for Nuclear Island
KDA	Severe Accident Control and Instrumentation System
KDS [DAS]	Diverse Actuation System
LB-LOCA	Large Break Loss of Coolant Accident
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOCC	Loss of Cooling Chain
LODCL	Loss of Main Control Room Air Conditioning
LODVL	Loss of Electrical Division of Safeguard Building Ventilation System
LOMFW	Loss of Main Feedwater
LOOP	Loss of Off-Site Power
LRF	Large Release Frequency
LUHS	Loss of Ultimate Heat Sink
MCA	Multi Compartment Analysis
MCD	Medium Pressure Rapid Cooldown
MCR	Main Control Room
MCCI	Molten Core Concrete Interaction
MFW	Main Feedwater
MGL	Multiple Greek Letter
MLD	Master Logic Diagram
MSLB	Main Steam Line Break
MS-DOS	Microsoft Disk Operating System
MSO	Multiple Spurious Operations
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PAR	Passive Autolytic Recombiner
PACE	Probabilistic Accident Consequence Evaluation
PCSR	Pre-construction Safety Report
PDS	Plant Damage State
PIE	Postulated Initiating Event
POS	Plant Operating State
PSA	Probabilistic Safety Analysis
PSF	Performance Shaping Factor
PSV	Pressuriser Safety Valve
PTR [FPCTS]	Fuel Pool Cooling and Treatment System
PWR	Pressurised Water Reactor

RAW	Risk Achievement Worth
RBS [EBS]	Extra Boron Addition System
RCCA	Rod Cluster Control Assembly
RCD	Reactor Completely Discharged
RC	Release Category
RCP [RCS]	Reactor Coolant Pump
RCV [CVCS]	Chemical and Volume Control System
RDF	Risk Decrease Factor
RGP	Relevant Good Practice
RHR	Residual Heat Removal System
RIF	Risk Increase Factor
RIS [SIS]	Safety Injection System
RO	Regulatory Observation
RP	Requesting Party
RPE [VDS]	Nuclear Island Vent and Drain System [VDS]
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RRI [CCWS]	Component Cooling Water System
RQ	Regulatory Query
SAA	Severe Accident Analysis
SADV	Severe Accident Discharge Valve
SAMG	Severe Accident Management Guideline
SAP(s)	Safety Assessment Principle(s)
SAS	Safety Automation System
SB-LOCA	Small Break Loss of Coolant Accident
SBO DG	Station Blackout Diesel Generator
SCD	Secondary Cooldown
SEC [ESWS]	Essential Service Water System
SED [DWDS NI]	Demineralised Water Distribution System
SEL	Seismic Equipment List
SFIS	Spent Fuel Interim Storage
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Structural Integrity
SoDA	(Environment Agency’s) Statement of Design Acceptability
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
TAG	Technical Assessment Guide(s)
TEG [GWTS]	Gaseous Waste Treatment System

THERP	Technique for Human Error Rate Prediction
TSC	Technical Support Contractor
WENRA	Western European Nuclear Regulators’ Association
V&V	Verification and Validation
VDA [ASDS]	Atmospheric Steam Dump System

TABLE OF CONTENTS

Tables

Annexes

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 Probabilistic Safety Analysis (PSA).

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 RPs, ie, 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 DAC for ONR and a Statement of Design Acceptability (SoDA) for the Environment Agency.

4. The GDA for the generic UK HPR1000 design followed a step-wise approach in a claims-argument-evidence hierarchy which commenced in 2017. Major technical interactions started in Step 2 which focussed on an examination of the main claims made by the RP for the UK HPR1000. In Step 3, the arguments which underpin those claims were examined. The Step 2 reports for individual technical areas, and the summary reports for Steps 1, 2 and 3 are published on the joint regulators' website. The objective of Step 4 of GDA 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 matters identified during the earlier Step 2 and 3 assessments;
   - judging the design against the SAPs (Ref. 2) and whether the proposed design ensures risks are 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; and
   - 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 PSA 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 RQs and ROs 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 PSA of the generic UK HPR1000 design undertaken as part of GDA. I carried out my assessment using the 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 TAGs (Ref. 4), were used as the basis for my assessment. Further details are provided in Section 2. The outputs from my assessment are consistent with ONR's GDA Guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

10. The strategy for my assessment of the PSA 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 the GDA Step 4 assessment plan for PSA (Ref. 5).

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

- overall suitability and sufficiency of the PSA;
- scope of the PSA;
- assessment of internal and external hazards in the PSA;
- detailed assessment of a sample of the PSA models;
- data used in the PSA;
- consistency and sufficiency of the modelling of severe accidents in the Level 2 PSA and the interface with the Level 3 PSA;
- consideration of Examination, Maintenance, Inspection, and Testing (EMIT) in the PSA;
- adequacy of support systems modelling in the PSA;
- consideration of computer-based systems and software in the PSA;
- the RP's use of PSA in its demonstration that relevant risks have been reduced to ALARP; and
- the RP's demonstration that the SAP Targets 7-9 have been met.

2.3 Out of Scope Items

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

- Seismic PSA modelling and results. No Seismic PSA models or results were submitted for the UK HPR1000 design. However I did consider the insights from Fangchenggang Nuclear Power Plant Unit 3 (FCG3) (a plant of similar design in China used as the reference design for the UK HPR1000) where a detailed seismic PSA has been conducted. I did not conduct a detailed assessment of the FCG3 Seismic PSA; however I did consider the impact of the insights and level of risk from the FGC3 Seismic PSA within my assessment for the UK HPR1000.
- Throughout GDA the UK HPR1000 design has continued to be developed and refined. To support the design development process and regulatory assessment of the PSA the RP has submitted PSA models which are based on different Design References (DRs) over the course of GDA. The final GDA design reference is DR3, however the majority of the PSA models submitted to ONR are based upon either DR1 or DR2.1. The RP has submitted an Impact

Report (Ref. 6) to calculate the impact on the PSA of the final GDA design reference (DR3). A summary of the various PSAs and related design references submitted is provided below and in Table 2. During the authoring of this report the RP submitted an updated Internal Events PSA reflecting DR3, which supports the conclusions of the Impact Report (Ref. 6). However detailed assessment of this submission was not performed.

- Verification and Validation (V&V) of computer codes related to thermal-hydraulic analysis for supporting PSA (this work was mainly performed by the Fault Studies and Fuel and Core (F&C) topic areas).
- Fuel handling operations undertaken after spent fuel has been transported out of the fuel building, including work within the spent fuel interim storage (SFIS) building.

2.4 Standards and Criteria

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

2.4.1 Safety Assessment Principles

16. The SAPs (Ref. 2) constitute the regulatory principles against which ONR judge the adequacy of safety cases. The SAPs applicable to PSA are included within Annex 1 of this report.

17. The key SAPs applied within my assessment were SAPs FA.10, FA.11, FA.12, FA.13, FA.14 and AV.1, AV.2, AV.3, AV.4, AV.5, AV.6, AV.7, AV.8 and NT.5, NT.6, NT.7, NT.8 and NT.9. These SAPs are related to regulatory expectations for PSA, assurance of the validity of data and models and SAP Targets.

2.4.2 Technical Assessment Guides

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

- NS-TAST-GD-005, Guidance on the Demonstration of ALARP (As Low as Reasonably Practicable)
- NS-TAST-GD-030, Probabilistic Safety Analysis
- NS-TAST-GD-042, Validation of Computer Codes and Calculation Methods
- NS-TAST-GD-017, Civil Engineering
- NS-TAST-GD-019, Essential Services

2.4.3 National and International Standards and Guidance

19. Many international standards and guidance were used as part of this assessment (such as found in Refs 7, 8, 9, 17, 18, 19, and 20). Some of the most important international standards and guidance are:

- Western European Nuclear Regulators' Association (WENRA) Reactor Reference Safety Levels, Issue O, PSA.
- IAEA, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, SSG-3
- IAEA, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, SSG-4

- IAEA, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, TECDOC-1804
- IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1
- ASME Standard for Level 1/Large Early Release Frequency Probabilistic Risk Analysis for NPP Applications, ASME/ANS RA-S.
- Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), RA-S-1.2-2014
- ASME Standard for Radiological Accident Offsite Consequences Analysis (Level 3 PRA) to Support Nuclear Installations Applications, ASME/ANS RA-S-1.3-2017
- ASME Requirements for Lower Power and Shutdown PRA, ASME 58.22-2014
- EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Final Report, USRNC, NUREG/CR-6850
- Common-Cause Failure Database and Analysis System: Event Data Collection, Classification and Coding, Rev. 1, USNRC, NUREG/CR-6828

2.5 Use of Technical Support Contractors

20. It is usual in GDA for ONR to use 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.

21. Table 1 below sets out the areas in which I used TSCs to support my assessment. I used this support to provide additional assessment capability and access to independent advice and experience.

Table 1: Work Packages Undertaken by the TSC

Number	Description
1	Independent review of a range of the RP’s PSA documentation (ONR-395) which included the following aspects of work during GDA: • review, compare with RGP and provide ONR with comments on the RP’s PSA methodologies (Refs. 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31 and 32); • review, compare with RGP and provide ONR with comments on the RP’s PSA models and accompanying analysis reports (Refs. 33, 34, 36, 37, 6, 37, 38, 39, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51 and 52); • assist ONR with creating RQs to be sent to the RP based on the TSC’s review of the above submissions; • review the responses to RQs and provide ONR with feedback on RQ responses; • complete a risk-gap analysis report (Ref. 53) to advise ONR on the TSC’s most risk important concerns with the above submissions; and • produce a final report (Ref. 53) documenting the TSC’s work during of GDA.

22. The TSC provided detailed technical input to ONR following its review of the RP's submissions at my direction. I worked closely with the TSC throughout GDA. I used the input provided by the TSC to inform any RQs and ROs I raised, and my consideration of the adequacy of the PSA submission and authoring of this report. When reviewing the TSC's input, I considered the risk significance of any of the TSC's conclusions and therefore not all such matters were progressed with the RP or discussed within this report.

2.6 Integration with Other Assessment Topics

23. 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 matters that span multiple disciplines. I have therefore worked closely with a number of other ONR inspectors to inform my assessment. The key interactions were:

- Fault Studies took the lead regarding the RP's design and safety case of the containment heat removal (EHR [CHRS]) system, while I assessed the PSA aspects of inadvertent injection to the reactor pit during full power operation.
- Human Factors (HF) took the lead regarding the RP's qualitative demonstration of the suitability and sufficiency of human actions in the design basis analysis part of the safety case, while I assessed the human reliability analysis (HRA) calculations and HRA modelling used in the PSA.
- F&C took the lead regarding the physics calculations for the reactor core after a large break loss of coolant accident (LB-LOCA), while I assessed the PSA consideration of this accident.
- Fault Studies took the lead regarding assessment of the V&V of the computer codes used in the support analysis for PSA, while I assessed the success criteria that was derived from those analyses.
- Severe Accident Analysis (SAA) took the lead regarding assessment of the severe accident safety case, while I assessed the probabilistic aspects in the Level 2 PSA.
- Civil Engineering took the lead assessing the design of the containment structure, and I assessed the Level 2 PSA modelling that was derived from those analyses.
- I took the lead assessing the modelling of software and digital control and instrumentation (C&I) in the PSA, while C&I supported my assessment.
- IH took the lead assessing the deterministic parts of the IH safety case, while I assessed the internal hazards PSA.
- External Hazards took the lead assessing the deterministic parts of the external hazards safety case, while I assessed the external hazards PSA.
- Chemistry took the lead in assessing the source terms for the Level 3 PSA, while I assessed the other aspects of the Level 2 and Level 3 PSA.

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the Generic UK HPR1000 Design

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

25. The reactor core contains zirconium clad uranium dioxide (UO_2) fuel assemblies and reactivity is controlled by a combination of control rods, soluble boron in the coolant and burnable poisons within the fuel. The core is contained within a steel Reactor Pressure Vessel (RPV) which is connected to the key primary circuit components, including the Reactor Coolant Pumps (RCP [RCS]), Steam Generators (SG), 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.

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

3.2 The Generic UK HPR1000 Safety Case

27. The RP has produced and submitted a PSA which covers: Spent Fuel Pool (SFP) PSA, internal events Level 1 PSA, Level 2 PSA and Level 3 PSA with consequence analysis developed for both core damage and non-core damage accident sequences leading to a release of radioactivity.

- Level 1 PSA estimates the frequency of accidents that cause damage to the reactor core. This is commonly called core damage frequency (CDF).
    - A Level 1 PSA models the various plant responses to an event that challenges plant operation. The plant response paths are called accident sequences. A challenge to plant operation is called an initiating event. There are numerous accident sequences for a given initiating event. The various accident sequences result from whether plant systems operate properly or fail and what actions operators take. Some accident sequences will result in a safe recovery and some will result in core damage (or fuel damage for SFP PSA). The accident sequences are graphically represented with event trees. Each event in the event tree (called a functional event) generally depicts a system that is needed to respond to the initiating event. An analysis is performed for each top event in the event tree. This analysis is graphically represented with a fault tree.
    - The frequency for each core damage accident sequence is estimated, and the frequencies for all core damage sequences are summed to

calculate the total core damage frequency. In that way, the Level 1 PSA provides the first measure of risk (i.e. CDF) which is the input to the Level 2 PSA.

- Level 2 PSA, which starts with the Level 1 core damage accidents, estimates the frequency of accidents that release radioactivity from the nuclear power plant.

  - A Level 2 PSA models the plant's response to the Level 1 PSA accident sequences that results in reactor core damage. Such core damage sequences are typically referred to as severe accidents. A Level 2 PSA analyses the progression of an accident by considering how the containment structures and systems respond to the accident, which varies based on the initial status of the structure or system and its ability to withstand the harsh accident environment.
  - Once the containment response is characterised, the amount and type of radioactivity released from the containment is analysed.

- Level 3 PSA, which starts with the Level 2 radioactivity release accidents, estimates the consequences in terms of injury to the public and damage to the environment.

  - Consequences result from the radioactive material released in a severe accident such as human health effects (i.e. short-term injuries or long-term health effects) resulting from the radiation doses to the population around the plant
  - Consequences are estimated based on the characteristics of the radioactivity release calculated by the Level 2 PSA. Those consequences depend on several factors. For example, health effects depend on the population in the plant vicinity, and the path of the radioactive plume. The plume, in turn, is affected by wind speed and direction, as well as rainfall or snowfall.
  - The Level 3 PSA estimates the final measure of risk by combining the consequences with their respective frequencies and provides a response to the questions: what can go wrong, how likely is it, and what are the consequences?

28. Throughout GDA the UK HPR1000 design continued to be developed and refined. To support the design development process and regulatory assessment of the PSA the RP has submitted PSA models which are based on different Design References (DRs) over the course of GDA. The final GDA DR is DR3, however the majority of the PSA models submitted to ONR were based upon either DR1 or DR2.1. The RP has submitted an Impact Report (Ref. 6) to explain the impact on the PSA of the final GDA design reference (DR3). A summary of the various PSAs and related design references submitted is provided below and in Table 2. During the authoring of this report the RP submitted an updated Internal Events PSA reflecting DR3, which supports the conclusions of the Impact Report (Ref. 6). However, as explained in section 2, detailed assessment of this submission was not performed.

29. To demonstrate that the methodology used for the UK HPR1000 PSA meets RGP, the RP submitted several methodology documents for the following PSA topics:

- Identification of postulated initiating events (PIEs) (Ref. 21)
- Level 1 PSA (Ref. 22)
- Human Reliability Analysis for PSA (Ref. 23)
- Spent Fuel Pool PSA (Ref. 24)
- Level 2 PSA (Ref. 31)

- Level 3 PSA (Ref. 25)
- Internal Flooding PSA (Ref. 26)
- External Hazards PSA (Ref. 27)
- Internal Fire PSA (Ref. 28)
- Seismic PSA (Ref. 32)
- Worker Risk (Targets 5 and 6) (Ref. 54)

30. The RP claims that the above PSA methodologies are based on RGP such as:

- IAEA SSG-3 (Level 1 PSA), SSG-4 (Level 2 PSA), SSR-2/1 (Safety of Nuclear Power Plants: Design), TECDOC-1804 (Level 1 PSA) (Ref. 8)
- ASME/ANS RA-S (Level 1/ Level 2 PRA) (Ref. 17)
- NUREG/CR-6928 (Generic Reliability Database) (Ref. 9)
- NUREG/CR-1829 (LOCA IEFs) (Ref. 9)
- NUREG/CR-4772 (ASEP HRA Procedure) (Ref. 9)
- NUREG/CR-1278 (Handbook of HRA Procedure) (Ref. 9)
- NUREG/CR-6883 (SPAR-H HRA Procedure) (Ref. 9)
- EPRI 3002002691 (Spent Fuel Pool and Fuel Route PSA) (Ref. 14)

31. The PCSR, Chapter 14 (Ref. 3) presents the purposes of the PSA and demonstrates how the PSA models and reports meet these purposes. The RP claims the purposes of the PSA are to:

- inform the design process and evaluate risk levels;
- demonstrate that the assessed risk levels are ALARP and meet the UK legal requirements;
- demonstrate that a balanced design for the UK HPR1000 has been achieved, so that no particular feature or initiating event (IE) makes a disproportionately large or significantly uncertain contribution to the overall risk, and that, to the extent practicable, the levels of defence in depth are independent;
- assure that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff edge effects), are prevented; and
- compare the results of the PSA with the SAPs Targets 7-9 for relevant risks.

32. The PCSR also contains a list along with explanatory text of the various PSA reports summarised as follows:

- The Internal Events Level 1 PSA model and report (Ref. 36) document the analysis of the design and operation of the plant in order to identify sequences of events that can lead to core damage and the CDF is calculated.
- The Spent Fuel Pool (SFP) Level 1 PSA model and report (Ref. 37) document the analysis of the design and operation of the fuel route and SFP in order to identify sequences of events that can lead to fuel damage, and the fuel damage frequency is calculated.
- The Hazards PSA models and reports document the analysis of the design and operation of the plant in order to identify sequences of events affected by hazards that can lead to core damage. The CDF is calculated via the following PSA models and reports:

  - Internal Fire Level 1 PSA (Ref. 48)
  - Internal Flooding Level 1 PSA (Ref. 46)
  - External Hazards Level 1 PSA (Ref. 41)
  - External Flooding Level 1 PSA (Ref. 40)
  - Risk Insights of Seismic PSA for UK HPR1000 (Ref. 45)

- The Level 2 PSA model and analysis report (Ref. 42) document the calculation of the large release frequency (LRF) of radioactive releases from the plant due to accidents in the reactor and fuel route and due to hazards (except seismic) as well as calculating the frequency of release categories (RCs) to support the Level 3 PSA.

- The Level 3 PSA model and analysis report (Ref. 44) document the calculation of the dose consequences for accident sequences resulting in off-site releases. The consequences are then combined with the frequencies of these from the results of the Level 1 PSA, Level 2 PSA, SFP PSA and hazard PSAs to allow for comparison against ONR SAP Targets 7, 8 and 9.

33. In addition to the above PSA reports and models, the worker risk was calculated, and the results and risk insights are documented in: Worker Risk Assessment Report (Targets 5 and 6) (Ref. 46). Analysis to understand the risk to on-site workers typically contains a much broader selection of the safety case than is analysed in PSA. Reflecting this, Ref. 46 contains fault sequences from a broad selection of the safety case, more than just the PSA sequences that could result in on-site worker dose. The RP has also included PSA accident sequences that do not result in core damage, Fault Studies sequences related to Target 4 and waste stream accident sequences.

34. The PSA scope includes all plant operating states (POS) including full power, low power, and shutdown. The UK HPR1000 design POS are grouped for the PSA on the basis of common plant response as considered in the PSA and are described as follows in Ref. 36:

- POS A: Reactor at full power; hot standby; hot shutdown; and intermediate shutdown with temperature <295°Celsius (C) and primary pressure in the range of 130 to 155 bar abs. This POS is stated to last for 335.09 days per year.
- POS B covers a range of states and this POS is stated to last for 2.68 days per year:

  - Intermediate shutdown with temperature >135°C and primary circuit pressure in the range of 32 to 130 bar abs;
  - Intermediate shutdown with the Safety Injection System (RIS [SIS]) – Residual Heat Removal (RIS-RHR) connection conditions, temperature in the range of 135°C to 140°C, and primary circuit pressure in the range of 24 to 32 bar abs.

- POS C covers a range of states and this POS is stated to last for 2.36 days per year :

  - Intermediate shutdown with RIS-RHR connection conditions with temperature 10°C to 140°C and primary circuit pressure 24 to 32 bar abs;
  - Normal cold shutdown with RCP [RCS] pressurisable (i.e. the primary circuit is not open in this POS).

- POS D: Normal cold shutdown for maintenance. This POS is stated to last for 4.59 days per year.
- POS E: Normal cold shutdown for refuelling. This POS is stated to last for 2.94 days per year.
- POS F: Core totally unloaded. This POS is stated to last for 16.76 days per year.

35. The RP has also provided a summary report (Ref. 6) of the impact on the internal events Level 1 PSA results from an update that included: all of the GDA modifications to the design, errors in the models that were found during GDA, and reduction of conservatisms found in the model during GDA. This is carried forward to the final version of the internal events Level 1 PSA (Ref. 55) which is based upon DR3.

36. The PSA is modelled and quantified using Risk Spectrum for all the models. This program has been developed by Lloyds Register and is commonly used throughout the world for the construction and evaluation of PSA models.

37. The RP also produced a report on ‘ALARP Demonstration Report for PSA’ (Ref. 56) in response to RO-UKHPR1000-043 (Ref. 57). This report provides evidence that the PSA methods meet RGP approaches, and that the risk calculated by the PSA is low. The report also provides evidence to demonstrate that the PSA has been used to identify areas of the design where, as stated by the RP, further risk reduction may be practicable both during GDA, and post-GDA, and areas where, as stated by the RP, it would be disproportionate to further reduce the risk.

38. Table 2 presents a summary of the PSA results as reported in Chapter 14 of the PCSR (Ref. 3). Note that these results are for DR2.1, unless stated otherwise.

Table 2: Summary of Level 1 and Level 2 PSA Results

Initiating Event Type		UK HPR1000 Results (1/ry)	
		Core Damage Frequency	Large Release Frequency
Internal Events	Internal Events	3.85x10^{-7}	6.05x10^{-8}
Internal Hazards	Internal Fire Hazards	3.47x10^{-7}	(DR1) 1.51x10^{-8}
	Internal Flooding Hazards	4.65x10^{-9}	(DR1) 1.34x10^{-9}
External Hazards	External Hazards (except for seismic hazard and external flooding)	2.11x10^{-8}	(DR1) 5.28x10^{-9}
	External Flooding Hazards	6.03x10^{-9}	6.03x10^{-9}
	Seismic Hazards	2.29x10^{-8}	N/A
Spent Fuel Pool	Spent Fuel Pool (SFP) Total	Total Fuel Damage Frequency Thermal (FDF-T): 6.64x10^{-9} Total Fuel Damage Frequency Mechanical (FDF-M): 6.0x10^{-5}	Total FDF-T: 6.64x10^{-9} Total FDF-M: 6.00x10^{-5}
	SFP Internal Events	FDF-T: 6.44x10^{-9}	
	SFP Internal Fire Hazards	FDF-T: 5.01x10^{-11}	
	SFP Internal Flooding Hazards	FDF-T: 6.35x10^{-12}	
	SFP External Hazards (except for seismic and external flooding)	FDF-T: 3.39x10^{-11}	
	SFP External Flooding	FDF-T: 1.40x10^{-11}	

39. Table 3 presents a summary of the results from the Level 3 PSA, as reported in Chapter 14 of the PCSR (Ref. 3).

Table 3**:** Summary of Level 3 PSA Results

SAP Target		UK HPR1000 Result (1/y)
7		$1.14x10^{-7}$
8	0.1-1 effective dose	$2.27x10^{-5}$
	1-10 effective dose	0
	10-100 effective dose	$2.67x10^{-7}$
	100-1000 effective dose	$1.93x10^{-7}$
	>1000 effective dose	$8.11x10^{-8}$
9		$2.34x10^{-7}$

40. Tables 4 and 5 present a summary of the results against SAP Targets 5 and 6 from the Worker Risk Assessment Report (Ref. 46).

Table 4**:** Summary of Results Against SAP Target 5

Risk of Death from Accidents Any Person on the Site	UK HPR1000 Result (1/y)
Generic Worker Total *(Generic Worker – SFP workers only)*	$4.53x10^{-7}$ *($1.06x10^{-7}$)*
Main Control Room (MCR) Worker	$1.89x10^{-8}$

Table 5**:** Summary of Results Against SAP Target 6

Accident	UK HPR1000 Result	
	Frequency (/y)	Dose (mSv)
Gaseous Waste Treatment System (TEG [GWTS]) pipeline failure in Nuclear Auxiliary Building (BNX)	$8.42x10^{-5}$	<BSO
SFP level drops to +8.78m-Internal Fire hazards	$6.76x10^{-4}$	<BSO
Main Steam Line Break (MSLB)	$6.29x10^{-4}$	<BSO
Anticipated Transient Without Scram (ATWS)	$5.20x10^{-5}$	<BSO
TEG delay beds failure in BNX	$2.98x10^{-4}$	<BSO
SFP level drops to +8.78m-Internal Event	$2.92x10^{-4}$	<BSO
Feedwater Line Break (FLB)	$2.65x10^{-5}$	<BSO
Chemical and Volume Control System (RCV [CVCS]) volume control tank failure	$1.95x10^{-4}$	<BSO
Nuclear Island Vent and Drain System (RPE [VDS]) tank or pipeline failure in BNX	$1.69x10^{-4}$	<BSO
Intermediate Break Loss of Coolant Accident (IB-LOCA)	$1.35x10^{-5}$	<BSO
LB-LOCA	$2.39x10^{-6}$	<BSO
Level 2 PSA sequences	$1.47x10^{-7}$	<BSO
SFP level drops to +8.78m-Internal Flooding hazards	$7.92x10^{-7}$	<BSO
SFP level drops to +8.78m-External hazards	$3.72x10^{-7}$	<BSO

Accident	UK HPR1000 Result	
	Frequency (/y)	Dose (mSv)
Spectrum of Rod Cluster Control Assembly (RCCA) Ejection Accidents	1.00×10^{-4}	2.75×10^{2}
Spent fuel assembly drop	5.59×10^{-5}	2.19×10^{2}
Residual Heat Removal (RHR) System Break (Outside Containment)	1.00×10^{-4}	1.04×10^{2}

4 ONR ASSESSMENT

42. This section contains a record of my assessment of the UK HPR1000 PSA submitted to ONR in GDA, including my conclusions and findings. My approach for assessment was to work with my TSC to coordinate the assessment work such that overall a broad spectrum of all PSA submissions were reviewed. I assigned the TSC several samples from which they performed a deep review and compared the RP's work with RGP. I selected different samples from the TSC and performed a similar deep review and comparison against RGP.

4.1 Structure of Assessment Undertaken

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

- In sub-section 4.2, I present my assessment of the RP's PSA methodologies and PSA scope for all of the various PSA models and reports that were submitted. These form a foundation for the rest of my assessment.
- In sub-section 4.3, I present my assessment of the RP's assumptions used in the PSA.
- In sub-section 4.4, I comment on the computer codes and inputs that the RP used to support the PSA. I have not assessed the computer codes and inputs, however, I present my discussion on the ONR position on codes used by the RP to support its PSA.
- In sub-section 4.5, I present my assessment of the RP's identification and grouping of initiating events used in the internal events Level 1 PSA. This section is further sub-divided to consider the RP's approach, demonstration of the validity of the approach and justification of the IE frequencies used by the RP.
- In sub-section 4.6, I present my assessment of the RP's determination of success criteria used in accident sequence development in the internal events Level 1 PSA.
- In sub-section 4.7, I present my assessment of the RP's event sequence modelling used in accident sequence development. This section is further sub-divided to consider the LB-LOCA event tree modelling, the event tree end states, dependency modelling in the event tree modelling and initiators in the event tree modelling.
- In sub-section 4.8, I present my assessment of the RP's Level 1 and Level 2 PSA system analysis.
- In sub-section 4.9, I present my assessment of the RP's human reliability analysis used in the internal events Level 1 PSA. This section is further sub-divided to consider the RP's approach, quantification of human error probabilities and operator action dependency calculations.
- In sub-section 4.10, I present my assessment of the RP's modelling of C&I in the internal events Level 1 PSA.
- In sub-section 4.11, I present my assessment of the RP's data analysis used in the internal events Level 1 PSA. This section is further sub-divided to consider: the RP's calculation of individual component failure probabilities; unavailability due to test and maintenance; and common cause failures.
- In sub-section 4.12, I present my assessment of the RP's modelling of low power and shutdown modes in the internal events Level 1 PSA.
- In sub-section 4.13, I present my assessment of the RP's spent fuel pool PSA. This section is further sub-divided to consider: the RP's overall plan and scope of the spent fuel pool PSA; initiating event identification, grouping, frequency calculation and screening; determination of success criteria; event sequence modelling; overall results; and hazards spent fuel pool PSA.

- In sub-section 4.14, I present my assessment of the RP's use of uncertainty analysis, quantification of the internal events Level 1 PSA and interpretation of the internal events Level 1 PSA results. This section is further sub-divided to consider the internal events Level 1 PSA quantification, uncertainty analysis, importance analysis, sensitivity analysis and main results and insights. In addition, I have included a sub-section presenting my assessment of the RP's impact report analysis of the internal events Level 1 PSA results and a commentary on the RP's Version C of the internal events Level 1 PSA.
- In sub-sections 4.15 to 4.18, I present my assessment of the RP's Level 1 PSA for internal fire, internal flooding, external hazards and seismic analysis hazards respectively.
- In sub-sections 4.19 to 4.24, I present my assessment of the RP's Level 2 PSA. These sub-sections cover the overall scope and approach, plant damage states, phenomenon analysis, containment event trees, release category and source term analysis respectively, and the overall results.
- In sub-section 4.25, I present my assessment of the RP's Level 3 PSA. This section is further sub-divided to consider justification for Level 3 PSA codes and approaches; methodology; overall results; and ONR's comparison analysis.
- In sub-section 4.26, I present my assessment of the RP's worker risk assessment relating to the SAPs Targets 5 and 6. This section is sub-divided further to consider methodology and results.
- In sub-section 4.27, I present my assessment of the overall PSA results. This includes contribution from all of the different PSA models and reports as discussed in previous sub-sections.
- In sub-section 4.28, I present my assessment of the RP's use of PSA in demonstrating that relevant risks have been reduced to ALARP.
- In sub-section 4.29, I present my assessment of the RP's consolidated safety case for the PCSR Chapter 14.

44. For each of the relevant 'assessment expectations' in the tables presented in Appendix 1 of NS-TAST-GD-030, ONR's PSA TAG (Ref. 4), a view on the adequacy, or otherwise, of the submitted documentation, including any appropriate RQ and RO responses, has been taken. In cases where limitations and/or potential gaps have emerged there has been dialogue with the RP in an effort to resolve the matter or identifying if further information could be provided.

45. My Step 3 PSA assessment (Ref. 65) found that most of the PSA submitted aligned favourably with RGP, however in a few specific technical areas, I identified gaps against RGP. These areas included: absence of UK HPR1000 seismic PSA for GDA, lack of adequate support system modelling/analysis; absence of consideration of C&I; spurious C&I IEs; poorly substantiated IE frequencies; and poor documentation in general. My work through Step 4 of GDA identified further gaps in a few areas of the PSA. I raised a series of ROs (Ref. 57) to ensure that the gaps be closed during GDA. The RP closed these gaps and by the end of Step 4 of GDA I have closed all of these ROs.

46. The ROs I raised and closed during GDA were:

- RO-UKHPR1000-0013, Modelling of Computer Based System Reliability in the PSA
- RO-UKHPR1000-0018, Substantiation of HRA Inputs in PSA Model
- RO-UKHPR1000-0019, Substantiation of Initiating Event Frequencies in the PSA
- RO-UKHPR1000-0020, Veracity of PSA Data
- RO-UKHPR1000-0029, Internal Fire PSA
- RO-UKHPR1000-0043, Demonstration of ALARP for PSA
- RO-UKHPR1000-0047, Suitable and Sufficient Level 2 PSA

47. I contributed to the following ROs which were led by a different specialist inspector's:

- RO-UKHPR1000-0004, Development of a Suitable and Sufficient Safety Case was raised by the Management for Safety and Quality Assurance (MSQA) inspector and is reported in the MSQA Step 4 AR (Ref. 58).
- RO-UKHPR1000-0021, Demonstration of the Adequacy of Examination, Maintenance, Inspection and Testing of Structures, Systems and Components Important to Safety was raised by the Fault Studies inspector and is reported in the Fault Studies Step 4 AR (Ref. 59).
- RO-UKHPR1000-0023, Demonstration of Diverse Protection for Frequent Faults was raised by the Fault Studies inspector and is reported in the Fault Studies Step 4 AR (Ref. 59).
- RO-UKHPR1000-0032, Inadvertent Flooding of Reactor Pit was raised by the SAA inspector and is reported in the SAA Step 4 AR (Ref. 63)
- RO-UKHPR1000-0050, Selected Spent Fuel Interim Storage Technology ALARP Demonstration was raised by the Radwaste Decommissioning and Interim Spent Fuel Storage Inspector and is reported in the Spent Fuel Interim Storage AR (Ref. 64)

4.2 Level 1 PSA Methodologies and PSA Scope

48. The scope of the RP's PSA includes all sources of radioactivity at the facility, including the reactor core, SFP (including fuel handling facilities), radioactive waste and new fuel during all POS. Fuel handling operations undertaken after spent fuel has been transported out of the fuel building, including work within the spent fuel interim storage (SFIS) are outside of the scope for GDA.

49. For seismic hazards, the RP submitted a Seismic PSA Methodology (Ref. 32) and a seismic risk-insights study (Ref. 45) based on the UK HPR1000 reference design (FCG3), however a full scope Seismic PSA was not performed for the UK HPR1000 design. The RP justified this by claiming that a site-specific seismic PSA was not in the scope for GDA, being a generic assessment, and that the risk-insights study would provide enough design-specific understanding of the seismic risk from the plant to be useful for GDA.

50. The RP has submitted a number of specific methodologies for use in the GDA PSA. The following list contains a reference for the methodologies of each topic area in the PSA (see Section 3):

- Identification of postulated initiating events (PIEs) (Ref. 21)
- Level 1 PSA (Ref. 22)
- Human Reliability Analysis for PSA (Ref. 23)
- Spent Fuel Pool PSA (Ref. 24)
- Level 2 PSA (Ref. 31)
- Level 3 PSA (Ref. 25)
- Internal Flooding PSA (Ref. 26)
- External Hazards PSA (Ref. 27)
- Internal Fire PSA (Ref. 28)
- Seismic PSA (Ref. 32)
- Worker Risk (Targets 5 and 6) (Ref. 54)

51. The RP has stated that its methodologies were based on RGP such as Refs 8 and 17.

4.2.1 Assessment

52. The TSC and I reviewed the methodologies (see Section 3) associated with the different PSA models and reports and compared them with RGP such as Refs 8 and 17 and ONR expectations in the SAPs and PSA TAG (Ref. 4). I found that the RP's

methods were very similar to RGP and where I found discrepancies, these were not significant. I found some minor shortfalls, and I have outlined these findings in the relevant assessment sub-sections in this report for each of the PSAs. The TSC also performed an independent review and comparison of all of the submitted methodology documents and the TSC findings can be found in their final report (Ref. 53). I considered the TSC's opinion as part of my own review and am content that the methodologies for each type of PSA do not have significant differences with RGP. Thus I am content with the RP's use of these methodologies to perform the PSA during GDA.

53. I assessed the RP's reasons for not performing a detailed seismic PSA during GDA and am content with their alternate scope of work to demonstrate the risk importance of seismic hazards. I have presented my assessment of the RP's demonstration of risk insights from seismic hazards in more detail in the relevant sub-sections later in this report.

4.2.2 Strengths

54. The scope and approaches used for the PSA meet regulatory expectations compared with the ONR SAPs and PSA TAG.

55. The scope of the PSA was quite broad and comprehensive.

4.2.3 Outcomes

56. My assessment of the RP's submissions on Level 1 PSA methodologies and PSA scope against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.2.4 Conclusion

57. Overall, I find that the PSA methodologies, approaches, and scope meet favourably with expectations established by RGP.

4.3 Level 1 PSA Assumptions

4.3.1 Background to Assessment of RP's Level 1 PSA Assumptions

58. Each of the different PSA reports contain a separate section documenting the assumptions used in that PSA topic (e.g. Section 3.4 of Ref. 36) as well as rationalisation for each assumption. In addition, the RP provided sensitivity studies for some of the significant assumptions in each PSA topic report.

59. The assumptions listed in each PSA report can be broken down into different types of assumptions:

- operational assumptions (e.g. in RHR operation mode, it is assumed that train A and B are running, and train C is in standby for RHR and component cooling water system (RRI [CCWS])); and
- design assumptions (e.g. it is assumed that spurious RPV failure leads directly to core damage)

4.3.2 Assessment

60. The TSC reviewed a sample of the assumptions in each of the PSA topic reports. I also reviewed a sample of the assumptions in these reports. The TSC and I compared the identification, description, justification and use of the sampled assumptions against ONR expectations as described in the PSA TAG (Ref. 4) and in IAEA SSG-3 (Ref. 8). The TSC provided me with questions and comments regarding some of the sampled

assumptions and these were included in RQ-UKHPR1000-0236, RQ-UKHPR1000-0484, RQ-UKHPR1000-0485 (Ref. 66). The assumptions, although clearly identified, were not always categorised well, and thus it was difficult to understand how a particular assumption was being used in the relevant PSA model. In addition, some assumptions were not always traceable to the underlying justification (sometimes referred to as the 'golden thread' of the safety case). However, when I requested further information the RP was able to provide it. Following multiple discussions with the RP and reviewing responses to the RQs I am content that the assumptions contained within the PSA have been identified and justification is available, although the link to the justification may not be obvious or clear within the PSA reports

61. In addition to my review of the RP's work in describing and justifying the use of assumptions, the RP also provided sensitivity studies for many assumptions in the PSA topic reports, including Ref. 36. The RP stated that these sensitivity studies were provided to gain a measure of understanding of the sensitivity of the relevant PSA topic results to these underlying assumptions. The RP has provided studies of these sensitivity calculations in the various reports. I sampled some of the RP's analysis and the analysis showed that the assumptions that the RP made were not risk important to the Level 1 PSA. I have provided an example of my assessment of two of the assumptions that I sampled.

62. I sampled the RP's assumption in the Level 1 PSA that the failure probability of the RCP [RCS] pump seals was $1x10^{-4}$. This assumption was clearly identified and described; however, I did not find that the justification was complete. In addition, I noted that this failure probability was somewhat lower than I had expected. Ref. 33 documented that the failure probability was an assumed value from engineering experience. To further investigate this assumption, I wrote RQ-UKHPR1000-0615 (Ref. 66). In the response to this RQ, the RP provided further justification for this assumed failure probability and claimed that these seals are a modern hydro-dynamic type of seal and thus have a high reliability compared with older less advanced designs used in traditional PWRs. In addition, the RP provided sensitivity calculations demonstrating that the PSA results are not sensitive to this assumption (i.e. when a failure probability for the pump seals 100x greater was used ($1x10^{-2}$) the internal events Level 1 PSA CDF rose by only 11%). After discussions with the RP, I am content that this assumption has been clearly identified and described.

63. I sampled the RP's assumption in the SFP PSA that the RPV will not be damaged in the event of a dropped load. This assumption was clearly identified, however further information or a description and justification were not apparent in the text of the SFP PSA Report (Ref. 37). Thus, I raised RQ-UKHPR1000-0737 (Ref. 66) to seek more information regarding this assumption. The RP's response outlined that this assumption was based on analysis found in Ref. 67. This report provided analysis to show that the RPV was not damaged in the event of a head drop. The RP argued that if the RPV was not damaged in a head drop accident, a much lighter dropped load such as a fuel element would be considered bounded by the head drop. I discussed this report with the structural integrity inspector and IH inspector and determined that the RP's justification for this assumption was reasonable and that evidence existed to provide confidence for the assumption. Thus, I am content that this assumption was clearly identified, and the golden thread of the safety case was clear. For GDA, the justification is adequate, however, the description and justification of this assumption will need to be improved post-GDA within the PSA reports.

4.3.3 Strengths

64. The RP has properly identified the assumptions used in the PSA.

65. The RP has provided in depth sensitivity studies for assumptions to understand the effect of reducing the conservative nature of some assumptions. This report was

particularly useful in understanding the RP's efforts to judge whether or not assumptions made were risk important and if conservatisms should be reduced.

4.3.4 Outcomes

66. My assessment of the RP's submissions on Level 1 PSA assumptions against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.3.5 Conclusion

67. The RP identified assumptions used in the various PSA models and provided analysis to understand the sensitivity of the PSA results to assumptions. However, traceability of assumptions to their underlying information to justify the validity of assumptions was not always clear and required follow-up discussions with the RP to verify.

4.4 Computer Codes and Inputs

68. The RP performed support analysis using several computer codes and input information, which are discussed in Appendix A of Ref. 36. The RP used the following codes for PSA support analysis:

- LOCUST V1.0.2 – for thermal-hydraulic analysis for LOCAs, SGTR, and feedwater line break
- LOCUST-K V1.0 – a more conservative version of LOCUST, used for SB/IB-LOCA and LB-LOCA thermal-hydraulic analysis
- CATALPA V1.1.0 – for containment analysis during LOCAs
- COCO V1.1.12 – for nuclear data calculation for LOCA accident analysis
- ASTEC V2.1 – for severe accident analysis of both the reactor coolant system and the containment chemical-physical phenomenon analysis

69. In the PSA TAG (Ref. 4), ONR's expectations for computer codes and inputs are that for any codes used, they have been verified, validated or qualified, as appropriate, and that the codes meet ONR quality expectations as outlined in SAPs para 678 ff and TAG-042 (Ref. 4). As I did not perform assessment of these codes, I relied on the assessment of the validation of these codes performed by other inspectors, as can be found in the next section of this report. Although some of these codes were used in a different way for PSA compared with design basis analysis, the underlying code was stated by the RP to be the same. The SAA, FS and F&C inspectors and their TSCs reviewed the validation of these codes.

4.4.1 Assessment

70. Assessment of the V&V of LOCUST and CATALPA was performed by the Fault Studies inspector and the conclusions can be found in the Assessment Report for Fault Studies (Ref. 59). Assessment of the V&V of COCO was performed by the Fuel & Core inspector and the conclusions can be found in Step 4 Assessment Report for Fuel & Core (Ref. 68). Assessment of the V&V of ASTEC was performed by the SAA inspector and the conclusions can be found in the Step 4 Assessment Report for SAA (Ref. 63).The assessments did not undermine confidence in the use of these codes (except in one specific area of LOCUST: clad ballooning - see Ref. 68). In general, the FS, SAA and F&C inspectors' assessment of these codes provided me with confidence in the ability of these codes to appropriately estimate the success criteria and approximate timings for use in PSA modelling. With respect to the matter regarding clad ballooning modelling and LOCUST, I have discussed this topic later in this report in sub-section 4.7.2.1.

4.4.2 Strengths

71. No matters of significance were identified as a strength compared with my expectations for the RP's PSA related computer codes and inputs

4.4.3 Outcomes

72. My assessment of the RP's submissions on PSA related computer codes and inputs against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.4.4 Conclusion

73. Assessment of the V&V for computer codes used in the support analysis for PSA was performed by FS, F&C and SAA inspectors and the conclusions can be found in those reports (Refs 59, 68 and 63). The FS, SAA and F&C inspectors did not identify any matters which undermined my confidence in use of these codes for PSA except for clad ballooning where the F&C inspector found gaps that will need to be addressed in by the licensee as the safety case develops (see Ref. 68).

4.5 Level 1 PSA: Identification and Grouping of Initiating Events

74. The RP's approach for identifying IEs is found in Ref. 21. In summary, the RP identified all of the IEs through systematic analytical methods such as hazard and operability (HAZOP) analysis, failure mode and effect analysis (FMEA) and master logic diagrams. The RP also used lists of IEs for similar plants to help in identifying all IEs. To begin the process of identification and grouping of IEs, the RP used different criteria to make the long list of IEs to be used in the PSA for all operating modes of the plant more manageable. The following sub-sections describe the steps taken to process the IE list and my assessment.

75. The RP performed grouping/bounding and screening analysis in order to limit the analysis required for the PSA. The RP used three criteria to group IEs as per guidance of Ref. 17. These criteria were:

- similarity in plant response, success criteria, timing and effect on the operability and performance of operators and relevant mitigating systems;
- similar impact on the plant from the IE; and
- similar consequence from the IE.

76. This grouping and bounding process resulted in a set of 31 IE groups. After arriving at the list of IEs to be analysed in the PSA, the RP performed comparison analysis against similar plants which have their IE list published. This comparison was used by the RP to confirm that the IE list for the UK HPR1000 PSA met RGP.

77. Finally, IE frequencies (IEFs) were assigned for those IEs in the final list. The RP assigned these frequencies using several different approaches, depending on the nature of each IE. The RP also provided a comparison of their IEFs with generic data, such as NUREG-6268 (Ref. 9). The RP used an order of priority whereby Operational Experience (OPEX) data, generic data, fault tree analysis, and assumed values were used in descending order of priority.

- For IEs where OPEX existed in the Chinese nuclear database sources (summarised in Ref. 33) and the IE had occurred greater than five times, the RP used a simple n/T calculation, where n is the number of occurrences, and T is the number of reactor years.
- For IEs where there less than five occurrences in the Chinese nuclear database, the RP used Bayesian approaches to combine Chinese OPEX with international OPEX (see Ref. 33).

- For a few IEs, the RP created a fault tree to understand the frequency of the IE, for example for support system failure IEs such as loss of cooling chain (LOCC).
- For a few IEs whereby the above three approaches were not applicable, assumed values were provided, with discussion and substantiation included.

78. After the IEFs were assigned for each IE, the RP performed a final screening exercise whereby some IEs were screened out and thus detailed analysis in the PSA was not performed for these IEs. The criteria used to screen IEs was as per Ref. 17, and included five criteria of which an IE was screened out of further analysis if it met one:

- IEF < 1x 10^{-7} /ry, and the event does not include an Interfacing System Loss of Coolant Accident (IS-LOCA), containment bypass or RPV rupture.
- IEF < 1x10^{-6} /ry, and core damage (CD) cannot occur unless at least two trains of mitigating systems fail independently from the IE.
- IE could lead to CD or containment bypass, but the risk caused by it is far less than the CDF, ie, the IEF <1x10^{-9} /ry.
- For IS-LOCA IEs, leakage pathways are screened out where the pipe diameter < 16mm (area <2cm^2) as leakage rates of this small size are within the makeup capacity of the RCV [CVCS].
- For IS-LOCA IEs where at least two means of redundant isolation are available (diverse C&I) and where the loss of coolant is detected. The means of isolation cannot be impacted by the IS-LOCA (i.e. they must be separated by flood barriers).

4.5.1 Assessment

79. TAG-30 (Ref. 4) and SAPs FA.12 and FA.13 (Ref. 2) describe ONR expectations for identification and grouping of IEs. The RP's approach must be clear and demonstrated to be appropriate for use in the UK compared with similar RGP approaches. IE frequencies that are used in PSA models in the UK should be clearly linked with underlying OPEX, if possible, and if no OPEX is available, then alternative methods for deriving a frequency should be clearly explained and justified as appropriate for use in PSA models in the UK. I have followed this guidance in my assessment of the RP's submissions relating to IE identification and grouping.

80. The TSC reviewed the list of IEs and selected a sample to perform more in-depth assessment. I also selected a few of the more risk-important IEs as a sample and performed more in-depth assessment on these. As a result of the TSC and my assessment, I included questions on the sampled IEs in the following RQs: RQ-UKHPR1000-0056, RQ-UKHPR1000-0235, RQ-UKHPR1000-0308 and RQ-UKHPR1000-0484 (Ref. 66). Taking the TSC assessment and the RP's response to my RQs in account, I concluded that there was a gap in the justification and documentation of the IE list used in the Level 1 PSA. To address this gap I raised RO-UKHPR1000-0019 (Ref. 57). In response, the RP updated the PSA documentation (see Refs 33, 34 and 33) to provide a more complete justification of the IEs used in the UK HPR1000 PSA. My assessment of the updated reports, which formed part of my decision to close the RO is set out in the sub-sections below.

4.5.1.1 Approach for Identification, Grouping and screening of Initiating Events

81. The TSC reviewed the RP's approach for identifying and grouping the initiating events that were analysed in the PSA (Ref. 33) and provided positive feedback. In my opinion, the RP has provided an adequate justification to demonstrate that the methods and approaches used to select, group, and screen the list of IEs used in the UK HPR1000 PSA are suitable and sufficient for use in the safety case and meet ONR's regulatory expectations.

82. The RP's approach taken for selection of the initial group of postulated IEs is similar to that suggested by RGP, such as Refs 8 and 17, and uses a master logic diagram together with FMEAs. This approach is a common and adequate way to select an initial pool of IEs from which to group and screen from.

83. The RP's approach for grouping and screening is also similar to that suggested by RGP such as Refs 8 and 17, which suggest grouping and screening should be on the basis of:

- similarity in plant response;
- success criteria;
- timing;
- the effect on the operability; and
- performance of operators and relevant mitigating systems.

84. The IE groups were then bounded by the worst case within the group. The final list of IE groups was then screened by the RP using similar approaches to RGP such as Refs 8 and 17. The final IE list contains the IEs that I would expect to be analysed and the RP provided adequate justification for IEs that were screened out.

85. When I reviewed the RP's approach for combining US and Chinese OPEX, I noticed that the RP used at least 'five' incidents in Chinese data as the minimum number required for using pure Chinese data. This number appeared to be arbitrary, and the RP did not adequately explain why this is an appropriate number to use to combine data. In the IEs that I sampled, it did not appear that this significantly affected the results of the PSA, however I found this to be an anomaly in an otherwise well documented part of the safety case. I expect that the licensee will need to ensure that this approach is credible post-GDA to combine generic and Chinese data. However, this will be part of normal business.

86. In my opinion, the approaches used to select, group, and screen the list of IEs is similar to RGP and are appropriate and have been justified and meet the expectations as outlined in the PSA TAG (Ref. 4) and in the SAPs.

4.5.1.2 Demonstration of the Validity of the Approach for IE Frequency Derivation

87. The TSC sampled some of the IEs to review the demonstration of the validity of the approach for IE frequency derivation. The TSC advised me that the approach which the RP used is similar to RGP such as NUREG/CR-6268, NUREG/CR-6928, and NUREG/CR-1829 (Ref. 9). I reviewed the approach and compared it with RGP, and in my opinion, the approach used to derive the frequencies of the IEs used in the UK HPR1000 PSA is suitable and sufficient for use in the PSA and meets ONR's regulatory expectations. The RP provided a comparison between their IEFs chosen for use in this project and other generic IEF data, such as NUREG/CR-6268, NUREG/CR-6928, and NUREG/CR-1829 (Ref. 9). This comparison demonstrated that IEFs used in the UK HPR1000 PSA are broadly similar to the generic IEF databases.

88. The primary source of IEFs is OPEX from CGN operated PWRs in China (Ref. 33). Ref. 33 is a reliability database that presents all reliability information used in the GDA PSA, including IEFs, failure rates, probabilities of failure on demand, proof-test intervals, etc. It also contains justification for why the RP has chosen each entry in the database, and the sources from where each entry was obtained. The RP lists the number of events and the operating life of the relevant station where the IE occurred, and thus calculates the frequency of the event. The IEF is then compared with other RGP and the RP provided further justification for selecting the IEF. After reviewing a sample of the database, the TSC advised me that the data being used had not been justified for use in the UK. The source of data used in IEFs can vary depending on the country from which the data originates, due to different expectations in operational

practice, weather, design and quality expectations, etc. I included this question in RQ-UKHPR1000-0235 (Ref. 66) and the RP stated in response that the data was appropriate for use in the UK HPR1000, as it was assumed for GDA that almost all equipment would be sourced, designed, and operated similar to the CGN PWRs in China. I found this response to be reasonable, given that as a part of normal business, the PSA would need to be updated post-GDA if this equipment sourcing, designing and operation was different from similar CGN PWRs in China thus leading to potential changes in those IE frequencies derived from Chinese OPEX.

89. In addition to CGN PWR OPEX, the RP next uses US PWR OPEX (Ref. 9). This is used to derive the IEF when there was insufficient OPEX from the Chinese nuclear fleet. As with the Chinese OPEX, the US data lists the number of events and the operating life from which the data originated. Significant discussion and justification are provided for those IEFs that use the US OPEX. The TSC sampled a selection of IEs which use US PWR OPEX. I also sampled a selection and found the sample to have used US PWR OPEX data appropriately with adequate justification for those in my sample.

90. For some IEs where the design may not be properly reflected in the Chinese or US OPEX, the RP uses fault tree analysis to derive IEFs. These are used for IEFs that are somewhat specific to the UK HPR1000 design, such as, loss of an Electrical Division of Safeguard Building Ventilation System (DVL [EDSBVS]). The data for the basic event failures used in the fault trees are sourced from the UK HPR1000 PSA database (Ref. 33). Explanation and justification are provided for IEFs which use fault tree analysis, including the fault tree itself. The TSC sampled a selection of IEs which use fault trees in their derivation. I also sampled a selection and found the sample to have used fault trees appropriately with adequate justification for those in my sample compared with RGP, such as the ONR PSA TAG (Ref. 4).

91. Expert judgement is used for assuming a value of IEFs where none of the above approaches are either appropriate or possible to be used, for example, the IEF of a RPV spurious rupture. Justification is provided for those IEFs which use expert judgement. In these cases, the RP used IEFs from PWR stations in China that were predecessors to the UK HPR1000 design (such as Daya Bay NPP). Explanation and justification are provided for the IEFs which use expert judgement to select the IEF.

92. In my opinion, the approaches used to derive the IEFs are appropriate and have been justified and meet the expectations as outlined in the PSA TAG (Ref. 4) and in the SAPs.

4.5.1.3 Demonstration of the Justification of IE Frequencies in the UK HPR1000 PSA

93. The TSC sampled the justification for a few IEs in the original reports and provided feedback to me on these. The TSC found that justification for some of the IEs in their sample was not always performed adequately compared with RGP such as the ONR PSA TAG (Ref. 4). In RO-UKHPR1000-0019 (Ref. 57), I included this topic for the RP to resolve. In response to the RO, the RP provided updated reports (Refs. 34 and 33), and I sampled these and chose several IEs with high importance to the overall internal events Level 1 PSA core damage frequency. In the following paragraphs, I have presented my assessment of the justification of three risk-important IEs:

- Loss of main feedwater
- Loss of Main Control Room Air Conditioning System (DCL [MCRACS])
- RPV rupture

94. IE Loss of Main Feedwater (IE-LOMFW) represents a total loss of main feedwater during any operating mode wherein main feedwater (MFW) is required. The IE is assigned an IEF of 3.97x10^{-2} /ry for normal full power operation (POS A) in Ref. 33.

The RP calculated this frequency by using Bayesian approaches to combine the Chinese OPEX and the US OPEX this event. I was easily able to trace through how the RP calculated this frequency in the references. The OPEX from China and the US show similar frequencies for this event, with the Chinese OPEX being slightly less frequent. When the data is combined, the final frequency used is slightly higher than the Chinese OPEX and slightly lower than the US OPEX. The RP also presented a useful justification and an explanation for why this frequency is appropriate to be used in the UK HPR1000 PSA. In my opinion, this frequency is appropriate to be used for the UK HPR1000 PSA as the RP followed their process for calculating and justifying the IEF and the RP's final frequency is in line with generic frequencies for this IE. The RP's arguments and calculations are reasonable and proportionate for using this IEF and meet the expectations as outlined in the PSA TAG (Ref. 4) and in the SAPs.

95. IE loss of DCL [MCRACS] (IE-LODCL) represents the total loss of MCR air conditioning, and the frequency is calculated through fault tree analysis of the DCL system. For POS A, the RP modelled a loss of two out of three trains of the DCL, and for the rest of the POS, the RP modelled a loss of all three trains. I reviewed the Risk Spectrum modelling of the fault trees and was able to easily understand the system modelling. It all appeared to have been modelled correctly. The IEF for POS A of IE-LODCL was calculated to be $5.71\text{x}10^{-2}$ /ry. The RP includes a discussion of the reasoning behind the success criteria as well as a justification for using the calculated frequencies for this IE. The main assumptions were listed and the RP explained why they are reasonable. In my opinion, the IEF for IE-LODCL has been calculated according to the RP's approach, and justified for why it is appropriate for use in the UK HPR1000 PSA. The RP's conclusions are reasonable and proportionate for using this IEF and meet the expectations as outlined in the PSA TAG (Ref. 4) and in the SAPs.

96. The IE for RPV rupture was calculated for a large rupture (exceeding the size that would be otherwise analysed as a loss of cooling accident (LOCA)). It is assumed by the RP that a RPV rupture of greater than 4558 cm^2 would lead directly to core damage. The RP has used the arguments outlined in NUREG/CR-1829 (Ref. 9) which used analysis of probabilistic fracture mechanics to arrive at a conclusion that a random RPV failure will occur with the frequency range of between $1.02\text{x}10^{-7}$ /ry and $9.86\text{x}10^{-10}$ /ry. The RP then follows the guidance in NUREG/CR-1829 which is to use a frequency of $1.25\text{x}10^{-8}$ /ry, with an error factor of 10. I observed that the IEF for RPV failure has been calculated according to the RP's approach, and adequate justification has been provided. The RP's conclusions are reasonable and proportionate for using this IEF and meet the expectations as outlined in the PSA TAG (Ref. 4) and in the SAPs.

4.5.2 Strengths

97. The approaches used to derive and quantify the IE list were similar to RGP and appropriate for use in the GDA PSA. The RP justified the approaches used well.

98. The RP documented the process for grouping, bounding, and screening the initial list of IEs appropriately.

99. The priority list of IEF source information meets ONR expectations as outlined in the PSA TAG (Ref. 4).

4.5.3 Outcomes

100. The RP's justification for using pure Chinese OPEX data depended on an assumption that the systems or equipment in question were designed, built and operated suitably similar to those used in the CGN operated PWRs in China. If this assumption changes post-GDA, those IEFs will need to be re-assessed as a part of normal business.

4.5.4 Conclusion

101. In my opinion, the IEFs used are justified for use in the UK HPR1000 GDA PSA and meet the expectations outlined in SAPs FA.11 and FA.12 (Ref. 2), as well as the PSA TAG (Ref. 4).

102. The RP has provided an adequate substantiation to demonstrate that the frequencies assigned to the UK HPR1000 PSA IEs are suitable and sufficient for use in the safety case and meet ONR's regulatory expectations.

103. In my opinion, the IEFs that I sampled used are appropriate and have been justified for use in the UK HPR1000 PSA. This provides me with confidence in the RP's approach for deriving IEFs throughout the different PSA models and reports.

4.6 Level 1 PSA: Accident Sequence Development – Success Criteria

4.6.1 Introduction to Assessment of Level 1 PSA: Accident Sequence Development – Success Criteria

104. ONR expectations for the determination of success criteria are outlined in SAPs FA.13 and the PSA TAG (Ref. 4). The success criteria used in PSA are generally different than that used in design basis analysis because PSA support analysis is generally performed on a more realistic basis to understand plant response to an initiating event. I have discussed and reviewed the differences in some of the success criteria used in other topic areas.

105. The RP has determined success criteria for all of the systems included in the internal events Level 1 PSA that either fulfil the function of reactivity control or heat removal from the reactor core; and in the SFP PSA for internal events that either fulfil the function of confinement of contamination or removal of decay heat from spent fuel. The most basic way of determining these success criteria is by understanding the minimum operating requirements for a system to avoid core damage until a safe stable state can be reached. The RP explains its philosophy to developing success criteria with considerable detail in Ref. 22. In addition to main safety systems, success criteria for support systems, human actions and other SSCs are also developed.

106. To define the success criteria for the SSCs and human actions as modelled in the PSA, thermal-hydraulic and physics analysis is used. In this analysis, the RP has presented the results of various accident sequences with system success criteria for relevant SSCs. This is presented in Appendix A of Ref. 36 for the Level 1 PSA, and Appendix B of Ref. 37 for the SFP PSA.

107. The success criteria for systems modelled in the PSA is described in the text of each of the accident sequence description sections.

4.6.2 Success Criteria Assessment Sample

108. The TSC and I chose to sample the success criteria for several accident sequences in the Level 1 PSA:

- MSLB
- Steam Generator Tube Rupture (SGTR)
- Secondary side transient
- IS-LOCA
- Loss of Main Feedwater (LOMFW),
- IB-LOCA, and
- Loss of off-site power (LOOP).

109. The TSC provided feedback to me and I included questions on the success criteria used in the above sample in RQ-UKHPR1000-0484 and RQ-UKHPR1000-0485 (Ref. 66). In the following paragraphs I have presented my assessment for three of the IEs' success criteria amongst the eight that were sampled. I included further discussion of these three IEs' success criteria because (as expected in the PSA TAG (Ref. 4)) these accident sequences are high contributors to the internal events Level 1 PSA results, and they contain a broad spread of the plant systems. Thus they are good representatives to gain confidence in the RP's treatment of success criteria for the Level 1 PSA. I have also assessed IE success criteria for SFP faults later in this report in the relevant sub-section for SFP PSA.

110. In Ref. 36, in the event of a LOMFW accident, feedwater is considered completely lost including both the MFW system as well as the Startup and Shutdown Feedwater System (AAD [SSFS]). To mitigate this accident the success criteria are credited for support systems such as the following:

- At least two of eight trip breakers must open successfully.
- To shutdown the reactor, no more than 3 control rods fail to insert successfully (N-3).
- After an initial release of primary circuit pressure, all pressuriser safety valves (PSVs) must re-close.
- At least one train of emergency feedwater (ASG [EFWS]) in an intact SG loop must succeed in supplying the SG with water, and at least one train of atmospheric steam dump system (VDA) in an intact SG loop must succeed in releasing steam.
- All three ASG [EFWS] storage tanks must be manually cross-connected to at least one out of three of the ASG [EFWS] trains.
- If the secondary passive heat removal (ASP) system is required to remove primary loop heat (i.e. when ASG [EFWS] or VDA [ASDS] has failed), at least two out of three trains of the ASP [SPHRS] system are required to remove heat through an intact SG.
- If feed and bleed (F&B) is required, at least two out of three pressure safety valves (PSVs) are required to be functional (i.e. able to open and close repeatedly), and the F&B operation must be manually performed for at least 1500 seconds.
- For the in-containment refuelling water storage tank (IRWST) function, the heat exchanger for at least one train of safety injection (RIS) must function correctly, or at least one train of EHR [CHRS] [CHRS] heat exchanger must perform successfully for at least 8390 seconds.

111. For each of the above success criteria, the RP referred to further information that was claimed to be found in the Level 1 PSA report (Ref. 36) Appendix A (the thermal-hydraulic analysis section). I sampled Appendix A to ensure the above success criteria were properly supported with analysis, and found only a limited number of cases where the success criteria linked successfully with the analysis in Appendix A. Furthermore, the explanations I found in the main report for the success criteria were not always consistent or clear. I also sampled IB-LOCA and LOOP success criteria and found much the same problem with the traceability from thermal-hydraulic analysis to the text, to the fault tree and event tree modelling.

112. The TSC also observed similar problems with the traceability of success criteria from thermal-hydraulic analysis as implemented in the PSA models. The TSC provided feedback to me outlining this gap against expectations for the success criteria of the Level 1 PSA.

113. I discussed the problem I had observed with traceability of success criteria with the RP in meetings and included questions on this subject in RQ-UKHPR1000-1022. In my opinion, after discussing this with the RP extensively and reviewing the response to the

RQ, I found this to be a significant gap in the Level 1 PSA documentation. However, I did not find this to be a gap in the RP's analysis, but only in its documentation of this analysis. In each case that the TSC and I discussed with the RP, the RP was able to present further analysis and clearly explain what the success criteria was and show the support analysis from where it was derived, however this was not reflected in the submitted Level 1 PSA documentation.

114. I raised an action in RO-UKHPR1000-0043 (Action 3) against this gap in documentation because I judged the initial submission to be insufficient for GDA. The RP submitted Ref. 69 to demonstrate that for two accident sequences the success criteria was clearly traceable to the underlying support analysis. They chose to perform this further documentation for IB-LOCA and LOOP accident scenarios. These are risk important IEs, and I am content that the selection of these IEs represented a broad enough sample of the PSA modelling to draw conclusions about the overall safety case.

115. The TSC sampled Ref. 69 and found that the report was much improved over the previous reports. I also reviewed this report and found that I was able to easily trace all the thermal-hydraulic analysis through to the descriptions of the success criteria in the accident sequence description sections. For example, for IB-LOCA, a table is included in Ref. 69 for all functional events. For all the success criteria listed, information is provided regarding the exact place in the reference thermal-hydraulic analysis, or system design manual (SDM) that is the primary source of evidence for each success criteria. When timings are listed, clear explanation and evidence is provided for each timing.

116. For example, for IB-LOCA, a success criterion is stated that at least one low head safety injection (LHSI) train is required to function on the intact loop, the RP refers to Appendix B.3.4 of Ref. 36. Appendix B.3.4 shows the thermal-hydraulic analysis results for various sizes of IB-LOCAs. It is clear core damage will not occur if one LHSI train functions. Thus, the 'golden thread' for this success criteria are confirmed. The text explains the accident progression well in this case, and the referenced sections match. All other success criteria that I sampled matched similarly well.

117. Overall, I found that Ref. 69 demonstrated that the traceability of the safety case was clear for IB-LOCA and LOOP accident scenarios. However, there are many other accident scenarios other than IB-LOCA and LOOP that will require the same careful and consistent approach to presentation of the success criteria. The RP committed to improving on this aspect of their reporting for future versions of PSA reports. In Version C of the internal events Level 1 PSA (Ref. 55), I briefly reviewed some sections to confirm that the RP had improved this aspect of the documentation. I observed that in this report, for the sections I reviewed, that the RP had improved the traceability of the success criteria and this provides me with increased confidence in the RP's success criteria used in the PSA.

4.6.3 Strengths

118. I found that in Ref. 69 the traceability of the success criteria for the two revised example IEs was well referenced, clear and met my expectations.

119. I found that the success criteria, as modelled in the PSA, is linked with existing thermal-hydraulic analysis.

4.6.4 Outcomes

120. The licensee will need to improve the PSA documentation associated with success criteria as per Ref. 69.

4.6.5 Conclusion

121. The PSA success criteria has used adequate, PSA specific, thermal-hydraulic analysis. The licensee will need to ensure future submissions improve the documentation of success criteria. This is considered a minor shortfall.

4.7 Level 1 PSA: Accident Sequence Development – Event Sequence Modelling

4.7.1 Introduction to Assessment of Event Sequence Modelling

122. The expectations for PSA event sequence modelling are outlined in SAP FA.13, and the PSA TAG (Ref. 4)

123. For the UK HPR1000 PSA, accident sequences are modelled using event trees (ETs). ONR regulatory expectations for event tree modelling are outlined in Table A1-2.3 of the PSA TAG (Ref. 4). The TSC chose a sample of the event trees to assess, and I also chose a sample. The combined sample included: IS-LOCA, LB-LOCA, MSLB, secondary transients, steam generator tube rupture (SGTR), LOOP and LOMFW.

4.7.2 Assessment

124. As discussed in Section 4.6.2, the TSC and I found that documentation, description, and justification of the event trees in the Level 1 PSA report (Ref. 36) did not meet expectations as it was not easy to trace the safety case from thermal-hydraulic analysis to success criteria, to the event tree models (as discussed in paragraph 117). I raised this matter in RQ-UKHPR1000-0484 (Ref. 66) as well as action 3 of RO-UKHPR1000-0043 (Ref. 57). The RP agreed and argued that this was a documentation matter, rather than an analysis problem. The RP submitted Ref. 69 to provide evidence for their argument. I sampled Ref. 69 and found that the documentation, description, and justification for the two event trees was improved. I found that Ref. 69 provided enough evidence to demonstrate that the RP's argument that this was a documentation problem rather than an analysis problem. This met my expectation for GDA, however, I expect that the PSA event tree documentation will be improved for all event trees in site-specific versions of the PSA reports.

125. I found that the event trees I sampled were constructed well and that they generally met regulatory expectations. As an example, I have presented more detailed comments on one of the event trees, LB-LOCA in the next sub-section. In the rest of the sub-sections I have presented my assessment for my sampled event trees on various aspects of event tree construction and modelling compared with RGP, such as the PSA TAG (Ref. 4).

4.7.2.1 Event Tree End States

126. The RP has defined all ET end states as either core damage ('CD'), success (safe state or 'OK'), or a transfer end-state to a secondary ET to further continue the accident sequence analysis. The definition of success end-states are well defined in Ref. 36. Core damage is defined as the uncovering and heat up of the reactor core to the point at which prolonged oxidation and severe fuel damage involving a large fraction of the core is anticipated, e.g. a severe accident. The criterion used in the thermal-hydraulic analysis supporting the PSA is a fuel cladding peak temperature exceedance of 1204°C. This fuel cladding temperature is explained by the RP to be a useful indicator for the PSA success criteria derivation but is not actually the indication of a severe accident in which case the severe accident engineered measures would be initiated. The indication for operators to initiate the severe accident systems is when the core outlet temperature (COT) is in excess of 650°C. Success is defined as when the system functions and human actions carried out in response to the IE have ensured that the core damage criteria are not exceeded.

127. I compared these definitions to RGP such as IAEA SSG-4 (Ref. 8) and found that these definitions are broadly similar to those in this and other reports. While different projects have slightly different definitions of core damage, the overall definition of success and failure states are usually directly linked to the beginning of a severe accident. Thus, the RP's definition of end states meets my expectations for GDA as compared with RGP.

128. The RP used the end states to further progress analysis in the Level 2 PSA, and assessment of the transfer of core damage end states as well as some success end states (e.g. SGTR) will be discussed later in this report in the Section on Level 2 PSA.

129. I find that the RP's definition and use of accident sequence end states was comparable with RGP and meets my expectations for GDA.

4.7.2.2 Dependencies Modelled in Event Trees

130. The RP has considered different kinds of dependency in the PSA. For event trees, functional dependency is mainly considered, although system dependency resulting from the sharing of support systems by different safety systems is also considered implicitly by combining the fault trees (FTs) with the ETs in the Risk Spectrum model. Other dependency (e.g. human error, common cause failures (CCFs), etc.) are modelled in the FTs, and I have documented my assessment of the RP's consideration of that type of dependency in the appropriate section of this report.

131. Functional dependency among systems was explicitly considered by the RP through the arrangement of the function events in the ET. For example, if the requirement on a certain function is dependent on the failure of another function, then this function is claimed following failure of the first function event. In my sampling assessment, I noted many examples of this. In addition, for ETs that claim a heat removal function by ASG [EFWS] and primary system F&B, I noticed that F&B is only considered in the ETs if the ASG [EFWS] system is considered failed. The ASG [EFWS] system consists of three emergency feedwater pumped trains to extract water from a set of three tanks and inject it into the SGs. The PSA credits this system to provide feedwater in accidents where the secondary cooldown (SCD) function was needed. Many accident scenarios claimed SCD function, and consequently the ASG [EFWS] system as the ASG [EFWS] injected water into the SGs through pipework connected to the main feedwater system. When the ASG [EFWS] system failed, the RP has claimed that F&B is used to remove heat from the reactor core through manual opening of a number of PSVs or manually using the MHSI system to inject water into the primary side. I found that the RP's decision to only claim F&B to function after a failure in ASG [EFWS] was logical and modelled appropriately in my sample.

132. Thus, in my opinion, the RP's functional dependency modelling was clear, it compares favourably with RPG, such as the PSA TAG (Ref. 4) and it meets my expectations for GDA.

4.7.2.3 Initiators in the Event Tree Analysis

133. For some ETs, the RP has used pre-IE small ETs, particularly for loss of support system ETs. Pre-IE small ETs are typically used to model a short sequence of events and if they occur it will lead to the plant conditions that are then represented by the IE. I sampled initiating event – large LOCA (IE_LLOCA_A) which is a pre-IE small ET for the LB-LOCA ET (LLOCA_A). The main purpose of the pre-tree IE_LLOCA_A is to distinguish the break occurring in different locations, or loops of the coolant system. I found that the ET modelling for this pre-tree was functionally correct for the LB-LOCA ET. The RP divided the probability of a LB-LOCA by 3 and assigned this IEF to each of the equally likely pathways to identify the broken loop. The RP uses logic in the risk spectrum model to carry this loop identifier forward, and so for the rest of the ET, if the

break was being modelled on loop 1, support and mitigation systems recognise this flag and function accordingly.

134. In my opinion, the use of pre-trees was performed correctly and met my expectations.

4.7.2.4 Assessment of LB-LOCA Event Tree Modelling and Documentation

135. I sampled the LB-LOCA ET and assessed the event sequence modelling. Although a LB-LOCA does not present a high level of risk in the PSA, ONR assessors in the F&C specialism found gaps in some of the underlying evidence for claims made in the LB-LOCA safety case, which had the potential to lower confidence in the PSA thermal-hydraulic analysis underpinning the ET modelling. I present my assessment of this matter in the following paragraphs.

136. The RP submitted Ref. 70 to ONR, and in this report the RP concluded that a main coolant line (MCL) LB-LOCA could result in internal fuel damage potentially affecting the ability to cool the core. I raised RQ-UKHPR1000-1119 (Ref. 66) to request further information on this matter and to understand any potential effect on the LB-LOCA ET modelling. The RP stated in the response to RQ-UKHPR1000-1119 that much of the analysis in Ref. 70 was not directly applicable to the PSA LB-LOCA ET because the analysis was performed upon a conservative basis.

137. The RP stated that the analysis provided in the Level 1 PSA (see Appendix A of Ref. 36) was supported by PSA specific, best estimate analysis and that this demonstrated that ability to cool the core was maintained in the event of a LB-LOCA with the level of confidence expected for PSA.

138. Subsequently the RP submitted additional analysis reports at the request of the F&C inspector such as Refs 60, 61, 62. The F&C inspector assessed these reports and found weaknesses against the expectations of SAP AV.2 for the LOCUST code validation, as well as several conservatisms. In addition, the F&C inspector noted that the LOCUST did not adequately analyse a phenomenon known as ‘fuel clad ballooning’ (see Ref. 68). As a result of these findings, the F&C inspector raised an Assessment Finding (AF-UKHPR1000-0127) to ensure that a future licensee performs adequate analysis to demonstrate that the core is coolable after a LB-LOCA.

139. I also considered the potential of direct and indirect consequential damage from a LB-LOCA potentially leading to dynamic damage due to pipe whip, steam jets, etc, affecting other loops. In the response to RQ-UKHPR1000-1119 (Ref. 66), the RP argued that according to the analysis results used in support of the PSA in Ref. 36, mitigation functions will still be available after LB-LOCA. Systems used for mitigating a LB-LOCA have three safety trains. The three-train safety systems and three primary loops are arranged within the internal containment separately. Each train and each loop were separated from the others by reinforced concrete structures designed to provide physical segregation. Pipe whip and jet impingement effect will be limited to one train and thus, sufficient SSCs remain available to deliver the safety functions.

140. Within the Level 1 PSA, LB-LOCA is modelled as a break on a high-integrity component, and the small frequency of this IE in the PSA reflects this (2.39×10^{-6} /ry). The CDF from LB-LOCAs is 1.01×10^{-9} /ry and contributes 0.26% towards the overall CDF. Thus, the risk from LB-LOCAs is low in the PSA.

141. My assessment of LB-LOCAs has been undertaken in close cooperation with ONR inspectors from the Fault Studies, F&C, IH, structural integrity (SI) and mechanical engineering (ME) topic areas and I note that ONR has outstanding questions regarding the RP’s conservative bounding analysis. However, I find that the event sequence modelling of LB-LOCA in the PSA to be reasonable and logical. The RP has used the PSA to demonstrate that the risk from LB-LOCAs is low and is a small contributor to

the overall plant risk, and thus, from a PSA perspective, it would not be proportionate to expect the RP to continue to work to further lower the risk in the PSA.

142. Furthermore, in the Level 1 PSA, the RP defined localised fuel damage following a LB-LOCA as a ‘success’ end state. A ‘success’ end state is an accident sequence consequence that is not a severe accident. This is different from an accident sequence ‘core-damage’ end state which assumes widespread fuel damage. Therefore, there is unlikely to be cliff-edge implications for the PSA CDF risk calculation if future deterministic analysis by a licensee is unable to demonstrate with the necessary level of confidence that limited fuel damage will not occur.

143. As a result, in collaboration with other inspectors I have reached a judgement that these matters should not prevent issue of a DAC because the LB-LOCA fault is outside of the design basis, the F&C inspector concludes that a more realistic LB-LOCA analysis may allow a licensee to demonstrate that a coolable geometry will be maintained, and the PSA CDF calculations is expected to be insensitive to any remaining uncertainties in the amount of localised fuel damage.

4.7.3 Strengths

144. In my opinion and in the sample I reviewed, the ETs have been constructed correctly and provide adequate representations of the evolution of the accident sequences following all the IE groups under consideration.

145. The use of pre-IE small ETs is a strength, as cascading logic from the IE contributors to the system FTs is sometimes simplified in RGP. The way that these small ETs were modelled and used properly had led to increased versatility in the ETs that use them.

4.7.4 Outcomes

146. Documentation of the description of the ETs was lacking. The RP demonstrated their capability to adequately document two ETs in Ref. 69, however, this will need to be cascaded out to all future PSA reports.

147. Related to the F&C AR (Ref. 68), the RP has not submitted sufficient evidence to demonstrate adequately to ONR F&C assessors that a LB-LOCA will result in a coolable core. The F&C AR raised AF-UKHPR1000-0127 on this matter.

4.7.5 Conclusion

148. The modelling of the ETs meets RGP and UK regulatory expectations, however documentation of the description of the ETs does not meet expectations as compared with RGP. For GDA, this is acceptable, however the quality of the documentation will need to improve post-GDA as a part of normal business.

149. I sampled the modelling and documentation of the LB-LOCA event tree and found that the modelling met my expectations and that the level of risk was small from this event, however ONR’s F&C assessors raised AF-UKHPR1000-0127 which is related to the RP’s implicit assumption in the ET modelling that the LB-LOCA will result in a coolable core.

4.8 Level 1 and Level 2 PSA: System Analysis

150. The TSC reviewed several UK HPR1000 systems (RIS, ASG [EFWS], DVL [EDSBVS], AC power and DEL) for detailed assessment and compared its consideration in the PSA models with RGP, such as ONR SAPs FA. 13, the PSA TAG (Ref. 4) and IAEA SSG-3 (Ref. 8). I also selected a few systems (EHR [CHRS] and Fuel Building Ventilation System (DWK [FBVS])) to sample in my assessment. In the following sub-sections I present my assessment of the consideration of three of these systems from

our sample within the UK HPR1000 PSA as well as my opinion as to the adequacy of the design of these systems from a PSA perspective. The systems are:

- ASG [EFWS]
- EHR [CHRS]/ In-Vessel Retention (IVR) (although this area of the report is assessment of Level 1 PSA, I have included my assessment of a Level 2 PSA system analysis in this section)
- Fuel Building Ventilation (DWK [FBVS])

4.8.1 Emergency Feedwater System Analysis

151. The ASG [EFWS] system consists of three emergency feedwater pumped trains to extract water from a set of three tanks and inject it into the SGs. The PSA credits this system to provide feedwater in accidents where the Secondary Cooldown (SCD) function is needed. Many accident scenarios claim SCD function, and consequently the ASG [EFWS] system.

152. I have compared the PSA modelling, descriptions, justifications, etc. provided by the RP for the ASG [EFWS] system against guidance outlined in the PSA TAG. The following paragraphs detail my assessment.

153. The RP has provided design description information relevant to the PSA model for the ASG [EFWS] system in Ref. 36 when describing various accident sequences. I found that the descriptions were adequate, although the RP could have linked the descriptions to other GDA submissions which contain much more design detail, such as the system design manuals. However, the description provided was adequate for understanding the FT model of the ASG [EFWS] system.

154. The RP models the ASG [EFWS] system’s failure due to either:

- an operator failure to cross-connect the ASG [EFWS] storage tanks; or
- the system is unavailable due to maintenance; or
- a signal failure leads to a failure to start the system.

155. For some of the accident sequences, a failure of all three trains is required to fail the system function thus the success criteria for these is 1oo3. However, for some more onerous accident scenarios, the FT models 2oo3 success criteria. This is accounted for with distinct fault trees.

156. The ASG [EFWS] system was stated by the RP to be controlled by digital C&I from the Class 1 reactor protection system (RPS) backed up by the Class 2 hardwired Diverse Actuation System (KDS [DAS]). The ASG [EFWS] pumps could be started automatically by the RPS or manually by the operator using KDS [DAS]. For example, in a SB-LOCA, if the pressure in the pressuriser dropped to the ‘PZR low 3’ setpoint, the safety injection signal would be triggered. Medium Pressure Rapid Cooldown (MCD) function was stated by the RP to be performed by the Atmospheric Steam Dump System (VDA [ASDS]) to reduce the primary pressure and temperature. The SG level on the secondary side would then fall, and the ‘SG low 2’ setpoint would trigger the ASG [EFWS] system to begin its function.

157. The ASG [EFWS] system fault tree was modelled in Ref. 36 such that each of the three trains have a probability of being unavailable due to maintenance, and these basic events were assigned a value of 9.84×10^{-4}. This is equivalent to approximately one day per three years. This figure (and all EMIT modelled in Ref. 36) originated with the UK HPR1000 design reference (FCG3) PSA. For GDA and for the PSA, the RP used the FCG3 PSA model EMIT information. It is not stated when the EMIT would take place for ASG [EFWS], but the FT model assumes that this is online maintenance as the unavailability is modelled for full power operating mode.

158. During the GDA, EMIT was assessed in detail across multiple specialisms (including PSA) and RO-UKHPR1000-0021 was raised to ensure the gaps identified were addressed adequately for GDA. As a result of this RO, the RP submitted several analysis reports: Refs. 71 and 72. I assessed parts of these reports where they had potential for affecting the EMIT modelled in the PSA.

159. For the ASG [EFWS] system, the RP presented a different plan for consideration of EMIT in ASG [EFWS] than was originally modelled in Ref. 36. These reports found that EMIT should not be performed on the ASG [EFWS] at power, but only during maintenance cold shutdown, refuelling cold shutdown and Reactor Completely Discharged (RCD) operating modes (i.e. POS D, E and F respectively). It was also noted in these reports that this is inconsistent with how the PSA was modelled in Ref. 36, and that during the next update of the PSA models and reports the new EMIT assumptions would be implemented in the PSA models. In addition, the RP committed to informing ONR of the effect of these changes through Ref. 6.

160. I assessed Ref. 6, Appendix B to understand the impact of these recommended changes to modelling of EMIT on the ASG [EFWS] system in PSA. In Ref. 6 the RP concluded that the results of the internal events Level 1 PSA core damage frequency was not expected to be adversely affected by the introduction of the new EMIT plan for ASG [EFWS]. The RP stated that all of the EMIT for ASG [EFWS] was planned to be performed when the plant was offline, and so unavailability of the ASG [EFWS] system during full power due to maintenance is no longer required to be considered in the PSA model. Thus, it was expected by the RP that the calculated reliability of the ASG [EFWS] system should be slightly improved than what was calculated in Ref. 36. As the ASG [EFWS] system was not required for shutdown operating modes, the EMIT plan was expected to have no effect on low power or shutdown PSA.

161. I assessed the HRA modelling present in the ASG [EFWS] system fault trees. The UK HPR1000 design considers human actions that are necessary during accidents for mitigation. In addition, there are some human actions that can result in an initiating event, in effect causing an accident to begin. As PSA is expected to cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults, human error is expected to be included as HRA. In general, the probability of failure of operator actions is modelled within fault trees as basic events and are assigned Human Error Probabilities (HEPs). I have presented my assessment of how the RP has used HRA in the UK HPR1000 PSA in Section 4.9 of this report, and more detail can be found there, however, I have presented my specific assessment of the HRA for the ASG [EFWS] system modelling in the following paragraphs for the purposes of my assessment of system analysis.

162. The system is dependent on manual operator actions. There are two operator actions that are required for the ASG [EFWS] system to perform its function successfully:

- Operator action to manually restart secondary cooldown following a number of different IEs (OP_ASG_S). This operator action is credited in a number of scenarios during POS C (LOCC, LOOP, SLOCA, etc.), however it is not risk-important.
- Operator action to cross-connect the ASG [EFWS] water supply tanks (OP_ASG_LINK). This operator action is risk-important, and thus I have included it in my sampling assessment as detailed in the next paragraphs.

163. The RP models manual operator action to cross-connect the three ASG [EFWS] tanks. The RP clearly identifies this operator action as opening two manual valves during a time limit of 1 hour. Opening these two valves will cross connect all three ASG [EFWS] tanks to provide water to a common header, from which the pumped trains obtain water from. This HEP is assigned a value of 2.1×10^{-3} (for more information on my general assessment of calculating HEPs, see Section 4.9 of this report). It is also

explained that a single ASG [EFWS] tank's inventory cannot satisfy the core cooling success criteria from full-power shutdown mode to RHR subsystem connection to the reactor coolant primary circuit. I raised RQ-UKHPR1000-0253 (Ref. 66) to gain further understanding into this operator action. The RP explained in the response to RQ-0253 that this operator action is a local field action, and that although in reality the volume of two tanks is likely to be sufficient, due to the uncertainty in this operator action, they have modelled all three tanks as being necessary until a stable safe state can be reached.

164. In addition to the system modelling in the Level 1 PSA, the design of the ASG [EFWS] system is generally quite simple and logical, and I am content in its viability. There was one feature of the system that I required more information for, and this was regarding the design of the multiple tanks for storage of water. In RQ-UKHPR1000-0253, I asked the RP to explain how the risk from the design of the system had been reduced to ALARP, as it seemed that a system with a single tank would be more reliable and thus reduce risk. The RP stated that that the inventory for the ASG [EFWS] (in however many tanks) is required to be in the RB, so as to minimise further containment penetrations. In addition, three tanks are required, as the volume of water that is required for the ASG [EFWS] system to fulfil its safety function is quite high. In RQ-UKHPR1000-0310 (Ref. 66), the RP stated that the required inventory would be approximately 1000 tonnes of water, and the three combined tanks provide 1530 tonnes. Thus, the RP claimed that a single tank for this size would not fit in the confines of the RB and so three smaller tanks were designed instead.

165. In the response to RQ-UKHPR1000-0253, the RP also addresses why it decided to make the cross-connect of the three tanks a manual field operation, rather than a MCR operation or an automated operation. The RP provided their calculations, which show that the reliability of the system does not improve substantially by making this automated, or an MCR action. I assessed these arguments and calculations and found them to be reasonable and calculated correctly.

166. The RP stated that the operator action to cross-connect the ASG [EFWS] tanks is modelled conservatively in the PSA because although the model assumes that all three tanks must be cross-connected, the volume of only two will be sufficient to provide enough inventory for the system. In addition, the operator action is claimed in all POS in the PSA, whereas in POS other than POS A, there will be enough inventory for a single tank to provide cooling. The RP also provided their optioneering study results which demonstrated how the design for three tanks was arrived at, and why the final design is the ALARP option. The RP claimed that the final design has low risk-importance and is balanced with a high degree of redundancy compared with the other design options.

167. In Ref. 73, the ASG [EFWS] system analysis report for PSA, the RP states that the system unreliability was found to be 1.77×10^{-5}. The most important failure event for the ASG [EFWS] system is a CCF of the three flow sensors, which contribute 54.64% to the overall unreliability of the system. Whilst ASG [EFWS] appears in the 19th most frequent MCS, ASG [EFWS] does not contribute significantly to the UK HPR1000 risk profile, therefore any improvements made in reliability would not significantly affect overall risk.

168. From a PSA perspective, I found that the design of the ASG [EFWS] system to be fit for purpose. Although it is possible the risk could be reduced with a large single tank, the RP demonstrated that this would not be possible due to the layout of the reactor building. The PSA modelling shows that the risk from the design of the ASG [EFWS] is already low. The RP have provided these arguments to ONR to demonstrate the claim that the design is ALARP. I assessed these arguments and the PSA modelling of the ASG [EFWS] system and found them to be adequate. Although these findings are limited to the ASG [EFWS] system analysis, if the system analysis outside of my

sample was of similar adequacy to the ASG [EFWS] system analysis, the PSA insights for the design as a whole would be further validated.

4.8.2 Containment Heat Removal System Analysis

169. The EHR [CHRS] system has two main safety roles: to prevent containment overpressure failure by spraying water inside the containment building; and to support (via the reactor pit flooding system) IVR of a melted core inside the RPV during a severe accident. Success of the IVR function should prevent ex-vessel steam explosions, molten corium concrete interactions (MCCI) and direct containment heating (DCH), and therefore help to maintain the integrity of the containment building (see Ref. 74 for more details on the design description).

170. The Level 2 PSA credits the EHR [CHRS] system in many Level 2 PSA accident progression event trees and is an important contributor to the Level 2 PSA results. Thus, I selected this system to assess during GDA as it is risk-important.

171. I have compared the PSA modelling, descriptions, and justifications provided by the RP for the EHR [CHRS] system against RGP such as IAEA SSG-3 (Ref. 8) and the ASME Level 1 PRA Standard (Ref. 17). Although the EHR [CHRS] system is only modelled in the Level 2 PSA, the fault tree modelling follows standard Level 1 PSA techniques. Thus, I have referred to Level 1 PSA RGP to compare the fault tree modelling of this system against.

172. The RP has provided design description information relevant to the PSA model for the EHR [CHRS] system in Ref. 42. I found the descriptions to be adequate, although the RP could have linked the linked the descriptions to submissions which contain much more design detail, such as the SDMs (such as Ref. 75). However, the description provided was adequate for understanding the FT model of the system.

173. The containment cooling spray function of the EHR [CHRS] system contains two trains, each containing an intake line from the In-Containment Refuelling Water Storage Tank (IRWST), a pump, a heat exchanger, and the spray line. The RP states that the success criteria are that at least one train is sufficient to cool the containment for all accident sequences, both for the short term and the long term mission times.

174. The EHR [CHRS] containment cooling spray system is controlled manually by MCR operator action (see Ref. 75). When the containment pressure exceeds the ‘high-high’ setpoint, the operator will signal the motorised isolation valves to open, and for the heat removal pump to start.

175. The reactor pit injection function of the EHR [CHRS] system contains two active trains each of which are physically separated and contain a pump, heat exchanger and pipework. Much of the EHR [CHRS] system is shared for the sprays and the reactor pit injection system, including the EHR [CHRS] heat exchangers and the EHR [CHRS] pumps. There are also two passive trains of the EHR [CHRS] reactor pit injection system separated from the active trains for part of the system (up to the isolation valve, which are shared between the active and passive systems). At the beginning of the mission, the system operates passively, by pulling water through gravity and injecting into the reactor pit, after a set of motorised isolation valves are automatically opened after the core temperature high outflow set point reaches 650°C. After a certain amount of time, the water inventory in the reactor flooding tank will be low and the operator must begin the active phase of operation to pump water from the IRWST to the reactor pit. The RP states that the success criteria is that one train is sufficient to provide reactor pit inventory fast enough to keep the RPV intact (both for the passive and active phase).

176. The EHR [CHRS] reactor pit injection system uses the Safety Automation System (SAS) platform and the Core Cooling Monitoring Cabinet (CCMC) for the containment heat removal function, and the Severe Accident C&I System (KDA) and CCMC for the IVR function. Operator action is integral to the control of the system responding to the information displaced in the MCR during a severe accident. For the reactor pit injection function, the failure of the operator action to manually switch from passive mode to active mode accounts for a significant proportion of the unreliability of the system (36.06% of the total unreliability).

177. The fault tree models the C&I systems that control the EHR [CHRS] injection isolation valves somewhat simplistically. The sensors are all modelled as basic events, however further logic and cabinet hardware are modelled as supercomponents. Modelling of the C&I throughout the PSA was the subject of an RO that I raised (RO-UKHPR1000-0013 (Ref. 57)) and I have assessed this aspect of the PSA in Section 4.10 of this report.

178. The EHR [CHRS] system is stated in Ref. 42 that all EMIT will take place during cold shutdown operating mode (POS-F), when the system is not required to function. I observed that the system model for EHR [CHRS] reflects this EMIT requirement, as EHR [CHRS] is not claimed in the Level 2 PSA for POS-F. Thus, I consider the modelling of EMIT to be appropriate for the EHR [CHRS] system analysis.

179. I assessed the HRA modelling present in the EHR [CHRS] system fault trees. The system has a mix of manual and automatic functions; however, operator errors tend to dominate the unreliability of the system. The most risk important human action claimed for the EHR [CHRS] system is for the operator to start the sprays manually to control the containment pressure (OP_L2_EHR [CHRS]3). The HEP calculated for this operator error is 5.24×10^{-2} while the Fussell Vesely (FV) importance for the LRF is less than 0.05, and thus is not very risk important overall. I found that the RP explained this operator action well and presented the claimed minimum time for the different required activities. This operator action was also subject to dependency analysis together with OP_L2_EUF, the operator failure to start the Containment Filtration and Exhaust System (EUF [CFES]). The RP found that a moderate level of dependency exists between these two operator errors, and thus OP_L2_EUF was adjusted to raise its initial probability of failure to be $\sim 1 \times 10^{-1}$ to account for this. I found this to be an adequate judgement of the dependency analysis for these two operator actions.

180. One of the matters that arose while assessing the EHR [CHRS] was found in discussions with the SI, Fault Studies and SAA inspectors. It did not appear that the RP had analysed a spurious operation of the EHR [CHRS] system leading to injection of water into the reactor pit at full power. ONR was concerned that the RP had not addressed either the fault analysis or consequences of this accident scenario in the safety case. This led to a number of RQs (for example RQ-UKHPR1000-0224 (Ref. 66)) and discussions with the RP. RO-UKHPR1000-0032 (Ref. 57) was raised to ensure the gaps identified in the safety case related to this matter were resolved during GDA. In this report I will discuss the probabilistic aspects of this RO resolution, whilst the deterministic aspects are discussed in the SAA and SI ARs (Refs 63 and 76)

181. To demonstrate that the risk was ALARP from a probabilistic viewpoint, the RP submitted new PSA modelling and an optioneering report (Ref. 77). The RP found that there were two ways to inject water inadvertently to the reactor pit at full power, an active pathway, and a passive pathway.

182. For the active pathway, the RP found that this could only occur if during a 1 hour proof test of a pump, several isolation valves in series spuriously opened or leaked. The RP found that this accident sequence would not be able to provide enough water during the 1 hour test interval to reach the bottom of the RPV. Thus, this accident pathway was screened out of further analysis in the Level 2 PSA. I found this decision to screen out the accident pathway from the Level 2 PSA model to be reasonable.

183. The RP found that for a passive inadvertent injection to the reactor pit, several valves in series would need to open spuriously or leak and then due to the design of the gravity driven feed tank, water could inject to the reactor pit. After completing fault tree analysis, the RP demonstrated that the frequency of this accident scenario was likely less than 1x10^{-8} /ry. I assessed this model and found it to be adequate.

184. The resolution from RO-UKHPR1000-0032 was that the Level 2 PSA modelling of the EHR [CHRS] needed to be modified in the next update to include this accident scenario as a normal business item. In my opinion, the original gap that was identified of an absence of analysing the spurious operation of the EHR [CHRS] system to inject to the RPV was adequately addressed by the work that the RP performed to respond to this RO.

185. Overall, I found that the design of the EHR [CHRS] system to be fit for purpose. I found the PSA system analysis of the EHR [CHRS] system to be adequate. If the system analysis outside of my sample was of similar adequacy to the EHR [CHRS] system analysis, the PSA insights for the design as a whole would be further validated.

4.8.3 Fuel Building Ventilation System Analysis in SFP PSA

186. In the SFP PSA, I assessed the system analysis for the most risk important system, DWK [FBVS]. Failure of this system accounted for 58.1% of the total thermal fuel damage frequency (FDF-T). The RP described thermal fuel damage as the exposure of bulk quantities of spent fuel in the SFP and subsequent damaged due to a loss of SFP cooling and loss of SFP inventory. More information on this accident scenario can be found in my assessment of the SFP PSA in Section 4.13 of this report.

187. The DWK [FBVS] depends on the safety chilled water system (DEL) for providing cooling water to the heat exchanger/chillers in the DWK [FBVS] ventilation system. The Fuel Pool Cooling and Treatment System (PTR) [FPCTS] depends on the DWK [FBVS] to provide cooling for the PTR [FPCTS] heat exchanger. Each train of the DWK [FBVS] is modelled as having identically design fans, and other sub-components. Thus, CCF of the similar components across all of the trains dominates the unreliability of this system. Loss of DWK [FBVS] is considered as in IE in the SFP PSA, and the frequency of this IE is modelled via a detailed system fault tree. A CCF of the DWK [FBVS] fans for the PTR [FPCTS] pump room leads directly to failure of all PTR [FPCTS] pump room recirculation units, requiring manual intervention to provide makeup water to the SFP to prevent the eventual uncovery of the fuel and thermal damage. This basic event is the most risk important event in the SFP PSA. The most dominant cutset in the SFP PSA is a combination of an IE of a loss of DWK [FBVS] leading to failure of the PTR, followed by a failure of the manual makeup measures. This sequence of events dominates the results for the SFP PSA thermal fuel damage by a contribution of 53.5%.

188. I observed that the risk profile of the DWK [FBVS] system was relatively high. Although the accident sequences have a low frequency leading to thermal fuel damage of the SFP, the risk profile is not balanced, as expected in SAP FA.10. In addition, to reduce the frequency of this accident scenario, the RP has depended upon significant operator intervention to provide makeup to the SFP. The RP has examined these in dependency analysis and notes that there is a dependency between these actions.

189. I raised RQ-UKHPR1000-0485 and RQ-UKHPR1000-0849 to discuss my assessment of the SFP PSA modelling. As a result of the PSA analysis of this system and ONR discussions with the RP, the RP decided to modify the DWK [FBVS] system to increase diversity and redundancy across the entire Heating, Ventilation and Air Conditioning (HVAC) systems via MOD 35 (HVAC diversity – Ref. 78). The RP committed to include these changes in DR3. I checked this in the UK HPR1000 Design

Reference Report (Ref. 97) and confirmed the system changes were implemented in DR3 as proposed.

190. In Ref.6, the RP has analysed the effect of these HVAC modifications that were agreed to during GDA and it was demonstrated that the contribution of the HVAC systems to the overall risk of the plant has been significantly reduced. The RP is expected to update the PSA models to reflect design changes such as these as a normal business item post-GDA, however for GDA, I found that the RP adequately demonstrated that the risk was reduced when these modifications were considered.

191. I am content with the system analysis for the DWK [FBVS] system, and with the modified design. The increased redundancy and diversity of many of the HVAC systems, including DWK [FBVS] leads to a reduction in the risk. The modelling of the DWK [FBVS] system in the SFP PSA was performed well compared with RGP, however it will need to be updated in future PSA revisions to adequately reflect the modified design as a part of normal business.

4.8.4 Strengths

192. For the systems that I sampled, the RP has analysed and modelled these systems well in the PSA.

193. The RP submitted evidence showing that the PSA was used to understand areas of risk that could be reduced. This resulted in design changes during GDA which were then demonstrated to have reduced the risk arising from the design.

4.8.5 Outcomes

194. My assessment of the RP’s submissions on Level 1 PSA system analysis against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.8.6 Conclusion

195. In my opinion, the FT modelling, system analysis and design of the ASG [EFWS], EHR [CHRS] and DWK [FBVS] systems was adequate for GDA compared with my expectations. These systems contained a broad spectrum of modelling techniques, including CCF, HRA, support systems, etc. and thus are a good representation of the overall system analysis modelling in the Level 1, Level 2 and SFP PSA. I have confidence that the adequate modelling of the three systems I sampled provide insight into the PSA modelling of the rest of the systems across the UK HPR1000 design. I am content in the manner in which the RP used PSA to inform the design of areas of highest risk and potential design improvement.

4.9 Level 1 PSA: Human Reliability Analysis

4.9.1 Introduction to Assessment of Human Reliability Analysis

196. The UK HPR1000 design considers significant human actions that are necessary during accidents for mitigation. In addition, there are some human actions that can result in an initiating event, in effect causing an accident to begin. As PSA is expected to cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults, human error is expected to be included as HRA.

197. The UK HPR1000 PSA includes consideration of human errors in the various PSA models. The RP based their approach (Ref. 23) for modelling human error in PSA on Refs. 8 and 17. These references contain the three approaches used in this PSA (Accident Sequence Evaluation Program (ASEP), Technique for Human Error Rate

Prediction (THERP) and Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H)).

198. The RP has considered three types of human failure events (HFEs):

- Pre-IE HFEs (Type-A)
- Human failure events (HFEs) that lead to IEs (Type-B)
- Post-IE HFEs (Type-C)

199. For Type-A, Type-B and Type-C HFEs, the RP has used ASEP, THERP and SPAR-H respectively to calculate the HEP. These HEPs are then assigned to different basic events in the PSA models (usually in FTs, although the few Type-B HEPs are modelled in ETs).

200. The RP has summarised the analysis, justification, and results in Ref. 38.

201. In addition to my assessment of the HRA modelling and documentation, I viewed several videos of some of the operator actions. I found this to be useful to understand some of the high level assumptions in the PSA and to gain confidence in the RP's capability to perform simulations and accident drills with the simulated MCR.

4.9.2 Assessment of HRA

202. The TSC assessed the RP's approach and modelling of HRA in the UK HPR1000 PSA and provided advice and feedback. I also assessed this and with the TSC's input, I found gaps in the justification of the approaches used, the sources of data for calculating the HEPs and the demonstration that the numbers were appropriate for use in the UK. I raised questions on these potential gaps with RQ-UKHPR1000-0227, RQ-UKHPR1000-0236, RQ-UKHPR1000-0253, RQ-UKHPR1000-0254, RQ-UKHPR1000-0484, RQ-UKHPR1000-0485 and RQ-UKHPR1000-1022 (Ref. 66).

203. Following parallel reviews of the RQ responses, both the TSC and I were of the view that there remained a gap in the RP's approach and modelling of HRA with respect to the justification of the sources of data used and approaches used compared with RGP such as the PSA TAG (Ref. 4) and USNRC NUREG/CR-1278 (Ref. 9). Thus, I raised RO-UKHPR1000-0018 (Ref. 57) to address the gaps against regulatory expectations and the RP responded with updated versions of Refs 23 and 38. I have discussed this gap and the RP's response to the RO in the following sub-sections.

204. I have assessed the RP's approach for calculating HRA and their calculations for deriving the HEPs in the following sub-sections.

4.9.2.1 HRA Approach

205. The RP's primary justification that the three HRA approaches (ASEP, THERP and SPAR-H) are appropriate for use in the UK to estimate the HEP is that these methods meet RGP expectations outlined in NUREG/CR-4772, NUREC/CR-1278, NUREG/CR-6928 (Ref. 8) and the ASME Level 1 PRA Standard (Ref. 17).

206. In my opinion, the RP's argument is logical; as these techniques are broadly used internationally for calculating HEPs in PSA it is reasonable that they are used for PSA in for the UK HPR1000. It is also noted that the techniques are comparable to those commonly used by licensees in the UK.

207. In addition to using the three HRA approaches to calculate HEPs, the RP has also performed dependency analysis to determine the level of dependency between various HEPs. The basic approach for dependency analysis is to first identify if there are possible groups of HEPs in the cutsets of the PSA results. When the RP determined all of the possible dependency groups, they then used the SPAR-H recommended

approach for determining the level of dependency, and thus what HEP to assign to the basic events in the PSA model. This SPAR-H method depends on assigning values to four variables (same work crew, same time, same location, and cues). The dependency of one operator action on a previous one can then be determined based on these variables (e.g. if the crew was the same, if the time between both actions was similar, if the location is the same and if there are any visual clues to alert the operators of a problem).

208. The RP described how they would use this approach and presented their justifcation for using it in Ref. 23.

209. In my opinion, the expectations established in the SAPs (Ref. 2) and PSA TAG (Ref. 4) are met.

4.9.2.2 HRA Quantification

210. The RP has listed all input variables used to calculate HEPs in Ref. 38 along with justification arguments for why the sources of the inputs variables are appropriate for use in the UK.

211. The TSC and I sampled several HEPs from all types of the HRA (Type A, Type B and Type C) and was able to trace the golden thread of substantiation easily. The claims, arguments and evidence are supported by adequate substantation for GDA. The HEPs that were sampled included all types and for different POS:

- I&C-SG-1731MN_EC, Type A error, operator accidently sets Main Feedwater Flow Control System (ARE [MFFCS]) sensor to wrong setting prior to an initiating event.
- OPB_RHR_TR3, Type B error, operator fails to start RHR train 3 manually.
- OP_FB_SGTR_A-1, Type C error, operator performs F&B after an SGTR accident when MCD fails, however the damaged SG is successfully isolated.
- OP_ASG_S_SLOCA_C-1, Type C error, operator manually starts SCD after a SB-LOCA, with MHSI success and RHR recovery failure.
- OP_RHR_S1_SLOCA_D, Type C error, during POS D, operator manually starts RIS-RHR after a SB-LOCA with MHSI success.
- OP_MCR_A, Type C error, after a loss of DCL [MCRACS] HVAC, field operator manually starts local backup air conditioners.
- OP_ASG2_LINK, Type C error, during SCD, upon failure of ASG [EFWS] tank B, operator connects other ASG [EFWS] tanks manually by opening two valves.

212. To assess the HEP calculations, the TSC and I sampled the above HEPs and using the input data, I was able to reproduce the HEPs. For each of the HEPs in my sample, I reviewed the selected choices of the Performance Shaping Factors (PSFs) and the justification provided for selection of the PSFs and found them to be adequate.

213. Although I was able to reproduce the sampled HEPs, I observed limitations in the task decomposition and qualitative analysis including gaps in documentation. I reviewed Ref. 38 collaboratively with the ONR HF inspector to determine if the human based safety claims were adequately underpinned by qualitative analysis and whether it was adequate for GDA. The TSC and I sampled some of the HBSCs related to the above group of sampled HEPs. I observed that Ref. 38 was well presented and has adequately demonstrated the validity of the human reliability quantification. However, I observed a minor shortfall on the linkage to detailed task analysis, which was not adequately demonstrated. As qualitative HRA and detailed task analysis is outside the scope of this report, assessment of these topics can be found in the HF assessment report (Ref. 79).

4.9.2.3 HRA Dependency Calculations

214. If two or more operator actions claimed in any accident sequence in the Level 1 PSA, there is the potential that the failure of the first operator action claimed in the accident sequence could result in a consequential failure of the second or other operator actions in the sequence. Normally, the second or tertiary operator action, if found to be partially or fully dependent on the first operator action will have their probability changed to a higher value to reflect the fact that the first operator failure affects them. This is termed 'dependency analysis'. Before assigning a probability value for HEPs into the PSA model, the RP performed dependency analysis.

215. The RP determined that there were no dependent sets of Type-A HEPs because they were due to failures during independent EMIT activities. The RP argued that it was not logical for two or more Type A operator failures (such as calibrating a sensor to a wrong setting) to depend on each other when the work to set and test sensors, for example, is performed by different crews and separated by extensive time between EMIT activities. I found the RP's reasoning for Type-A dependency calculations found in Ref. 38 and to be logical and met expectations as outlined in the PSA TAG (Ref. 4).

216. The RP determined in Ref. 38 that there were no dependent sets of Type-B HEPs because there were no sets of Type-B errors. As Type-B errors lead to IEs, they are all analysed individually, rather than in a set. I reviewed the RP's argument and found it to be reasonable for Type-B HEPs.

217. In Ref. 38, the RP reported several sets of potentially dependent Type-C HEPs and conducted dependency analysis on each of these sets. As a result, several values were changed in the PSA model for those HEPs found to be dependent to reflect the increased probability of failure of the subsequent HEPs in a set after the initial human error. I assessed a few of the Type-C HEP dependency calculations and found them to meet ONR expectations.

218. In Ref. 38, the RP also performed inter-type dependency analysis (for example Type-A-Type B, etc) and did not find any applicable dependent sets. I assessed the RP's arguments and am content with their findings.

219. My assessment of the dependency calculations found that the RP quantification of HEP dependency met regulatory expectations as outlined in the PSA TAG (Ref. 4) and thus was adequate.

4.9.2.4 Risk Important HEPs

220. In Ref. 36, the RP has presented a summary of the top 20 HEPs in the internal events Level 1 PSA. I sampled some of the most risk important HEPs and my assessment of the calculation of the HEPs, the documentation of the calculations and the RP's ALARP discussion is discussed in the following paragraphs.

Operator Manually Performs Feed & Bleed (OP_FB_RT_A)

221. The RP notes that the operator action to manually perform feed & bleed (F&B) after a general transient IE during full power operation (OP_FB_RT_A) is one of the most risk-important (i.e. the PSA results are highly sensitive to the value) human actions credited in the Internal Events Level 1 PSA. It is assigned a probability of failure of $3.0x10^{-2}$ and has a FV importance of $8.09x10^{-2}$. I reviewed the HEP calculations including the assignment of the PSFs that the RP presented in Ref. 38 and found them to be sensibly selected, and that the accompanying documentation for the reasons for selecting the PSFs was adequate.

222. In Ref. 38, the RP explained the high risk importance of this operator action is due to the fact that the Level 1 PSA primary system transient IE has a relatively high

frequency. The UK HPR1000 primary system transient IE frequency was calculated by combining the frequencies of several different PIEs which all result in the same plant response such as RCCA failures, boron concentration failures, pressuriser failure leading to increased primary side pressure, etc. In addition, if the MCD and SCD functions fail and if the ASP [SPHRS] fails, manual operation of F&B is the only way to decrease the pressure of primary coolant loop. I reviewed the minimal cutset list and found that the RP's claims were traceable and thus, the reason for the high risk importance was reasonable.

223. I found the HEP calculation to meet ONR expectations compared with the PSA TAG (Ref. 4), the PSFs justified adequately, and the high risk-importance explained and justified adequately. Thus, the HEP modelling of OP_FB_RT_A met ONR expectations compared with RGP.

Operator Manually Cross-Connects ASG [EFWS] Tanks (OP_ASG*)

224. The RP also noted that there are three operator actions credited in the PSA to cross-connect the three ASG [EFWS] tanks (OP_ASG1_LINK, OP_ASG2_LINK and OP_ASG3_LINK – one operator action to connect tanks for each SG). More information regarding the design of the ASG [EFWS] can be found in this report in Section 4.8.1. These three actions are modelled as mutually exclusive events in the FTs, and thus completely independent events. I raised RQ-UKHPR1000-0253 (Ref. 66) to gain more insight into this operator action. The RP clarified that these three basic events are used to model the cross-linking of all three tanks, and only one is claimed in any single accident sequence. For example, if the fault was on SG1, OP_ASG1_LINK would be used, and this would represent the situation when the water level of ASG [EFWS] Tank 1 decreases to "low-3" alarm level and then Tank 2 (or Tank 3) is required to cross-connect to the ASG [EFWS] Pump 1. The operator will open the isolation valves 1&2 (or isolation valves 1&3). The RP claimed that although there are three tanks in the design, in reality, it is likely that the inventory from only two tanks will contain sufficient volume for a 24 hour mission time. Thus, the RP claimed that the PSA modelling is conservative.

225. These three operator actions are assigned a probability of failure of $1.2x10^{-2}$ and have a FV importance of $3.64x10^{-2}$. In Ref. 36 and Ref. 38, the RP has presented a description and justification for how this HEP was assigned. In addition, the relatively high FV for these operator actions is explained by the RP to be due to the fact that ASG [EFWS] is credited in many cutsets, and if the operator action to cross-link the ASG [EFWS] tanks fails, ASG [EFWS] will fail.

226. I assessed the calculation of the HEP for this operator action in Ref. 38, as well as the documentation for the selection of the PSFs, and the discussion for the risk-importance of this operator action. I also reviewed the minimal cutset list and noted the accident scenarios in which this operator action is claimed. In my opinion, the HEP calculation was performed correctly, and the RP's justification and documentation was adequate. Thus, in my opinion, I found the consideration of this operator action meets my expectations compared with RGP.

Operator Starts up Portable Air Conditioner Manually after LODCL Accident (OP_MCR_A)

227. The RP credits the operator with using portable air condition units manually in the MCR after a LODCL accident. This operator action is assigned an HEP of $3x10^{-4}$ and is a relatively high contributor in the Level 1 PSA, due to the fact that failure of the DCL [MCRACS] has a relatively high IEF ($5.71x10^{-2}$ /ry), and the operator action to start up the manual A/C units is required following this IE. The RP provides good description and substantiation for this operator action in the internal events Level 1 PSA report

(Ref. 36). I could follow the calculation of the HEP and the human based safety claims (HBSCs) chosen were reasonable.

228. The RP has included the DCL [MCRACS] system in modification M-35 (Ref. 78) and the system diversity has been improved. In Ref. 6, the RP assessed the effect on the PSA results due to modification M-35 and the contribution to the CDF from IE-LODCL is decreased from 1.59×10^{-8} /ry to 1.34×10^{-8} /ry (an improvement of more than 15%). Although the probability of OP_MCR_A does not change, the importance of the operator action is decreased from most important, to 9th most important. The HEP in Ref. 6 has an FV importance of 2.19×10^{-2} and is thus not risk significant after modification M-35.

229. After reviewing the derivation of the HEP for OP_MCR_A, including the justification for the PSFs and the calculation of the HEP, I am content that the RP has calculated this HEP correctly, provided adequate documentation and justification for the PSFs and discussed the risk-importance of this HEP adequately. In addition, during GDA, the RP has demonstrated that they have lowered the risk from this HEP significantly and, in my opinion, it would not be proportionate to further reduce the risk.

Overall HRA Results in Level 1 PSA

230. The RP submitted an HRA summary report (Ref. 80) which presented several tables in which all of the HEPs were set to 1, 0.1, 0.01 and 0.001. The following table shows the effect of this sensitivity study on the CDF and LRF.

Table 6: HRA Sensitivity

HEPs Value	CDF /ry	LRF /ry
1	1.3	1.21
0.1	2.63×10^{-3}	7.26×10^{-4}
0.01	1.70×10^{-6}	2.09×10^{-7}
0.001	2.92×10^{-7}	4.84×10^{-8}

231. Although this was a simple sensitivity study, it provides further risk insight that this design is sensitive to operator actions, like most NPPs. Although design rules and modern standards are effective in reducing the reliance on operators, they remain important, and it is an example of why it is important for the RP to have performed detailed HRA in the Level 1, Level 2 and SFP PSA, and that operators are trained to minimise the risk of failure. Although this sub-section is related to Level 1 PSA, the lessons apply across to the Level 2 PSA and SFP PSA.

232. In my opinion, however, the RP has used acceptable approaches for deriving the HEPs; adequate descriptions and justifications for calculating the HEPs; and has modelled the HRA adequately for GDA.

4.9.3 Strengths

233. The RP has provided substantiation for the techniques used in calculating HEPs.

234. The RP has provided an adequate demonstration of the level of risk arising from claimed operator actions in the design.

4.9.4 Outcomes

235. Timings used in the HRA calculations are as yet based on assumptions, and the underlying qualitative, realistic understanding of the operator actions is still largely theoretical.

236. The underpinning qualitative understanding of the operator actions is largely absent from the safety case. For GDA, this is acceptable, but it will require a significant effort post-GDA to improve the analysis.

4.9.5 Conclusion

237. In my opinion, the consideration of HRA in the PSA for the UK HPR1000 GDA is adequate, however the qualitative analysis underpinning the HEP calculations will need to be further developed during site-specific design. The HF AR (Ref. 79) contains the assessment of the qualitative HRA as it is outside the scope of PSA.

4.10 Level 1 PSA: C&I

4.10.1 Background

238. Early in Step 3 the review of the methodology for internal events Level 1 PSA Rev A (Ref. 29) was conducted with the support of the ONR PSA TSC and queries were raised through RQ-UKHPR1000-0026 (Ref. 66) to seek clarity on the C&I modelling. The response indicated that the approach to C&I modelling in the PSA was to use simplified modelling with very limited representation of the hardware and software failure of the C&I systems used. The effect of this approach to modelling had two notable outcomes namely:

- The contribution of the C&I systems to plant risk appeared to be insignificant.
- The models of the C&I systems had no aspect of incorporation of software failures.

239. This aspect was identified as a significant matter at the end of Step 3 and therefore I raised RO-UKHPR1000-0013 (Ref. 57) at the beginning of Step 4.

240. At the beginning of Step 4, ONR identified a number of specific matters in RO-UKHPR1000-0013 related to C&I system modelling in UK HPR1000 PSA for GDA:

- lack of holistic identification of computer-based systems and components to be modelled in the PSA;
- need to explain on how these will be modelled in the PSA;
- justification of the source of data to be used in estimating the computer-based system reliability and demonstration that it is suitably underpinned;
- justification of the relevant standards applied and how the methodology follows industry-accepted practices;
- dependency modelling (between systems and between components and subsystems within the same system) needed to be identified and explicitly addressed by the analysis; and
- approach to give due consideration to the factors that could lead to common cause failures of computer-based systems

241. In response to RO-UKHPR1000-0013, the RP produced a new methodology for modelling C&I systems in the UK HPR1000 PSA (Ref. 30) and the application of the methodology to a sample of safety significant C&I systems to demonstrate the veracity of methodology (Ref. 81).

4.10.2 Assessment of Level 1 PSA: C&I

242. The key SAP (Ref. 2) applied within my assessment is SAPs FA. 13 on ‘adequate representation of the site’, and the associated TAG-30 (Ref. 4). In addition, I have judged against the paragraph 657 of the SAPs, which states “When models are used for the calculations of input probabilities, for example in human errors or failures of computer-based systems (including software errors), common cause failures, or the failures of structures, then the methodologies used should be justified, and should account for all the key influencing factors.”

243. During Step 4 of GDA, while the work of resolving the RO was ongoing, I proactively engaged with the RP and the RP’s UK contractor. The RP’s UK contractor was tasked to provide advice relating to the gap associated with RO-UKHPR1000-0013 and to assist in the production of the methodology. The ONR C&I inspector and I assessed the progress of work, direction of travel and the depth of the planned work to address RO-UKHPR1000-0013. I found that the discussion provided me confidence in the RP’s approach for the methodology and implementation in the case studies informed by both deterministic and probabilistic analyses RGP contained in IEC 61508 (Ref. 10), IEC 61360 (Ref. 11), IEC 62340 (Ref. 12) and NUREG CR/6303 and 7007 (Ref. 9).

244. My assessment of the methodology provided me confidence on the approach and the details presented based on the following observations.

- The methodology provided a comprehensive listing of all the centralised computer-based C&I systems.
- From the overall list, it presented a complete list of the systems that are part of the modelling of the Level 1 and Level 2 PSAs (although this sub-section relates to my assessment of the Level 1 PSA, the findings are also applicable to the Level 2 PSA for FT system modelling as the technique is identical).
- The methodology listed the various failure modes pertaining to hardware and systematic failures based on international electrotechnical commission (IEC) standards and how these failures would be modelled as ‘basic events’ in the PSA.
- Software failure modes are comprehensively identified, and the methodology to model the same is proposed including appropriate sensitivity analysis. The basis of this approach is aligned to RGP based on IEC standards.
- The methodology for identification of potential CCF susceptibilities and eventual modelling in the PSA is proposed. This also included a discussion on the various parametric methods for incorporating the CCFs in PSA model and a conclusion on the most appropriate method. A summary table was provided based on the justifications in the report for the various specific modelling applied to CCFs for each of the component types.
- A comprehensive review of the data sources for the component failures, software failures, and CCF parameters is made. The most appropriate choices are proposed along with the justification and compared with RGP.

245. In my opinion this approach is acceptable and meets the regulatory expectations of SAPs FA. 13 and paragraph 657 of the SAPs.

246. In addition to the methodology, the RP submitted the analysis of three case study systems (Ref.81). All three examples are risk significant to the PSA. Therefore, I sampled one of the three for a detailed assessment, namely the Simple Engineered Safety Features Actuation System (ESFAS).

247. My assessment of the application of the methodology was compared against my expectations based on the PSA TAG (Ref. 4) and the SAPs. Based on my assessment, I observed:

- The case study assiduously followed the methodology for the modelling of the system with all the failure modes and integration of hardware and software components.
- Schematics necessary for comprehending the system architecture enabling the review of the fault trees shown, had been provided.
- Consistent discussion on the mapping of the input and output side failures to the components shown in the fault trees was provided.
- CCF potentialities, CCF groupings and modelling, and CCF parameters were presented in a consistent and traceable manner.
- Analysis results, sensitivity analysis for software failures were presented and discussed comprehensively and justified where necessary.

248. Overall, I found the analysis presented for the ESFAS system is reasonable and adequately meets the expectations of SAP FA.13 and the paragraph 657 of the SAPs (Ref. 2) and the PSA TAG (Ref. 4).

249. Similarly, I assessed the other two case studies for consistency with the Simple ESFAS study. Based on my assessment I am content with the conclusions drawn for the other two case studies.

250. However, this methodology as applied to the C&I system modelling cannot be applied to the UK HPR1000 PSA model immediately due to lack of maturity of the C&I system design at the GDA stage. As a result there are significant limitations to the GDA PSA modelling which reduce my ability to reach an understanding of the contribution the C&I systems make to the overall UK HPR1000 risk results. Given the importance of the C&I design to the scope of my GDA review, I have captured this as an Assessment Finding in according with ONR guidance (Ref. 1).

> AF-UKHPR1000-0104 – The licensee shall, as part of detailed design, undertake PSA to demonstrate the risk from C&I failures. This analysis should explicitly include C&I hardware and software failures in the PSA models and should include both Level 1 and 2 PSA for all categories of initiating events and plant operating states.

4.10.3 Strengths

251. The RP’s proposed methodology, as demonstrated through a limited application during GDA, for addressing C&I hardware and software in the PSA modelling appears to have the potential to meet ONR expectations.

4.10.4 Outcomes

252. I have raised Assessment Finding AF-UKHPR1000-0104 to address the shortfall related to C&I modelling in the UK HPR1000 PSA.

4.10.5 Conclusion

253. Overall, the work done on this topic provides confidence in the approach of the RP towards the inclusion of C&I modelling meeting regulatory expectations in the site-specific stage of the project. However, a lack of maturity of the C&I system design at the GDA stage was noted, which resulted in an inability on the part of the RP to fully address the risk from C&I in the PSA. Therefore, I have raised Assessment Finding AF-UKHPR1000-0104.

4.11 Level 1 PSA: Data Analysis

4.11.1 Introduction to Level 1 PSA: Data Analysis

254. PSA Data includes IEFs, individual component failure probabilities, unavailabilities due to test and maintenance and CCFs. ONR SAP FA.13 and the PSA TAG (Ref. 4) outline the expectation that PSA data should be best-estimate as far as possible, and where this is not practicable, conservative assumptions may be used with the sensitivity to the PSA results of these assumptions being established. FA.13 also established the preferred order of quality of PSA data derivation to be (in descending quality): facility specific data, generic data, expert judgement data.

255. Early in GDA, I identified a gap in the RP's documentation and substantiation and traceability of data used in the PSA modelling. In addition, there appeared to be some optimistic data being used, and a general lack of explanation of the RP's approach for data derivation. Thus, I raised RO-UKHPR1000-020 (Ref. 57) to ensure this gap was closed during GDA. As a response to this RO, the RP produced a report (Ref. 35) that included the majority of the data analysis used in the PSA, along with justification for all data. Following this, the RP performed a complete update of the Level 1 PSA, Level 2 PSA and SFP PSA using the new data. Although this sub-section is related to my assessment of the Level 1 PSA, the findings also apply to Level 2 PSA and the SFP PSA as the FT modelling techniques are identical.

4.11.2 Assessment

256. My assessment of the IEFs can be found earlier this report. My assessment of the individual component failure probabilities, unavailabilities due to test and maintenance and CCFs will be presented in the following sections.

4.11.2.1 Individual Component Failure Probabilities

257. I sampled the RP's revised reliability database (Ref. 35) by choosing several generic components including check valves, motor driven pumps and station blackout emergency diesel generators (SBO DGs). These components were selected due to their high importance in contributing to the overall PSA results.

258. Much of the reliability data was derived from the Chinese national nuclear reliability database (CCRDR), which is owned and maintained by the Chinese national nuclear regulator. The RP explained the process whereby the CCRDR was obtained, screened, and justified from the Chinese nuclear fleet. Each of the steps in creating the CCRDR was described in detail with several examples provided. Some of the component data appeared to have less providence than reliability data typically used UK PSA models, due to the relatively small amount of time and NPPs that exist in China, compared to western European countries, or the US. The RP justified this by comparing each of the cases of this with other generic international databases and showing that either the data was similar, or in some cases, replacing the Chinese data with generic international data if that data was considerably of better provenance.

259. The PSA reliability information for those component types that I sampled contained adequate justification. The database included how many failures occurred in the Chinese or US OPEX and how many demands or hours were recorded for operation. The derivation source of the reliability data was described in detail.

260. A comparison was provided to show the CCRDR reliability figures and the US generic database figures side-by-side and to describe why a particular figure was chosen for use in the UK HPR1000 project. For all reliability data chosen for use, justification was provided for the choice. The approach to combine the two generic databases was described in detail and justification was provided for this approach.

261. Check valves failing in the closed position (stuck closed) were assigned a failure on demand probability of 7.28x10^{-5}, based on 17 events and 233620 demands in the CCRDR. The RP provided justification for using this failure rate through discussion of the CCRDR information and comparison with US OPEX (Ref. 9). The US failure rate was slightly higher than that contained in the CCRDR (1.57x10^{-4} /demand), however in this case, the Chinese OPEX recorded a significantly higher number of demands on check valves. The RP argued that this means that the Chinese data should be able to provide a failure rate with lower uncertainty than the US data, and closer to a best-estimate figure. In my opinion, these arguments are reasonable, and thus I considered this failure rate adequate for use in the UK HPR1000 GDA PSA.

262. Motor driven pumps failure to start were assigned an on demand failure probability of 1.83x10^{-4}, based on 22 events and 120444 demands in the CCRDR. The RP provided justification for using this failure rate through discussion of the CCRDR information and comparison with US OPEX (Ref. 9) The US failure rate was higher than that contained in the CCRDR (7.94x10^{-4} /demand). The RP argued that they decided to use the CCRDR data (even though it was less than the US generic data) because the CCRDR data still contained more than 120 000 demands, and the number of failure events was statistically relevant. In addition, the RP argued that assuming the pump designer and manufacturer was of Chinese origin, the quality of the CCRDR data was of higher providence than the US OPEX, which is of unknown designer and manufacturer. In my opinion, these arguments are reasonable, and thus I considered this failure rate adequate for use in the UK HPR1000 PSA.

263. SBO DGs failure to start was assigned an on demand failure probability of 2.98x10^{-2}. The source of this data was the US OPEX (Ref. 9) as the CCRDR did not contain information on SBO DGs. The RP argued that the failure rate was appropriate for use in the UK HPR1000 PSA because the component boundaries in the PSA model, the CCRDR and Ref. 35 are all identical by design. Thus, the RP expects that although the design and manufacturer may be different between the US and China, the failure rate information is still adequate for use in the UK HPR1000 PSA. In my opinion, these arguments are reasonable, and thus I considered this failure rate adequate for use in the UK HPR1000 PSA.

264. In my opinion, for the sample of the revised reliability database that I assessed the RP has adequately justified the failure rates that are used in the UK HPR1000 PSA. The database contains:

- the source of all data used in the PSA;
- a description of the derivation for how the data was obtained;
- a thorough description of how the CCRDR was created;
- a comparison and justification for the use of all data; and
- a thorough description of the approach used to combine the CCRDR with US generic reliability data.

4.11.2.2 Unavailabilities Due to Test and Maintenance

265. Earlier in this report (Section 4.8) I have presented my assessment of how the RP considered EMIT in a few specific sampled FTs. In this sub-section I present my general assessment for how the RP considers EMIT across the various PSA models from a high-level approach. The EMIT information that was contained in Ref. 33 was based on the design reference plant (FCG3). The RP argued that this assumption is reasonable for GDA as it is likely that the actual EMIT plan should be similar to the design reference plant. In addition, the RP noted that the full EMIT plan for the UK HPR1000 is not part of the scope of GDA, and thus, for all EMIT data that is used in the PSA should be considered an assumption for GDA (e.g. for proof testing, train-based planned maintenance, and temporary unplanned maintenance).

266. The ONR Fault Studies inspector raised RO-UKHPR1000-0021 (Ref. 57) against gaps that Fault Studies and other topic areas identified for EMIT. As part of the RP's process to address the gaps in this RO, new preliminary EMIT information for the UK HPR1000 was submitted to ONR (Refs. 82 and 83). This new information was different than that described in the internal events Level 1 PSA (Ref. 36). Thus, I identified a gap whereby the RP had not demonstrated that the EMIT information contained in Refs. 82 and 83 was compatible with the PSA topic area or the effect on the PSA. The RP then produced Ref. 6 which presented an analysis of the impact of this EMIT information on the PSA.

267. I sampled Ref. 6 to understand the effect of the revised approach for addressing EMIT and its effect on the Level 1 PSA. The RP presented a list of the EMIT information that could affect the PSA modelling as well as a comprehensive analysis of the effect of this change to the models. The RP identified several inconsistencies between the PSA EMIT assumptions based upon the reference design data and the new EMIT information contained in Refs. 82 and 83. The RP concluded that the new EMIT information was compatible with the PSA and demonstrated that there was no significant effects on the PSA results. Finally, the RP presented the risk importance of the new EMIT information in Ref. 6. It was clear from this report that the PSA modelling shows that differences between the new EMIT information and that used in the internal events Level 1 PSA did not result in a significant difference in the Level 1 PSA results.

268. I am content that the RP has demonstrated that the revised EMIT data is adequate for use in the UK HPR1000 PSA. The licensee will need to revise the PSA as EMIT data changes during the site-specific stage as a part of normal business.

4.11.2.3 Data Analysis for Common Cause Failures

269. The PSA TAG outlines regulatory expectations for CCF analysis in PSA: the approach used to select CCF groups should be clear, fit for purpose and include both inter-system and intra-system CCFs. In addition, the method chosen for CCF parameter estimation should be transparent and meet expectations compared with RGP such as NUREG/CR-6268 (Ref. 9). The PSA TAG (Ref. 4) also expects that the quantification of CCFs be transparent, well documented, and traceable to the underlying analysis.

270. The process by which CCF values are identified for common components is described in Ref. 22. The RP has used the 'multiple Greek letter' (MGL) approach to calculate the common cause unavailabilities of components.

271. The RP selected CCF groups using three key principles:

- identical non/diverse components that are designed to be redundant (generally located in the same system);
- for inter-system identical components, unless the components are identical in terms of function, operating conditions, environmental conditions, EMIT, etc, they are not included in the same CCF group; and
- components that are designed to be redundant but are also diverse in design are not included in the same CCF group, unless the diverse components have identical sub-components

272. This approach is similar to RGP such as NUREG/CR-6268 (Ref. 9) and in my opinion, meets ONR expectations compared with the PSA TAG (Ref. 117). It includes consideration of intra-system and inter-system CCFs.

273. The MGL approach to quantify the CCF group probabilities is commonly used and the RP has documented their parameters used as well as the final CCF probabilities in the various PSA reports. I sampled some of the CCF probabilities used in Ref. 36 and was able to reproduce the RP's probabilities for all CCFs sampled.

274. I identified a gap against my expectations compared with RGP such as the PSA TAG (Ref. 4) in that the RP did not produce a summary table of the final results of all CCFs used in the PSA. However, there was significant discussion of all risk-important CCFs throughout the various discussion and results sections of the PSA reports. Thus, although this is a gap against my expectations, I consider that the analysis of CCFs is adequate for GDA as compared with RGP. In future PSA reports, a clearer summary of all CCF analysis will be expected to be produced, and this should be normal business for a licensee.

4.11.3 Strengths

275. The data analysis of the PSA was well documented and justified.

4.11.4 Outcomes

276. I would expect the EMIT information contained in the revised PSA Reliability Database should be updated with site-specific, design-specific information for the UK HPR1000 design as part of normal business for a licensee.

4.11.5 Conclusion

277. I found that the PSA data analysis met my expectations as compared with RGP. The data was generally documented and substantiated well, and I was able to trace the golden thread clearly. Thus, I am content in the RP's data analysis for the PSA for GDA.

4.12 Level 1 PSA: Low Power and Shutdown Modes

278. SAPs FA.12 and FA.13 and the PSA TAG expect that the PSA considers all operating modes, including shutdown and low power.

279. In Ref. 36, the RP explains how the PSA covers all POS including low power and shutdown. As explained in Section 3.2 of this report, there are six POS, and the RP has included specific PSA modelling for all six. Each system FT included specialised modelling for each POS, and where success criteria or unavailability of support systems were different, the FTs include 'house events' which identify each POS. The SFP PSA, hazard PSAs and Level 2 PSA all include this type of specialised modelling for all POS.

4.12.1 Assessment

280. The TSC sampled several low power and shutdown accident sequences in the Level 1 PSA and provided ONR with advice and feedback. I also assessed a sample of the specialised modelling in the accident sequence ETs and system FTs for different POS. The combined TSC and ONR sample included accident sequences and FTs during low power and shutdown for the following Level 1 PSA accident sequence ETs and system FTs:

- ETs for LOOP during POS B and D
- RHR FT during POS C and D
- RCP [RCS] seal FT during POS C
- Low-Head Safety Injection (LHSI) FT during POS D
- ET for SGTR during POS B
- ET for MSLB during POS B
- ET for ISLOCA during POS C

281. In my opinion, the modelling met ONR expectations for those areas sampled compared with RGP such as the PSA TAG (Ref. 4). I observed that for POS-D, the RP reported a

higher than expected risk importance in Ref. 36, and I have presented my assessment of this aspect of the modelling in the following paragraphs.

282. The results of Ref. 36 showed that POS-A (full power) accounted for 77.66% of the overall internal events Level 1 PSA CDF. The next most important was POS-D (normal cold shut down for maintenance) which accounted for 14% of the risk.

283. To understand why POS-D results in a much higher risk contribution than the other low power or shutdown POS, I sampled the modelling of the highest risk contributors for POS-D. The most important cutset for POS-D is: IE-LOCC, followed by a CCF of the Essential Service Water Pumping Station Ventilation System (DXS [ESWVS]) combined with an operator error to start the LHSI system. This cutset is the third highest contributor to all internal event Level 1 PSA results.

284. Ref. 36 explained that this relatively high contribution to the PSA results from a low power operating state is because a DXS system failure in POS-D will result in a LOCC. In addition, during POS-D, after an LOCC accident, an operator is required to manually initiate the LHSI system, and the probability of failure for this operator error is $1x10^{-3}$. For normal full power operation, mitigation of the DXS failure is automated, and thus not very important to the PSA results, however, during POS-D, manual actions are required to mitigate the fault.

285. The relatively high contribution to the level of risk from a DXS system failure was discussed in the internal events Level 1 PSA as a sensitivity case. The RP found that prevention of a DXS system failure would improve the overall internal events Level 1 PSA CDF by 41%. During the course of GDA, the RP proposed a modification (Mod-35, Ref. 84) which added diversity and redundancy to many HVAC sub-systems including DXS. In Ref. 6 the RP analysed the effect on the PSA results of many of the modifications, including Mod-35 and demonstrated that the risk contribution from loss of DXS during POS-D was significantly reduced. This is a significant improvement in the internal events Level 1 PSA results and the real plant risk, however, as it came quite late in GDA it was not included in the internal events Level 1 PSA (Ref. 36). I have assessed the sensitivity study and am content that the results demonstrate the low risk from low power and shutdown operating state accidents.

4.12.2 Strengths

286. The RP has considered all operational power modes in the PSA, including shutdown and low power for internal events Level 1 PSA. I consider the modelling of Hazards PSA during low power and shutdown modes to be a strength.

287. The RP found that during POS D, a particular HVAC system contributed to a higher-than-expected risk, and a design change was implemented to reduce the risk. The PSA was used to risk-inform this design change.

4.12.3 Outcomes

288. My assessment of the RP’s submissions on Level 1 PSA low power and shutdown mode against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.12.4 Conclusion

289. I am content with the consideration of low power and shutdown modes of operation in the Level 1 PSA, compared with RGP. The RP modelled this aspect of the design robustly in the PSA.

4.13 Level 1 PSA: Spent Fuel Pool PSA

4.13.1 Introduction to Spent Fuel Pool PSA Assessment

290. The RP submitted a SFP PSA model and report (Ref. 37) up to Level 1 PSA, including internal and external hazards. The RP has also submitted a combined Level 2 PSA (Ref. 42) which considers input from multiple Level 1 PSAs including the SFP PSA. The Level 3 PSA (Ref. 44) includes consideration of the off-site releases from the SFP PSA.

291. The results from the SFP PSA are displayed differently than for the internal events Level 1 PSA in that they are the frequency of fuel damage rather than core damage, both mechanical fuel damage (6.0x10^{-5} /ry) and thermal fuel damage (6.64x10^{-9} /ry). The SFP PSA uses a significant portion of the internal events Level 1 PSA model, especially for support system fault trees.

292. In this section I will discuss my assessment of the portions of the Level 1 SFP PSA model which were unique to the SFP PSA, as the portions that were copied from the Level 1 PSA have been assessed in the relevant sub-sections of this report.

293. The TSC sampled portions of the SFP PSA, compared it with RGP and provided ONR with advice and feedback (Ref. 53). I used this information in my assessment of the SFP PSA, and in addition, I sampled different portions of the SFP PSA and compared it with RGP, such as the PSA TAG (Ref. 4). My assessment of the SFP PSA is presented in the following sub-sections.

4.13.2 Spent Fuel Pool PSA Overall Plan and Scope

294. The RP provided a methodology for the SFP PSA (Ref. 24) which outlined the proposed approaches to be used and the scope of the SFP PSA for GDA. The scope of the SFP includes all POS and IEs for internal events, IH, and external hazards.

295. The methodology and approaches used in the SFP PSA are stated to be from IAEA SSG-3, IAEA TECDOC-1804 (Ref. 8), NUREG-0612, NUREG-1774, NUREG-1738, (Ref. 9) and the ASME Level 1 PSA Standard (Ref. 17). These references are standard guidance and RGP for performing SFP PSA, and I consider that the RP's approaches used are in line with the references.

296. The RP's definition for a postulated initiating event for the SFP PSA is: 'an event that could lead directly to fuel damage, or that challenges normal operation, and which requires successful mitigation measures to prevent fuel damage'. This is slightly different than the internal events Level 1 PSA definition for an IE, but in this context, I consider that it is reasonable and in line with RGP. This definition is important as it means that the accident sequence development models the plant response to various IEs in an effort to prevent or mitigate fuel damage. Thus, the end states are designed to be different from the reactor side PSA, and success will mean fuel damage has been prevented, whereas instead of core damage, the end state for a failed sequence is termed 'fuel damage (FD)'.

297. The RP has also split the FD end states into two types: thermal (FD-T) and mechanical (FD-M). The FD-M represents event sequences wherein fuel cladding or fuel elements are damaged leading to a release. FD-T represents a situation where decay heat is not successfully removed from the spent fuel and thus some fuel melt is likely. FD-T accidents are mostly related to the fuel inside the SFP where the decay heat removal requirements in freshly removed fuel tends to be much higher than in spent fuel containing fission products that have decayed after many years and is being manipulated by the fuel handling processes for movement out of the SFP.

298. The scope of the SFP PSA was stated by the RP to include:

- new fuel handling;
- irradiated fuel handling;
- irradiated fuel storage in the SFP; and
- loading of spent fuel into the long-term storage casks and subsequent transfer operations within the fuel building (FB)

299. Thus, fuel movements outside of the RB or FB are outside the scope of this PSA. To be clear, the PSA scope does include fuel route operations up to loading a full long-term storage cask onto the lorry but does not include fuel route operations after storage cask have been placed onto the lorry, nor operations at the SFIS facility. In my opinion, the scope of the SFP PSA is reasonable and appropriate for GDA.

300. I worked with the inspector from the radwaste, decommissioning and spent fuel management specialism to identify a gap for a potential accident scenario where fuel clad integrity might be lost due to overheating from excessive hold time within a transfer cask. The safety case identified the requirement for forced ventilation in the transfer cask to provide cooling, and therefore provide control over the temperature of the fuel, reducing the likelihood of fuel clad integrity being lost. Although this IE was not identified in the SFP PSA, the IE was clearly within the scope of the SFP PSA.

301. I raised RQ-UKHPR1000-1593 (Ref. 66) to understand how the RP intended to address this accident scenario in the safety case and PSA for GDA. In the response to the RQ the RP justified not explicitly including this fault within the PSA scope because of the RP’s assumption that the consequences (release of radioactive material due to fuel clad failure) from the IE would not be realised, as the canister would never be opened. However, the radwaste inspector noted this to be inconsistent with the UK HPR1000 spent fuel management strategy and SFIS facility design. The radwaste inspector raised RO-UKHPR1000-0050 (Ref. 57) to address these gaps, and I supported the resolution of this RO from a PSA perspective.

302. To resolve this RO, the RP agreed to add a new IE to the list considered within the SFP PSA (H-311 in Ref. 85) to address the fault. This fault is for an accident scenario where the transfer time exceeds the limit for spent fuel transfer, leading to thermal fuel damage. As the SFIS is still in conceptual design this hazard was recorded in the PIE list for further analysis when the detailed design is more mature.

303. I assessed the RP’s response to this gap and was content for GDA that the fault was added to the shared PIE list between FS and PSA for further analysis when the SFIS design is complete post-GDA. The gap has not been analysed, and thus there remains an area of the design where the level of risk has not been assessed. Although this gap is within the scope of the PSA, I am content that it can be analysed post-GDA because of the relatively low level of risk that I expect to arise from this fault. The low expected level of risk is due to two factors. Firstly, fuel cask movements are only expected three times per year. Secondly, transfer casks are typically quite robust and thus the random failure probability is low for a cask to spuriously open during the small amount of time at risk. For these reasons, in my opinion, it would be disproportionate to require the RP to perform more analysis during GDA, however post-GDA it is expected that this fault be included in future PSA versions. This is a gap against my expectations and will be addressed through normal business by the licensee. Thus, I am content with the RP’s arguments for why this gap in the GDA safety case is not a barrier to ONR reaching a judgement on the adequacy of the UK HPR1000 fuel route.

4.13.2.1 SFP PSA IE Identification, Grouping, IEFs and Screening

304. The RP has used the same methods to identify postulated IEs for the SFP PSA as with the Level 1 internal events PSA (for example, master logic diagrams (MLD) and FMEA). I have assessed this approach as described earlier in this report and find it to be adequate. After the large list of postulated IEs was derived (see Ref. 85), the RP

then performed grouping and screening in order to limit the analysis required for the SFP PSA to a manageable size.

305. In the MLD for the SFP PSA, the RP described three ways of arriving at thermal FD: re-criticality, loss of SFP cooling and loss of SFP water inventory. These three groups are termed 'Abnormal Operational States' (AOS) and the RP lists fifteen different system failures that could lead to one of the three AOS. These fifteen system failures become the fifteen thermal FD SFP PSA IEs that are analysed further in the report. I assessed the grouping exercise and find it to meets with my expectations compared to RGP. Similarly, mechanical FD followed a methodical process to examine fuel movements. This process resulted in twenty-three IEs for mechanical FD.

306. Before assigning IEFs to the IEs, some are screened out from further consideration based on physical impossibility. The RP provided justification for those that were screened in this way. The RP then assigned frequencies to the SFP PSA list of IEs using a mix of Chinese OPEX, fault tree analysis and generic data (see earlier in this report for my assessment of IEF derivation). After assigning IEFs, some PIEs were screened out if frequency of FD is much smaller than the total FDF (less than 1%). The final IE list for the internal events SFP PSA contains twelve thermal FD IEs and twenty-three mechanical FD IEs. In my opinion, this screening criteria meets expectations compared to RGP and thus is reasonable.

4.13.2.2 SFP PSA Determination of Success Criteria

307. The RP has presented the approach for determining the success criteria of systems analysed in the SFP PSA in Ref. 37. For those support systems which were previously modelled in the Level 1 PSA, the success criteria remain the same as listed in Ref. 36, as was assessed earlier in this report.

308. Thermal-hydraulic support analysis is provided in Appendix A of Ref. 37, which was used to determine the success criteria for the SFP PSA specific systems including reactor cavity PTR, emergency diesel generators (EDGs), SBO DGs and other systems used to cool the SFP.

309. I assessed the thermal-hydraulic support analysis and found it to meet expectations compared to RGP. Although I was able to trace the success criteria in the report to the Appendix A tables I found that the golden thread of the safety case was not always clearly stated. I needed to search through the report to find the clear path of claims, arguments, and evidence. However even though there were weaknesses in documentation, I did not find that there were gaps in the analysis or design. Thus, for GDA, I found the determination of the success criteria to meet my expectations as compared with RGP.

4.13.2.3 SFP PSA Event Sequence Modelling

310. The SFP PSA ETs are modelled following the same approaches used in the internal events Level 1 PSA (Ref. 36). I have assessed those approaches earlier in this report and find that they are adequate for GDA, although the 'golden thread' was not easy to follow.

311. I sampled several ETs in the SFP PSA (including SFP_DR_FUEL_A, SFP_IN_DWK [FBVS] _N) and I provide my assessment of these ETs in the following paragraphs.

SFP_IN_DWK [FBVS] _N

312. I assessed ET loss of DWK [FBVS] train A in the non-refuelling state (SFP_IN_DWK [FBVS] _N), which is the most risk important accident sequence in the SFP PSA and assigned an IEF of 6.65x10^{-1} /ry. The RP describes this event as a failure of the DWK [FBVS] system operating train HVAC for cooling the PTR [FPCTS] system. This leads

to an interruption in the SFP cooling and consequential increase in the SFP temperature. Eventually, this would lead to SFP boiling and inventory decrease. When the water level drops to the level alarm setpoint in the SFP, operator actions are credited to start up the standby PTR [FPCTS] trains for cooling of the SFP. Should this fail, the water level will continue to decrease, leading to a claim on the operators to provide makeup water to the SFP on low water level alarm to prevent the fuel assemblies from being uncovered. The ET credits at least one of three different systems to provide makeup water to the SFP: Nuclear Island Demineralised Water Distribution System DWDS (NI), Secondary Passive Heat Removal System (ASP [SPHRS]) or an externally located water source using a mobile water pump.

313. This IE and accident sequence is the most important to the SFP PSA results for FDF-T. The IE contributes 58.1% to the total FDF-T frequency. The RP notes in the risk insights section of Ref. 37 that the reason for this relatively high contribution to the FDF-T is because of a lack of diversity and redundancy in the HVAC systems used to cool the fuel building, and the SFP cooling system. The RP notes that this suggests diverse designs for DWK [FBVS] and the safety chilled water system (DEL [SCWS]) would improve this.

314. The RP submitted a plan to modify the HVAC in many different systems by improving the diversity of significant portions (modification M-35 – Ref. 78). This modification was agreed during GDA and thus the risk insights on this event recommended by the SFP PSA were adopted. Although the actual risk arising from FD-T events is low, the SFP PSA revealed a weakness in the design of HVAC. This weakness was also noted by the mechanical engineering specialism and thus the modification was made to the generic design during GDA. The safety of the plant was improved by this work and it was accepted during GDA. The SFP PSA has not been updated within GDA to reflect DR3. I recognise this is a gap due to the low risk arising from the SFP PSA and the RP's demonstration during GDA that DR3 should not affect the SFP PSA FDF significantly. I am content with this for GDA. I would expect the SFP PSA to be updated adequately to reflect the plant design in the site-specific stage as part of normal business for a licensee.

315. I am content with the event tree analysis for loss of DWK [FBVS] train A in the non-refuelling state. This work from the RP led to a modification which highlighted potential problems with the diversity in the HVAC elsewhere in the design. Modification M-35 increases the reliability of all the HVAC systems, including DWK [FBVS] through increased redundancy and diversity between HVAC trains. This modification was not accepted early enough in GDA to be implemented in the SFP PSA. I would expect that if this modification were included in the SFP PSA, the risk from the IE "SFP_IN_DWK [FBVS] _N" would be lowered significantly from the additional redundancy and diversity in the three DWK [FBVS] HVAC trains.

SFP_DR_FUEL_A

316. I also assessed the event tree analysis for IE SFP_DR_FUEL_A. In this grouped IE the RP presented analysis of a dropped fuel assembly or component due to a fault in fuel route operations. The RP included these accidents in their probabilistic assessment of mechanical fuel damage in the SFP PSA.

317. The event tree analysis for dropped loads in the SFP PSA was quite simple, with an single event tree. The frequency of the IE for this ET was calculated using a fault tree where all the basic events are under an OR gate. Each basic event was assigned a probability based on the overall dropped load frequency per lift that was used in the SFP PSA multiplied by the number of those lifts in a year.

318. I assessed the frequency of a dropped load calculation and raised RQ-UKHPR1000-0737 (Ref. 66) to seek more information. The RP used NUREG/CR-1738 and NUREG-

0612 (Ref. 9) to derive the generic dropped load frequency. In this reference, the RP chose a single-failure-proof load handling system, which in NUREG/CR-1738 (Ref. 9) is estimated to have a dropped load frequency of 9.6x10^{-6} /ry with 100 lifts per year. The RP then divided the frequency by 100 to reach a dropped load frequency of 9.6x10^{-8} /lift.

319. I requested further justification for the dropped load frequency per lift by raising RQ-UKHPR1000-0849 (Ref. 66). In response to this RQ, the RP performed sensitivity calculations and demonstrated that the FDF-M is not highly sensitive to the dropped load frequency used. The RP compared the frequency with other RGP generic dropped load frequencies and noted that the frequency used in the UK HPR1000 SFP PSA is smaller than other generic sources (such as NUREG-0612, NUREG-1774 (Ref. 9) and EPRI-009691 (Ref. 11)). The RP also provided further analysis of the implications of this small frequency for GDA and found that even if the frequency was increased, it was unlikely to affect the risk due to the fact that many dropped fuel loads would be over water, and that the fuel cask drops should be mainly lower than the rated lifting height for the cask. In addition, the RP also noted that the design of the fuel crane and fuel building was being considered for significant modification which may remove a portion of the most risk important dropped loads from a future SFP PSA. This modification is M-94 (Ref. 86). In my opinion, the RP's argument is reasonable as the risk from fuel route faults is low, and if it was higher, the risk would still be acceptable. In addition, although the SFP PSA has not been updated to include the design changes from modification M-94, the RP presented evidence that this modification will eliminate the most risk important faults in the SFP PSA, thus lowering the risk further.

320. The RP also provided further arguments and evidence in the response to RQ-UKHPR1000-0849 that dropped loads over the SFP will not result in a catastrophic concrete failure, and thus would not lead to SFP draining. I reviewed the RP's arguments and evidence and discussed it with the ONR civil engineering inspector. In my opinion, the RP's arguments and evidence were reasonable and suitable for GDA.

321. I assessed all of these arguments and in my opinion, I find that the risk from dropped loads has been addressed adequately in the SFP PSA. Although the dropped load frequency was found to be lower than RGP, the RP adequately demonstrated that even if a higher frequency were used, the risk from dropped loads was still expected to be low. Risk is a product of frequency and consequence, and the consequence of physical damage to fuel is much less than a widespread fuel damage in a severe accident inside the reactor.

322. In addition, the changes being made to the fuel building and lifting devices through modification M-94 should further reduce the risk from dropped loads, as some of the dropped loads scenarios currently considered in the SFP will be physically impossible in the new design. Thus, in my opinion, the SFP PSA dropped load safety case is adequate and demonstrates that the level of risk is low from dropped loads. The changes that are described in modification M-94 are likely to reduce the risk further, however the SFP PSA was not updated to reflect DR3 in GDA. I expect the SFP PSA to be updated adequately to reflect the plant design in the site-specific stage as normal business for a licensee.

SFP PSA HRA

323. The SFP PSA makes significant claims on operator actions in many of the accident sequences modelled. The two most risk important operator actions are: failure to recover operator actions after water makeup action in the SFP has failed (SFP_N_REC_H2 – 5x10^{-2}); and operators fail to start makeup water for SFP (SFP_N_H2 – 1.1x10^{-4}). These two operator actions appear in many of the most dominant minimal cutsets for the SFP PSA as the operator will need to perform

makeup to the SFP after either a failure of cooling or loss of inventory. The RP performed dependency analysis on these two operator actions and found low dependency (but nonzero) due to the two actions being separated in time such that a different shift would undertake each. Thus, SFP_N_REC_H2, the recovery action HEP was changed from an original estimate of $3x10^{-4}$ before dependency analysis was performed to be $5x10^{-2}$ (as stated above) to account for this dependency.

324. I have previously assessed the approach for deriving HEPs and dependency in this report and thus will not repeat the assessment in this section. I raised RQ-UKHPR1000-0737 (Ref. 66) to understand the RP's claims for these two operator actions and to understand their justification for the dependency calculations better. The RP explained that dependency analysis was followed as per the HRA Methodology (Ref. 23) and according to this approach the two operator actions have low dependency. I find this justification reasonable and adequate. Overall, I find that the RP's documentation, justification, and modelling of HRA in the SFP PSA to be adequate compared to RGP such as the PSA TAG (Ref. 4) or the reports listed in paragraph 205 of this report.

SFP overall results

325. The SFP PSA results show that the risk of FDF from all faults included in the SFP PSA is not high compared with the Level 1 PSA core damage frequency, or the Level 2 PSA large release frequency. In addition, the Level 3 PSA (Ref. 44) shows that FDF-T does not represent a high level of risk and are less than the BSOs for Targets 7, 8 and 9. FDF-M is a significant contributor in the Level 3 PSA results, however, mechanical fuel damage faults result in consequences less than the BSOs for Targets 7, 8 and 9.

326. In addition, the Level 3 PSA (Ref. 44) shows that the consequences of accidents related to the SFP PSA are lower compared with accidents arising from severe accidents in the reactor.

327. In my opinion, the RP has adequately demonstrated that the SFP PSA results are low compared with SAPs Targets 7, 8 and 9. In addition, I expect the risk to be further reduced when the SFP PSA is updated to include the design changes to the crane discussed previously in this report.

SFP hazards PSA

328. The approach of the SFP PSA for internal plant faults is replicated for the SFP for hazards. The SFP PSA for the internal fire hazard is reported as part of the internal fire PSA (Ref. 48), similarly for internal flooding (Ref. 46), external hazards (Ref. 87), and external flooding (Ref. 40)

329. The overall contribution of the hazards to FDF-T is very small in comparison to the internal plant faults as can be seen in the following table.

Table 7: FDF-T Results

Initiating Event category	FDF T (1/ry)	Percentage (%)
Internal events	6.55×10^{-9}	98.50
Internal fire	5.01×10^{-11}	0.70
Internal flooding	6.35×10^{-12}	0.10
External hazards (except seismic and external flooding)	3.39×10^{-11}	0.50

Initiating Event category	FDF T (1/ry)	Percentage (%)
External flooding	1.4×10^{-11}	0.20
Total	6.65×10^{-9}	100

330. Mechanical damage to fuel caused by accident sequences associated with fuel cask drops, fuel assembly or component drops during fuel route operations is denoted as FDF-M. For GDA, the frequency of these events has only been calculated for refuelling and spent fuel operations during normal operations. Hence dropped loads are shown as the only initiators. No impact from internal fires, floods and external hazards is calculated. In my opinion this approach is targeted and proportionate to the risk from FDF-M.

331. Only two sequences modelled through event trees for spent fuel cask drops and fuel assembly or component drops during fuel handling contribute to FDF-M. The FDF-M is 5.99×10^{-5}/ry and 1.28×10^{-7}/ry for the fuel assembly and fuel cask drops respectively (Ref. 37). These sequences are then analysed for direct release in the fuel building and reactor building through the Level 2 PSA (Ref. 42). Though FDF-M is much higher than the FDF-T, the consequence of radioactive release is defined as restricted to either one fuel assembly (containing a maximum of 17 fuel rods) or one fuel cask (containing a maximum of 32 fuel assemblies) worth of release and is therefore of lower consequence (small release) than the large release due to FDF-T. I am content with the adequacy of the analysis and risk insights for these FDF-M sequences in Level 1 PSA for IH.

332. Based on the review of the quantitative contribution of the SFP FDF-T I can conclude that the hazards are not significant contributors to the risk in the spent fuel pool. However, it is noted that this excludes the seismic risk (see Section 4.18). However, for the GDA stage I am content that the analysis provided through the PSAs for the SFP is proportionate and targeted.

4.13.3 Strengths

333. The approaches used to model the SFP PSA were well explained, and met my expectations compared to RGP.

334. The scope of the SFP PSA was considerable and the RP has demonstrated an understanding of the areas of highest risk in the SFP.

4.13.4 Outcomes

335. A licensee should update the SFP PSA after detailed design is available as a part of normal business.

4.13.5 Conclusion

336. Overall, the SFP PSA meets regulatory expectations as compared to RGP for GDA. I have identified a few minor shortfalls that are discussed in the above paragraphs.

4.14 Internal Events Level 1 PSA Results

337. SAPs FA.13, FA.14 and the PSA TAG expect that results of the PSA be used to understand the level of risk arising from the design. One of the ways this is expected to be performed is by uncertainty analysis, sensitivity analysis and case studies.

338. In the following sub-sections I present my assessment of the use of the results of the PSA against the expectations outlined in the relevant SAPs and the PSA TAG.

4.14.1 Internal Events Level 1 PSA Results Quantification

339. The RP quantified the Level 1 PSA to provide an estimate of the core damage frequency (CDF) using applicable accident sequences which resulted in CD. The RP used a cut-off value of $1x10^{-14}$ so that minimal cutsets with a frequency of less than $1x10^{-14}$ are not included in the quantification calculations. The RP calculated that for this cut-off frequency, the relative error that is introduced by this process should be less than 2%. Table 2 above contains a summary of the results of the PSA, for Level 1 PSA, the results are as follows:

- Internal Events Level 1 PSA CDF: $3.85x10^{-7}$ /ry.
- Internal Fire Level 1 PSA CDF: $3.47x10^{-7}$ /ry.
- Internal Flooding Level 1 PSA CDF: $4.65x10^{-9}$ /ry.
- External Hazards (Except for Seismic Hazards and External Flooding) CDF: $2.11x10^{-8}$ /ry.
- External Flooding CDF: $6.04x10^{-9}$ /ry.
- Seismic Hazards CDF: $2.29x10^{-8}$ /ry.
- SFP Total FDF-T: $6.64x10^{-9}$ /ry.
- SFP Total FDF-M: $6.0x10^{-5}$ /ry.

340. The method for quantification that the RP is consistent with RGP and my regulatory expectations. The quantification results for the CDF shows that the level of risk arising from the design is low, as is expected for a modern NPP design. ONR does not have a CDF target for reactor designs, however when compared with RGP such as Ref. 88, the CDF compares favourably.

4.14.2 Internal Events Level 1 PSA Results Uncertainty Analyses

341. The RP considered uncertainty in the quantification process. The RP included consideration of uncertainty throughout the PSA model in that each and every individual basic event would have its own uncertainty, which accompanies the failure rates obtained from OPEX. This uncertainty from each basic event was systematically carried through in Risk Spectrum when quantifying all of the different accident scenarios, such that any result that was provided from the PSA contained uncertainty values.

342. The Level 1 PSA reported the uncertainty analysis results for each IE and presented a table showing the range of results from the point estimate, the mean, 5th percentile, median to 95th percentile. The point estimate value of UK HPR1000 Internal Event Level 1 PSA CDF is $3.85x10^{-7}$/ry, the mean value is $4.38x10^{-7}$/ry, the median value is $3.49x10^{-7}$/ry, the lower limit (5th percentile) value is $1.77x10^{-7}$/ry and the upper limit (95th percentile) value is $9.78x10^{-7}$/ry.

343. I consider that the RP's approach for uncertainty analysis meets expectations as compared to RGP such as the PSA TAG (Ref. 4) and that the results demonstrate a fairly low level of uncertainty and thus high level of accuracy in the Level 1 PSA results.

4.14.3 Internal Events Level 1 PSA Results Interpretation and Importance

344. To provide insight and interpretation, the RP has provided importance analysis for the Level 1 PSA results. Importance analysis is used to identify and verify the major contributors to the CDF, namely, component failure and human errors. Information given by importance analysis is significant for providing insights for plant safety and indicating some measures to reduce plant risk.

345. The RP used the following approaches to measure the importance of the PSA basic events, cutsets, etc: FV importance, risk decrease factor (RDF) and risk increase factor (RIF). FV importance measures the overall percent contribution of cut sets containing a basic event of interest to the total risk. RDF sets a basic event, parameter or other aspect of the model to 0 (i.e. 100% reliable) and then provides the factor by which the quantified result would change. RIF sets a basic event, parameter or other aspect of the model to 1 (i.e. 0% reliable) and then provides the factor by which the quantified result would change.

346. The RP presented detailed importance results for all component failures and human failure events including discussion and interpretation of these results. The most important findings were:

- CCF of DVL [EDSBVS] fans is the most important failure event by FV importance. This is discussed elsewhere in this report and addressed by modification M-35 (Ref. 84).
- A failure of more than three RCCA rods to insert successfully was the most important failure event by RIF importance.
- The most important human error by FV importance was a failure to perform F&B manually after a transient accident.
- The most important human error by RIF importance was failure to start portable air conditioners manually after a loss of DCL [MCRACS] accident.

4.14.4 Internal Events Level 1 PSA Results Interpretation and Sensitivity Analysis

347. The RP provided sensitivity analysis all of the PSA reports (Refs 36, 6, 37 and 42) to understand the sensitivity of some important topics that arose during quantification of the PSA. Risk Spectrum has a built-in capacity for calculating the sensitivity of all basic events in the model.

348. The RP found that for basic event sensitivity the most important were: time duration for POS A; frequency of a LOOP; time duration for POS D; and the CCF of the DVL [EDSBVS] fans. The RP stated that the time duration basic events are observed to be highly sensitive because they apply to all accident sequences by segregating the year into proportions for each POS.

349. The RP found that for human errors, the most important were: failure to operate LHSI manually after a LOCC accident in POS D, and failure to operate F&B manually after transient accidents.

350. These findings have been used along with other information from other engineering topic areas to improve the plant design by lowering the risk, such as modification M-35, the modification to improve diversity of HVAC systems (Refs 84 and 78) for example. The PSA found that HVAC systems such as DVL [EDSBVS] or DXS had a high level of sensitivity and this PSA sensitivity information was used by the RP in the optioneering of those HVAC systems to improve the diversity of the design. Thus, I found that these findings met my expectations for GDA.

351. In addition to the sensitivity analysis automatically performed by Risk Spectrum, the RP performed sensitivity analysis for five scenarios from which a high level of risk was associated: loss of DVL [EDSBVS], loss of DXS, induced LOOP after reactor trip, LOOP, and EMIT.

352. Of these sensitivity cases, the RP identified that the DVL [EDSBVS] fan diverse design was the most significant. If the diverse design of the fans was implemented, the sensitivity case showed a major improvement in the PSA results. I expected this to be the case and since the Level 1 PSA was performed, the modification for this change was included by the RP into DR3 (Ref. 78).

4.14.5 Internal Events Level 1 PSA Results Interpretation – Main Results and Risk Insights

353. The RP reported that the CDF is 3.85x10^{-7} /ry. The IE Loss of DVL (LODVL) was the highest contributor at 31.69% of the CDF, with IE LOOP following this with 17.09% and IE LOCC at 10.94% contribution. All other IEs contributed less than 7% towards the total CDF.

354. The RP reported that the most dominant accident sequence was an IE of LODVL at full power, followed by a loss of DC power, a failure of secondary cooldown, unavailability of the ASP [SPHRS] system and failure of F&B. Decay heat cannot be removed and so this leads to core damage. The frequency of this sequence was calculated to be 1.05x10^{-7} /ry and contributes 27.34% towards the CDF. All other accident sequences contribute less than 10% towards the CDF.

355. The RP reported a list of the top 20 most dominant minimal cutset, with the most dominant minimal cutset being a single event, spurious failure of the RPV, with a CDF of 1.25x10^{-8} /ry and a percentage contribution of 3.25%. Following this, the most dominant minimal cutset is a LOOP IE during full power, followed by a CCF digital C&I failure of the RPS, and an operator failure to start the SBO DGs. This minimal cutset has a CDF of 6.06x10^{-9} /ry and a percent contribution of 1.58%. All other MCS are less than this contribution to the CDF.

356. The RP provided risk insights that noted the following conclusions:

- The internal events CDF is 3.85x10^{-7} /ry, meaning the overall level of risk from internal events is low compared with RGP such as IAEA 75-INSAG-3 (Ref. 8) (which proposes a CDF target of 1x10^{-5} /ry for new reactors).
- The other CDFs calculated for hazards and SFP were also demonstrated to be low, meaning that the overall level of risk from hazards and the SFP is low.
- POS D has a relatively high contribution to the overall risk, which is due to the plant being in a depressurised state and consequently SCD is not available.
- IE LODVL and IE DXS both had a relatively high contribution to the CDF. This was due to both the fact the design of the HVAC had conservative assumptions and a lack of diversity of components. The PSA recommended a design change (which was accepted in Ref. 78).
- IE LOOP had a relatively high contribution to the CDF. This was due to the fact that for the IEF for LOOP was direct assigned from Ref. 95, without deducting the contribution of external hazards to the LOOP frequency. The PSA recommended design change for the EDG or ASP [SPHRS] start-up C&I (which was accepted in Ref. 96).

357. I found that the results of the Level 1 PSA along with the risk insights provided by the RP were well documented and consistent with the entirety of the rest of the PSA including hazards and SFP and input references to the PSA. The results show that the level of risk arising from the design to be low as compared with the expectations outlined in the relevant SAPs (Ref. 2) and the PSA TAG (Ref 4). In addition, the RP used the PSA to understand areas of weaknesses in the design.

4.14.6 Impact Report Analysis on PSA Results

358. Near the end of Step 4 of GDA, the RP submitted Ref. 6, which calculated the change to the internal events Level 1 PSA results after updating the model to include all relevant changes due to removal of conservatisms, applicable modifications (such as modification M-35 (Ref. 84) and errors in modelling.

359. The updated Level 1 results reported in Ref. 6 show that the point estimate of the CDF was 1.99x10^{-7} /ry, a reduction of approximately 52%. In addition, the impact report PSA

analysis shows that the contribution to risk is much more balanced, with no IE higher than 13% CDF contribution, and no accident sequence with a higher CDF contribution than 9%. The HVAC modifications have been reflected in this analysis such that they are not significant contributors.

360. I found that the impact report PSA results were well documented and show that the work through Step 3 and Step 4 of GDA have resulted in a reduction of plant risk (Ref. 6).

4.14.7 Comment on Internal Events Level 1 PSA Ver. C Results

361. The final version of the internal events Level 1 PSA (Ver. C – Ref. 55) was submitted towards the end of Step 4 of GDA and therefore has not been subject to the same level of detailed ONR assessment as earlier versions. However, from a high level review I was able to confirm that the Ver. C results for the modified UK HPR1000 design were consistent with estimates made in the impact report (Ref. 6). In addition, Ref. 55 documentation was improved.

362. ONR and its TSC performed detailed assessment of the Ver. B of the internal events Level 1 PSA (Ref. 36). Ver. B was linked with DR2.1 rather than the final DR3. The RP provided early sight of the changes to the results of the internal events Level 1 PSA and the Level 2 PSA through use of Ref. 6. I assessed Ref. 6 (as discussed in several sub-sections of this report), and it provided ONR with an understanding of the relative risk differences between the DR used for earlier versions of the internal events Level 1 PSA and Level 2 PSA, and DR3. While I have not assessed in detail the PSA models or reports directly linked with DR3, my high level review provides me with confidence that the RP has submitted enough information to demonstrate that the risk is low and well understood for DR3.

4.14.8 Strengths

363. The RP has used the PSA to understand the level of risk arising from the design and insights into the results.

364. The RP has used the PSA to assist with optioneering of any weak points in the design that were uncovered using the PSA results.

4.14.9 Outcomes

365. My assessment of the RP’s submissions on Level 1 PSA results against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.14.10 Conclusion

366. The RP’s use of the PSA results meets with expectations compared with the ONR SAPs and the PSA TAG.

4.15 Level 1 PSA: Analysis of Internal Fires

4.15.1 Background

367. During Step 3 of GDA, the RP submitted an Internal Fire PSA Ver. A (Ref. 47) to estimate the risks from internal fires from the UK HPR1000 design. I reviewed this model and report and found gaps compared to RGP and thus I raised RQ-UKHPR1000-015, 0466 and 0468. The gaps that were found in the Step 3 internal fire PSA related to:

- cable modelling;

- single and multi-compartment fire scenario analysis;
- traceability of fire initiator frequency calculations;
- main control room fire scenario analysis; and
- consideration of transient fires.

368. After a review of the full responses to these RQs (Ref. 66), it was clear that significant gaps existed in several areas of the internal fire PSA and that these gaps should be addressed by the RP during GDA. Thus, in Step 4 of GDA, I raised RO-UKHPR1000-0029 (Ref. 57) against the following gaps in the internal fire PSA:

- absence of sufficient level of detail and scope regarding detailed fire modelling;
- absence of multi-compartment analysis;
- absence of consideration of the effect of fires on nearby power and control cables;
- absence of explicit consideration of multiple spurious operations due to fires at ‘pinch-points’ in the design; and
- absence of information showing how the ignition frequencies have been evaluated and how ignition source counts and transient influencing factors have been established.

369. In response to RO-UKHPR1000-0029 the RP agreed to provide a comprehensive revision to the internal fire PSA in Step 4 of the GDA, through the resolution plan to RO-UKHPR1000-0029 (Ref. 57). However, as the plan for the delivery for the revised study was scheduled to be quite late into Step 4 of GDA, it was agreed that the RP would share with ONR the progress of the work and early findings, if any, through routine monthly meetings and periodic workshops. This provided a good opportunity to gain visibility of the RP’s work and to assess the use of RGP (Ref. 9), such as:

- NUREG-6850
- NUREG/CR-1805
- NUREG-2169
- NUREG-2178
- NUREG-1824
- NUREG-1805
- NUREG/CR-7010
- NUREG/CR-7150
- NUREG Fire PSA FAQs (FAQ 12-0064, 13-0004, 13-0006 and 13-0005)

370. I also raised RQ-UKHPR1000-0913 seeking clarifications on specific topics such as:

- Basis and justification for screening out components in the accounting for calculation of fire ignition frequency.
- Accounting criteria for transient fire source ignition frequency across various bins or groups (consistent with RGP, the RP’s approach in the UK HPR1000 internal fire PSA is that fire event frequencies are estimated based on the analysis of past fire experience and accounted through fire ignition source binning, fire location binning, and treatment of fire events reported during non-power operational modes) .
- Fire ignition frequency for MCR fires (Bin[1] 4).
- Approach for consideration of high energy arcing fault (HEAF) (Bin 16.a and Bin 16.b).
- Basis of weighting factor for fire ignition frequency for self-ignited cable fires (Bin 12) and junction boxes (Bin 18).

371. The responses provided to all the queries of RQ-UKHPR1000-0913 (Ref. 66) were stated by the RP to be based on the use of internal fire PSA RGP (see list above) and

[1] *In Internal Fire PSA, a bin is a group of IEs that are treated similarly in the PSA modelling.*

this provided me confidence on the appropriate application of the methodology. The result of this application of the methodology was the revised internal fire PSA Ver. B (Ref. 48), the assessment of which is discussed in the following paragraphs.

4.15.2 Assessment

372. The TSC and I assessed the revised Internal Fire PSA for the UK HPR1000 Ver. B (Ref. 48) against ONR's expectations for analysis of Internal Fires in the PSA models using Table A.1-2.7.2 of TAG 30 (Ref. 4) and SAPs FA.11 and FA.12. The TSC sampled the revised study in several areas related to the matters identified in the RO-UKHPR1000-0029 (Ref. 57) and provided advice and feedback to ONR. I also reviewed the revised Internal Fire PSA and in the following paragraphs my assessment is presented along with the qualitative and quantitative risk insights.

373. The revised study presented a systematic review of the various plant wide buildings and internal details to identify fire compartments. For each fire compartment the RP included several rooms as the identification is done based on room dimensions, boundary thermal properties, venting arrangements, and ventilation. The cable layout details for the UK HPR1000 design will not be available until detailed design, so for this internal fire PSA study the reference plant FCG3 details were used. Overall, I observed that the compartment identification and reporting has been systematically performed and documented in the revised report. This systematic and comprehensive approach in DFM use of the reference plant cable layout details provides confidence on the accounting of the risk contribution from cable fires to the internal fire PSA (Ref. 48).

374. Following identification of the fire compartments, fire modelling analysis of single compartment fires is expected to be performed using fire modelling software (the RP used CFAST) which uses the following as input information for each fire compartment:

- dimensional, locational and fire load information;
- information on the compartment fire detection and suppression systems;
- fire ignition sources;
- secondary combustibles;
- secondary target equipment; and
- habitability.

375. The aim of this analysis was to assess if the fire in one compartment can affect another exposed compartment based on damage to targets in the exposed compartment. If the targets in the exposing room were damaged, the RP considered fire spread. The fire growth and propagation analysis were conducted using the MOFIS software. Overall, around 50 bounding generic scenarios on a volumetric basis were identified and CFAST analysis was performed leading to 33 generic scenarios for fire growth analysis using MOFIS. These generic scenario analyses were used to further perform 18 plant-specific single compartment analysis using the Risk Spectrum based Level 1 internal fire PSA modelling.

376. The TSC and I assessed the methodology implemented for the Internal Fire PSA (Ref. 48) using a sample of scenarios including that of MCR fires for DFM. I found that the single compartment analysis regarding screening and detailed analysis met my expectations compared with RGP, such as NUREG/CR-6850 (Ref. 9, 10). The risk insights from the DFM to the internal fire PSA study is reported through table T-15-73 of the revised report (Ref. 48) which compares the contributions of the fire compartments to the total CDF by internal fire. I noted that the risk is low (CDF from internal fires = 3.47 x 10^{-7}/ry) and evenly distributed across the fire compartments with the greatest contributor being the safeguard buildings. The RP noted that safeguard building C compartment (BSC2401SFI) is the highest contributor of risk (13.95% of the internal fire CDF) due to this compartment containing a significant amount of safety system cable and equipment. The next most important fire compartments were

safeguard building A (BSA3301SFI) and safeguard building B (BSB3301SFI) (contribute 11.24% and 9.63% of the internal fire CDF respectively). These fire compartments contain a significant number of cable runs and most of the equipment relating to protection and mitigation functions. Additionally, the RP stated that the contribution of the MCR (BSC33C1SFS) fire is 4.32 x 10^{-9}/ry which amounts to only 1.24%.

377. The TSC and I reviewed the results of the component importance reported through FV importance greater than 5 x 10^{-3} and Risk Achievement Worth (RAW) larger that 2.0 through table T-17-1 and T-17-2 of the revised report (Ref. 48). This review provided me with increased confidence on the data used and the depth of coverage for the Internal Fire PSA. The risk insights provided by the single compartment fires provides confidence on the adequacy of the design features to mitigate the fire risk and the fire risk itself is not disproportionate to the risk from other sources.

378. Overall, I have noted that the internal fire PSA for DR2.1 has reported a CDF of 3.47 x 10^{-7}/ry (compared with the internal events Level 1 PSA CDF of 3.85 x 10^{-7}/ry (Ref. 36)). Like the similar figure for the Level 1 PSA, the estimated Level 1 PSA internal fire PSA CDF is low. Additionally the systematic approach to accounting for all the fire zones including DFM where necessary provides confidence on the adequacy of fire PSA modelling in evaluating the risk arising from internal fire hazards.

379. The TSC and I have assessed the RP’s Multi-Compartment Analysis (MCA) aspect of the revised internal fire PSA in Ref. 48, and noted that the MCA has been performed in a systematic way starting with development of an exposing-exposed compartment matrix, and later narrowing the list by using four stage screening processes to identify the seven scenarios to be taken up for analysis by MOFIS software. The MOFIS analysis was performed for seven MCA scenarios and the results show that none of them would result in damage to the exposed room/compartment. While the detailed MOFIS analysis demonstrated that multi-compartment fires are not likely, the simplified preliminary analysis during the screening process combined the risk of scenarios of MCA fires which was accounted for the in final fire risk aggregation.

380. The TSC and I have assessed the RP’s analysis of cable routing and multiple spurious operations in the revised report. On both the topics, the analysis performed and its traceability through the report meets my expectations. In addition, I will discuss the risk insights arising from these two topics in the following paragraphs.

381. As noted in the DFM risk insights, cable fires dominate the fire risk in most fire compartments. Effectively, cable routing, segregation and separation measures taken through deterministic principles enable the PSA to demonstrate that though the risk from cable fires would dominate the internal fire PSA it is not significant in quantitative terms. This aspect has been discussed in paragraph 376.

382. Similarly, the NEI-00-001 (Ref. 13) procedure of USNRC for multiple spurious operations (MSO) due to hot shorts in electrical equipment (which I consider as RGP) has been used by the RP to identify the MSOs for a systematic consideration of such spurious operations. Through the application of this procedure, the RP has analysed MSO scenarios for the VDA [ASDS] [ASDS] and turbine bypass system control valves. I have assessed the component importance tables of the Internal Fire PSA results and found these to be consistent with the expectations of the USNRC procedure. I also noted the result of contributions of fire compartments shown in Table T-15-73 of the revised internal fire PSA report (Ref.48) shows the contribution of the Turbine Generator Building (BMX) to be 5.48% of the Internal Fire PSA CDF, while those compartments which contain the VDA [ASDS] valves (safeguard building C) contribute to around 4% of the Internal Fire CDF.

383. The TSC advised me that Internal Fire PSA RGP (such as the list in paragraph 369) expects that an important confirmatory task that should be undertaken is a plant walkdown with special consideration of cable layout details for the UK HPR1000. This is not possible until the plant is constructed, and thus as previously discussed, the RP used data from the reference plant (FCG3). This is a limitation of GDA as it is important to validate design assumptions used in the Internal Fire PSA with a plant walkdown, but obviously not possible to be performed during GDA. This activity will only become possible as normal business activities in the site-specific stage for the licensee.

4.15.3 Strengths

384. The internal fire PSA study has been performed in good alignment with RGP and the presentation of Ref. 48 is also of a good quality enabling clear traceability of the information. The specific areas of significant improvements that the RP has demonstrated in the various topics of DFM, MCA, and cable routing consideration has been discussed in my assessment.

385. The RP’s analysis of MSO due to hot shorts in electrical equipment and C&I was systematically analysed and compared favourably with RGP, such as NEI-00-001 of USNRC (Ref. 13).

386. The traceability of IE frequency calculations, component accounting and Internal Fire PSA risk insights were other areas of strength.

4.15.4 Outcomes

387. My assessment of the RP’s submissions on Level 1 Internal Fire PSA against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.15.5 Conclusion

388. Based on my assessment of the revised internal fire PSA (Ref. 48), I am content that the internal fire PSA for UK HPR1000 meets ONR’s expectations compared with RGP such as Table A.1-2.7.2 of TAG 30 (Ref. 4) and SAPs FA.11. and FA.12 (Ref. 2).

4.16 Level 1 PSA: Analysis of Hazards – Analysis of Internal Flooding

4.16.1 Background

389. During Step 3 the RP submitted an Internal Flooding PSA Ver. C (Ref. 39) to estimate the risks from internal flooding from the UK HPR1000 design. The TSC and I reviewed this model (and accompanying report), and found gaps compared with RGP. I subsequently raised RQ-UKHPR1000-465 and RQ-UKHPR1000-0467(Ref.66). The gap that was found in the Step 3 Internal Flooding PSA was a lack of consideration of High Energy Line Breaks (HELBs). The RP decided to revise the Internal Flooding PSA to include consideration of HELBs during Step 4 of GDA. It was agreed that the RP would share with ONR the progress of the revision work and early findings through routine monthly meetings and periodic workshops. This provided a good opportunity to gain visibility of the RP’s work and compare it with RGP.

390. Prior to the RP beginning the revision work, the TSC and I reviewed the revised Internal Flooding PSA methodology and raised RQ-UKHPR1000-0913 (Ref.66). I found that the RP’s revised methodology met with my expectations compared with RGP such as:

- EPRI Report 1019194; and
- ASME/ANS RA-S 2018.

391. I have presented my assessment of the Internal Flooding PSA Ver. D (Ref. 46) report and model in the following paragraphs.

4.16.2 Assessment

392. In Step 4 of GDA for the UK HPR1000, the RP submitted the Internal Flooding PSA Ver. D (Ref. 46) report and model. The TSC and I assessed this report (and accompanying model), and our sample for my assessment was based on the risk significance of the results. My assessment compared the RP's submission against RGP such as ONR SAPs FA.11 and 12 and TAG 30 (Ref 4) and the list above in paragraph 390. Based on this assessment, additional clarifications were sought on the following topics:

- Operator actions in flooding scenarios.
- Analysis of flood propagation.
- Flooding events frequency induced by human actions.
- Identification of resultant scenarios of Level 1 PSA because of flood initiators.
- Assumption on hardware failures.

393. Discussions with the RP provided confidence to me that these areas of the Internal Flooding PSA had been modelled adequately compared with RGP, however the RP had not documented the analysis clearly in Ref. 46. Whilst this gap in the documentation has not prevented me from reaching a judgement in GDA on the adequacy of the RP's approach to internal flooding, it is my expectation that a licensee would address this quality shortfall post-GDA.

394. The TSC and I reviewed Ref. 46. I noted that the RP included a comprehensive review of the HELBs across the plant and identified the flooding compartments which are the highest contributors to the CDF from internal flooding. In my sample for assessment, I selected the compartment BFX10A1FPZ, which is a fuel building flood zone that contains multiple rooms at several elevations. In the internal flooding PSA report a list of 129 components were reviewed by the RP to identify the potential flood sources in this compartment. This list contains identification of potential targets arising from the flooding. The flooding zone I sampled contains one train of components related to the RCV [CVCS], Emergency Boration System (RBS [EBS]), RCS, PTR, fire water system for nuclear island (JPI [FW-NI]) and Demineralised Water Distribution System (SED [DWDS NI]) systems. HELBs in this compartment were shown to have the potential to cause a primary system transient[2] IE resulting in reactor trip. The event progression thereafter is the same as a primary system transient initiating event in Level 1 PSA internal events model. Using the Risk Spectrum model and supporting documentation, I traced the sequences arising from the primary transient initiating event caused by HELB in the compartment BFX10A1FPZ. In my assessment I noted that this HELB would not affect the systems required for the control and mitigation of the transient caused by the occurrence of the HELB. Based on my assessment I am content with the RP's modelling of the accident sequences arising from flooding in compartment BFX10A1FPZ. This provides me with confidence in the broader internal flooding PSA approach and model.

395. The TSC and I assessed the use of operator actions in the Internal Flooding PSA. I noted in my sampling assessment that the IE caused by an HELB in compartment BFX10A1FPZ credits two operator actions to potentially mitigate the accident. The two actions claimed are: operator intervening to stop the flood caused by equipment failure (OP_STOP_EFL) or operator intervening to stop the flood caused by human failure (OP_STOP_HFL). I sought further clarifications through RQ-UKHPR1000-1445. In the response to the RQ, the RP adequately demonstrated the feasibility of these two

[2] *A primary system transient is a change in the reactor coolant system temperature, pressure, or both, attributed to a change in the reactor's power output. Transients can be caused by adding or removing neutron poisons, increasing or decreasing electrical load on the turbine generator, or accident conditions.*

actions, however I found a minor shortfall where the licensee should improve the quality of the safety case. Additionally, in the report (Ref. 46) the RP has reported the sensitivity to the two operator actions. The FV importance for the sequence for flooding in BFX10A1FPZ was reported by the RP to be 0.129, or approximately a 13% contributor to the internal flooding CDF. Thus, the RP concluded that the risk from these accidents sequences, and the human failures modelled in them is low. I am content with the depth and detail provided for the consideration of HRA in the internal flooding PSA.

396. The TSC and I assessed the RP's consideration of hardware C&I failures in the Internal Flooding PSA. The RP's analysis demonstrated that internal flooding is unlikely to pose much risk due to the design rules whereby flooding sources are not allowed to be present where the electrical and C&I equipment are located. Even though the design rules are aimed at minimisation of the flooding risk, the internal flooding PSA needs to consider the residual risk. This aspect has been considered by the RP by modelling the effects of internal flooding on the switch boards and other C&I hardware due to flooding in the designated flooding compartments in Ref. 46. I compared the RP's approach towards consideration of hardware and C&I failures due to internal flooding with RGP, such as that listed in paragraph 390 and found it to be adequate for GDA.

397. Through RQ-UKHPR1000-1445, I sought clarification on the reason for non-consideration of the random failure of the flooding barriers. The RP provided a clarification based on the design of the barriers, which allows them to be treated as having negligible failure probability. I assessed the potential impact of the modelling of the random failure of the flooding barriers on the overall risk due to internal flooding and found it not to be risk significant and hence I consider this a minor shortfall. However, I would expect this aspect of assessing the failure probability of the flooding barriers would need to be revisited by a licensee post-GDA.

398. I engaged extensively with the IH inspector on the topic of HELBs and the fidelity of the high energy piping data provided to ONR. I shared the results of the PSA and the risk significance of the quantification. This engagement has provided increased confidence for me in the consistency of the deterministic and probabilistic aspects for the internal flooding safety case. Overall, based on my assessment of the accident sequences due to flooding of compartment BFX10A1FPZ, operator actions, considerations for C&I failures, and HELB consideration I am content the general modelling of the internal flooding PSA meets ONR expectations.

4.16.3 Strengths

399. The Internal Flooding PSA Ver. D and model (Ref. 46) is a comprehensive revision of the previous study providing a report with adequate detail to enable an independent review of the analysis performed. The traceability of underlying supporting analysis to the model and report was documented well.

4.16.4 Outcomes

400. My assessment of the RP's submissions on Level 1 Internal Flooding PSA against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.16.5 Conclusion

401. Overall based on my assessment of the internal flooding Level 1 PSA, risk insights from it and the supplementary clarifications provided to the RQ-UKHPR1000-1445, I am satisfied that the internal flooding Level 1 PSA meets the expectations of the SAPs

FA.11 and 12, TAG 30 Table 1.2-7 for adequacy of the modelling of the internal flood impact through PSA.

4.17 Level 1 PSA: Analysis of External Hazards and External Flooding PSA

4.17.1 Background

402. In Step 4 of GDA, the RP submitted an External Hazards PSA model and report (Ref. 41) and External Flooding PSA model and report (Ref. 40) using the Bradwell site (a potential site for the UK HPR1000) characteristics. The RP considered it to be proportionate to present a preliminary characterisation of external flooding hazards including a discussion of the external flood hazard envelope for UK sites. A full scope detailed site-specific external flood characterisation can only be performed during the site-specific stage of the project.

403. The TSC and I assessed the External Hazards and External Flooding reports (i.e. Refs 40 and 41) against the expectations of the SAPs FA.11 and 12, and the PSA TAG (Ref. 4). I used TAG 13 (Ref. 4) for judging against adequacy of the external flood characterisation and TAG 30 Table 1.2-7 for adequacy of the modelling of the flood impact through PSA.

404. My assessment of the External Hazards PSA and External Flooding PSA is presented in the following sub-sections. Although seismic hazards are an ‘external hazard’, I have presented my assessment of Seismic PSA for UKHPR1000 in sub-section 4.18 of this report, based on the independent submissions made on the topic by the RP.

4.17.2 Assessment

405. The RP’s stated purpose of the External Flooding and External Hazards PSAs was to estimate the risk arising from damage due to external flooding and other external hazards, and to identify any weaknesses in the design due to these hazards. The approach taken for the External Hazards PSA was to identify the likely initiating event scenarios arising from the various hazards. The scope of the External Hazards PSA covered the following scenarios.

- LOOP caused by strong wind, tornado, and snow;
- secondary system transient induced by the blockage of water intake caused by frazil ice, ice barriers, and organic material in water;
- beyond design basis tornado (two categories: 89 m/s ~ 120 m/s and 120 m/s ~ 134 m/s);
- LOCC induced by blockage of water intake caused by frazil ice, ice barriers, and organic material in water;
- MSLBs downstream of MSIV caused by within design basis tornado (61 m/s ~ 89 m/s); and
- MSLBs downstream of MSIV caused by within design basis strong wind (60.2 m/s ~ 80 m/s).

406. The scope of the analyses covered all sources of radioactivity with the potential for off-site releases or that could escalate to a severe accident in the reactor core and spent fuel pool. The External Flooding PSA included analysis for all buildings of the nuclear island and of the conventional island such as the Turbine Generator Building (BMX) and the Circulating Water Pumping Station (BPW). The PSA models also included all plant operating states including low power and shut down states.

407. In the context of assessment of External Hazards PSA and External Flooding PSA, I worked in close collaboration with the External Hazards specialist inspector of ONR.

408. The external flood characterisation as stated in the report (Ref. 40) includes external flooding defined as a flood initiated outside the plant boundary that can affect the operability of the plant, including both natural events (such as high tide, storm surge, extreme rainfall, tsunamis, etc.), and manmade events (failure of dams, levees, and dikes, etc.).

409. The TSC and I assessed the details of the generic sources of flooding, a selection of sources relevant to the GDA application, hazard curves resulting from the chosen sources, and resultant frequencies of reactor flooding on the broad area of flood characterisation. I compared the RP's submissions against the expectations of ONR TAG 13 and found some gaps in the following areas:

- inclusion of frazil ice as an external hazard for external flooding;
- the justification for the screening out of tsunami wave;
- justification for C&I cabinet and power bus can be guaranteed to operate for 2 hours after the loss of DVL [EDSBVS]; and
- hazard combination justification.

410. To gain clarity on the gaps I identified compared with RGP, I raised RQ-UKHPR1000-1025. I also assessed the hazard combinations and the justification for the specific combinations. I present my assessment of these topics in the following paragraphs.

411. On the query of inclusion of frazil ice in RQ-UKHPR1000-1025, the RP pointed to the External Hazards Level 1 PSA report Rev B (Ref. 87) where this is considered. I reviewed Ref. 87 and found that the CDF induced by organic material in water, frazil ice and ice barriers (grouped consideration) is 5.48 x 10^{-9}/ry. Subsequent to the Rev B of the External Hazards Level 1 PSA, another revision of the report was submitted (Ref. 41) where the reported CDF contribution (grouped consideration) increased to 8.37 x 10^{-9}/ry. However, given the overall external flooding risk is 6.03 x 10^{-9}/ry, the RP stated that the risk from frazil ice is low and proportionate to other external hazards. The total risk from all external hazards (excluding seismic and external flooding) is 2.11 x 10^{-8}/ry.

412. I reviewed the significant contributors to this risk for both frazil ice contribution and external flooding and observed that the Circulating Water System (CRF) pumps are claimed in many accident sequences including the most dominant accident sequence for external hazards. Thus, I sampled the modelling of the CRF system in the External Hazards PSA. The most dominant accident sequence for external hazards is:

- IE – blockage of water intake caused by external hazard;
- CRF pumps are then claimed, if they fail, a secondary side transient is initiated;
- Reactor trip signal is triggered;
- LOOP is not induced;
- RCCA rods insertion is successful;
- PSVs successfully close after opening;
- Secondary cooldown from ASG [EFWS] and VDA [ASDS] fails; and
- ASP [SPHRS] and F&B fail, resulting in core damage.

413. The frequency of this accident sequence was calculated to be 3.75x10^{-9} /ry and contributes towards 17.73% of the External Hazards PSA CDF.

414. I reviewed the RP's modelling of the CRF system in the External Hazards PSA and found that it was adequate for GDA compared with RGP such as the PSA TAG (Ref. 4). In addition, the results of the External Hazards PSA show that the risk from accident sequences that claim the CRF system are low, and thus I am content that the RP has demonstrated that it would not be proportionate to expect further changes in the CRF system design to reduce the risk from this system to be ALARP.

415. The TSC and I reviewed the RP's justification for the screening out of tsunami wave as a hazard for the analysis. I found gaps in the RP's justification for this screening, and thus I raised queries in RQ-HPR1000-1025 on this topic. The RP provided additional systematic review of all the evidence from the Storegga slide event (an underwater event on the edge of Norway's continental shelf) which occurred around 6100 BCE and the North Sea earthquake of 7 June 1931, with an epicentre offshore in the Dogger Bank area (120 km north east of Great Yarmouth). The North Sea earthquake did not cause any noticeable changes on the east coast of UK. Also, the maximum tsunami generated wave height can be bounded by extreme seawater level including storm surge, high tide, wind generated wave, etc. The RP used this information as justification to screen out tsunamis for consideration in the External Hazards PSA because such a low frequency event was not expected to adversely affect the External Hazards PSA CDF results. I was content with the RP's justification for screening and this view was also shared by the external hazards specialist inspector in our interactions. Overall, I was content with the rationale provided.

416. I assessed the justification that the C&I cabinet and power bus can be guaranteed to operate for two hours when there is a loss of DVL [EDSBVS] due to external flood. The RP provided the supporting calculations performed as part of the analysis for environmental requirements for buildings housing C&I cabinets under normal and accident conditions to justify the availability of the power bus. I was content with the evidence provided to justify the claim of two hours of operation to enable function of the ASP [SPHRS] system.

417. As part of an initial review of Ref. 40, I observed a gap in the RP's modelling for the various protective measures such as water sealing for penetrations and doors, with the assumption that the probability of failure of these components is negligible (i.e. these components were assigned a high reliability in the model). I included this query in RQ-HPR1000-1025 (Ref. 66) on this topic. The RP provided additional justification for adequacy of the sealing of penetrations and doors and justification of very low probability of failure based on evidence provided in other design documentation. Additionally sensitivity studies were performed by the RP to show the increase in risk by considering a justifiable failure probability is low. I also observed a gap in the RP's justification for consideration of Loss of Ultimate Heat Sink (LUHS) due to external flooding and included queries on this topic in RQ-HPR1000-1025 (Ref. 66). The RP provided justification for the consideration of LUHS by the use of boundary conditions modelling the loss of Essential Service Water System (SEC) in a LOOP scenario. I am content with the justifications provided for the PSA modelling queries and it provides me with confidence that the identified gaps were in the documentation, rather than the underlying analysis or modelling. Thus, this is acceptable for GDA, but I expect the documentation to be improved for a site-licensing External Hazards PSA.

418. The RP considered the following hazard combinations in Ref. 87:

- High tide and extreme rainfall.
- Wind generated waves and extreme rainfall.
- Storm surge and extreme rainfall.
- High tide and storm surge.
- Extreme seawater level (including storm surge and high tide) and wind generated waves.

419. The TSC and I reviewed a sample of the combined hazard modelling and documentation and found that compared to RGP it met ONR expectations, aside from a combined hazard whereby an external flood resulted in failure of the ASP [SPHRS] to provide cooling to the reactor and makeup water to the SFP concurrently. In the following paragraphs I have presented my assessment for this combined hazard scenario.

420. The ASP [SPHRS] system is a novel feature of the UK HPR1000 design. ASP [SPHRS] serves as the backup means of removing decay heat from the reactor core via the SGs. When the ASG [EFWS] or VDA [ASDS] systems fail, ASP [SPHRS] is claimed by the RP for removing the decay heat of the reactor core via the SGs. The RP also claims the ASP [SPHRS] for providing makeup water to the SFP if all trains of the PTR [FPCTS] cooling loop fail. The ASP [SPHRS] is composed of three identical cooling trains, each serving one SG. Each train consists of one steam inlet pipe, one condenser, feed pipes and associated valves. The condenser is submerged in the water tank which is located on the outer wall of the reactor building.

421. The TSC and I reviewed the External Flooding PSA reports and models (Ref. 40) and noted that the RP had not considered a combined accident scenario where an external flood event occurs, and the ASP [SPHRS] is required to provide makeup to the SFP at the same time as providing cooling to the reactor core. The RP had also not provided justification that the ASP [SPHRS] inventory size was designed to meet both of these demands at the same time. I also noted that the modelling of the SFP and reactor core were not combined into one Risk Spectrum model and thus the combined risk impact was not able to be demonstrated numerically. Thus, I included queries on this subject in RQ-UKHPR1000-1025 (Ref.66).

422. The RP responded that the ASP [SPHRS] system will only be required to provide cooling to the reactor core and makeup to the SFP at the same time in two accident scenarios:

- External flood + LOOP IE, failure of all EDGs, success of SBO DGs, SCD fails and PTR [FPCTS] fails.
- External flood + LOOP IE, failure of all EDGs, failure of all SBO DGs.

423. The RP further stated that in these two accident scenarios, the ASP [SPHRS] was designed to be used preferentially to provide cooling to the reactor core and thus there would be a temporary failure to perform the function of the SFP water makeup during this short time period. The RP noted that the calculated frequency of these accident scenarios was low (<1x10^{-9} /ry) and thus justified for exclusion in the PSA model assessed in GDA. I consider this is a minor shortfall as the scenarios where this matter applies is only applicable for external hazards and seismic events. However, I expect that this matter will be considered in the External Flooding PSA during the site-specific stage of the project, when more detailed design information will be understood for analysing external flooding hazards.

424. As an outcome of the collaborative effort with the External Hazards inspector, RQ-UKHPR1000-1452 (Ref.66) was raised to gain an understanding of the integration of the safety case across deterministic and probabilistic safety studies for external hazards mainly focussed on use of OPEX. In response the RP provided a comprehensive response with clear cross references to the review of the external hazard's PSAs in Rev. D of the ALARP demonstration PSA report (Ref. 56). Overall, this RQ response was assessed to be consistent with my expectations on showing the integration of the safety case across the deterministic and probabilistic topics for external hazards.

425. The TSC and I assessed the RP's use of generic information in the External Flooding PSA (Ref. 40) based on Bradwell B. I found that the use of seawater levels and wind generated wave heights met ONR expectations compared with RGP such as is listed in paragraph 403.

4.17.3 Strengths

426. The external flood characterisation follows a comprehensive consideration of the potential sources, screening of the flooding sources in a systematic manner with traceable justifications.

427. The quantitative analysis including detailed assessment of the hazard curves for rainfall, all the rainfall combined hazards were shown to be of lesser consequence when compared with the extreme sea water level. Finally, only the extreme sea water level combined with wind generated waves was taken for further consideration. The extreme sea water level included the storm surge and high tide combined effect.

428. The PSA models for the external hazards and external flooding and supporting documentation were clearly traceable and justified.

4.17.4 Outcomes

429. My assessment of the RP's submissions on Level 1 External Hazards and External Flooding PSA against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.17.5 Conclusion

430. Overall based on my assessment of the external flooding and external hazards Level 1 PSA, risk insights, and the supplementary clarifications provided to the RQ-UKHPR1000-1025, I can conclude that I am content that these PSAs meet expectations of the SAPs FA.11 and 12, TAG 13 for adequacy of the external flood characterisation and TAG 30 Table 1.2-7 for adequacy of the modelling of the PSAs.

4.18 Level 1 PSA: Analysis of Seismic Hazards

4.18.1 Background

431. Throughout the course of the UK HPR1000 GDA, the RP completed a full scope seismic PSA for the reference plant FCG3. No Seismic PSA models or results were submitted for the UK HPR1000 design. For GDA, it was agreed that the pragmatic approach for the RP to take in Step 4 of GDA would be for it to:

- submit the seismic methodology (Ref. 32) to be applied to UK HPR1000 in the site-specific stage;
- present the risk insights from the full scope seismic PSA performed for FCG3 Ref. 45); and
- discuss the risk insights applied to UKHPR1000 and to show the seismic risks are ALARP.

4.18.2 Assessment

432. My assessment was focussed on the evaluation of the adequacy of the seismic PSA methodology (Ref. 32) and the risk insights from the study (Ref. 45) as well as the RP's discussion of the ALARP implications of the study. The TSC and I assessed these reports against the expectations of the SAPs FA.11 and 12, TAG 13 for adequacy of the methodology adopted for seismic hazard characterisation and TAG 30 (Ref. 4) Table 1.2-7.4 for adequacy of the modelling of the seismic PSA.

433. In my assessment of the seismic risk insights report and the seismic PSA methodology, I have collaborated closely with the external hazards specialist inspector on the deterministic aspects and with the IH inspector on the expectation for the consequential and combined hazards such as seismic induced fire and flood.

434. In my assessment of the methodology adopted for the derivation of the seismic hazard curve I noted that the curve itself is for a site in China and is hence not fully representative of a UK site. The seismic hazard curve is documented to a reasonable level of detail for what would be expected in a PSA report. I have assessed the steps adopted for the seismic hazard characterisation against the expectations of TAG13 (Ref.4) and discussed the adequacy of the approach with the ONR external hazards specialist inspector. The methodology and references cited in the report demonstrates adequate alignment with RGP, such as EPRI TR-3002000709 (Ref. 15) and EPRI TR-103959 (Ref. 16). At a later stage of any project to build a UK HPR1000 reactor design in the UK, a UK site-specific seismic hazard will need to be specified and substantiated with greater details on the modelling and parameter values than have been provided during GDA. However, I am satisfied the submissions provided by the RP are adequate for the assessment judgements I have made in GDA.

435. Early in Step 4 of GDA prior to the completion of the risk insights report, the RP shared the seismic PSA methodology. I assessed the methodology and sought some clarifications through RQ-UKHPR1000-721.One of the key clarifications provided in the RQ-UKHPR1000-721 response (Ref. 66) was the incorporation of the combined and consequential hazards arising out of the seismic event. The RP has in the qualitative methodology shown that the SSCs relevant to the seismic-induced fire or flooding are identified and listed in the Seismic Equipment List (SEL), such as, induced fire due to the ignition of flammable material in tanks, vessels, pipes, loose wires; induced flooding due to failure of tanks and pipes of filled water, etc. The approach also sets out to systematically identify all potential sources of fire or flood hazards to determine whether their failures can induce fire or flooding, and further impact equipment in the vicinity according to their seismic capacities and arrangement. I consider this approach to the modelling of combined and consequential hazards is proportionate and targeted. I am content with this approach.

436. Consistent with the expectations set out in the RP’s methodology report, the seismic impact report clearly documents the SEL and the associated decisions made to generate that list (Ref.45). I raised a few questions included in RQ-UKHPR1000-1100 pertaining to the inclusion of equipment potentially lost due to seismic induced floods and not included in the seismic equipment list. The RP responded by pointing to the systematic review on the topic of seismic induced flooding in the building screening tables and seismic equipment list of the risk insights report, though the risk of seismic induced flooding was assessed to be low for FCG3. Additional information in the deterministic safety case documentation for external hazards was also cited. Additional evidence from the internal flooding PSA equipment review was used to demonstrate the overlap between the flooding risk component and seismic risk components. In my opinion, through its RQ response, the RP has adequately demonstrated that the risk due to consequential hazards has been accounted for.

437. In my RQ-UKHPR1000-1100, I had also raised a query regarding the reproducibility of the inputs for the seismic initiating event frequencies for the Risk Spectrum modelling from the seismic hazard curve. The RP provided clarification showing the detailed procedure of the Monte Carlo simulation approach adopted on the fragility curves to arrive at the initiating event frequencies. I am content with this approach and the traceability could be confirmed for the seismic initiating event frequencies.

438. As a part of the seismic risk insights report, the RP has provided a review of sixteen significant design differences (Table T-5.1-1 of Ref. 45) of DR2.1 of UKHPR1000 with FCG3 to provide confidence on the reading across of the risk insights from the FCG3 report. The sixteen design differences were, for example, modification of KDS [DAS] (addition of a division and higher classification), modification of SBO DGs (now of higher classification), modification of layout for the Steam Generator Blowdown System (APG [SGBS]) (to design against missile hazards), and HVAC system modification to meet indoor condition requirements. The RP concluded that these design differences

would not change the inputs of the seismic Level 1 PSA model to cause any impact to the seismic risk. I am satisfied that the review's conclusions are reasonable and consistent with RGP such as EPRI-3002000709 (Ref. 15).

439. The RP submitted several sensitivity cases (Section 5.3.1 of Ref. 45) including:

- the increased annual exceedance frequency due to adopting a site-specific hazard curve for UKHPR1000;
- potential UKHPR1000 specific human failure events;
- improved seismic capacity of severe accident C&I system components; and
- LOOP frequency impacted by seismic events.

440. Using these sensitivity cases the RP stated that a change of seismic hazard curve and a change in the seismic induced LOOP frequency has the highest risk significance. In Ref. 53, the TSC checked the veracity of the sensitivity results through an independent analysis by using a UK generic site hazard curve (which was found to be enveloped by the HPC seismic hazard curve). This analysis was performed using an alternative simplified method, by scaling the RP's FCG3 results to the UK generic hazard curve (without accounting for any screening impacts). The RP found that their analysis resulted in a CDF of $4.7\text{x}10^{-6}$/ry (compared with the CDF for FCG3 reported in Ref. 45: $2.29\text{x}10^{-8}$/ry). The RP explained that this significant different in CDF for the seismic PSA is a result of using the generic site hazard curve as it was higher than the FCG3 hazard curve for certain higher peak ground acceleration intervals by an order of 100 or more. Further sensitivity analysis performed by the RP (Section 5.3.1 of Ref. 45) resulted in a seismic PSA CDF of $2.0\text{x}10^{-7}$/ry when the RP used a multiplier of 10 for the annual exceedance frequency.

441. I compared the sensitivity analysis case performed by the RP and the independent analysis of ONR TSC, to form my opinion. I found that the RP's use of more conservative input parameters accounted for the increased Seismic PSA CDF, and thus, gives me the confidence that the site-specific hazard curve is the most risk significant input for the seismic PSA (as was stated by the RP in Ref. 45). Thus, I am content that the sensitivity analysis provided by the RP meets regulatory expectations compared with RGP such as is listed in paragraph 434. However, the site-specific hazard is clearly a significant consideration for any probabilistic analysis of the seismic risks for a specific deployment of a UK HPR1000 unit, and therefore I am limited in what I can conclude in GDA. I am reassured that the FCG3 seismic PSA CDF is low, and the supporting sensitive analysis gives me that confidence that the risk from seismic hazards from the UK HPR1000 should be commensurately low. Additional work will be necessary when a site is selected.

442. The RP presented a comparison of the FCG3 seismic PSA CDF and the FCG3 internal events Level 1 PSA in Ref. 45. The seismic PSA CDF of FCG3 was found to be $2.29\text{x}10^{-8}$/ry (compared with the internal events Level 1 PSA of FCG3: $2.0\text{x}10^{-7}$/ry). Based on previous PSAs performed for plants internationally where the seismic risk is small due to the siting of the plant on a low to medium seismic hazard site, it is expected that the seismic risk would be about 10% of the internal plant risk. This approximately matches what was presented in Ref. 45 for FCG3. However, this quantitative aspect would at best be indicative, as the plant design and hazard curve is related to the reference plant and not the UK HPR1000 design or the probable site. In my opinion, even though for FCG3 the seismic PSA CDF was approximately 10% of the internal events Level 1 PSA CDF, the UK HPR1000 seismic CDF is still largely not understood as the seismic PSA results are extremely sensitive to site-specific parameters.

443. The agreed position for Step 4 of GDA was to submit a seismic PSA methodology and a risk insights study for seismic hazards. As my assessment shows, this objective is

met. However, I observed that the seismic risk insights study only provided risk insights up to Level 1 PSA.

444. Based on the preceding paragraphs, I have identified a limitation in the UK HPR1000 safety case regarding the probabilistic seismic risk assessment:

- The RP did not submit a seismic PSA for the UK HPR1000 design.
- The RP has not used a site-specific seismic hazard curve in their preliminary seismic risk insights study.
- The risk insight study seismic CDF is highly sensitive to site-specific input parameters.
- The RP did not calculate a seismic LRF in the risk insight study.

445. These matters can only be fully resolved in the site-specific and detailed-design stage of work. This is a risk significant matter and requires tracking to resolution. This gap is recorded in Assessment Finding AF-UKHPR1000-0185 in accordance with ONR guidance (Ref. 1).

> AF-UKHPR1000-0185 – The licensee shall, as part of site-specific and detailed design activities, undertake PSA analysis to demonstrate the risk from seismic events. This should include both Level 1 and 2 PSA for all categories of initiating events and plant operating states.

4.18.3 Strengths

446. The seismic risk insights report for the FCG3 design was useful for my assessment and had a broad scope.

447. The RP conducted a systematic review of the UK HPR1000 design against the reference plant FCG3 to demonstrate the adequacy of the UK HPR1000 design to respond to seismic initiating events. The RP found that design differences between FCG3 and UK HPR1000 did not have any significant effect on results of the seismic PSA.

4.18.4 Outcomes

448. As a result of the RP not submitting a UK HPR1000 seismic Level 1 and Level 2 PSA and using a generic seismic hazard curve instead of a site-specific seismic hazard curve, a site-specific seismic PSA will need to be completed by a licensee.

4.18.5 Conclusion

449. Overall, I am content that the seismic PSA methodology and the seismic risk insights report meets the objective of GDA. I found these reports to be aligned with RGP and met my expectations against SAPs FA.11 and 12, TAG 13 for adequacy of the methodology adopted for seismic hazard characterisation and TAG 30 Table 1.2-7.4 for adequacy of the modelling of the seismic PSA. Notwithstanding this conclusion, I have raised Assessment Finding AF-UKHPR1000-0185 as the RP did not use a site-specific seismic hazard curve, presented seismic risks from FCG3, and did not submit a UK HPR1000 Seismic Level 1 PSA and Seismic Level 2 PSA.

4.19 Level 2 PSA: Overall Scope and Approach

4.19.1 Background

450. During Step 4 of GDA, the TSC and I assessed the Level 2 PSA Ver. A model and report (Ref. 50) submitted by the RP towards the end of Step 3. The TSC and I found

gaps compared with RGP such as the PSA TAG (Ref. 4) and thus, I raised questions in RQ-UKHPR1000-0227, 0308, 0425 and 0576 (Ref.66). After further discussions with the RP, there remained some gaps in the Level 2 PSA in the following areas which I sought resolution of through RO-UKHPR1000-0047 (Ref. 57):

- Definition of Large Releases (see sub-section 4.19.2)
- Release category definitions and interface with the Level 3 PSA (see sub-section 4.23.2)
- Containment fragility and supporting analysis (see sub-section 4.19.2)
- Phenomenology analysis supporting the Containment Event Tree (CET) modelling (see sub-section 4.21.2)
- Equipment survivability (see sub-section 4.19.2)
- Level 2 PSA ALARP review (see sub-section 4.24.2)

451. To address the gaps identified in RO-UKHPR1000-0047, the RP submitted the Level 2 PSA Ver. B report and model (Ref. 42) in Step 4 of GDA. The TSC and I assessed Ref. 42 and the sub-sections below present my assessment of this model and report. In addition, the RP submitted a Level 2 PSA Ver. C report and model (Ref. 52). I assessed this version at a high level to confirm that the RP's commitments were included in the final GDA version of the Level 2 PSA.

4.19.2 Assessment

452. The key SAPs (Ref. 2) applied within my assessment are FA.11 which expects the PSA to adequately represent the design and operations and FA.12 which expects that the PSA should cover all significant sources of radioactivity, all permitted operating states and all initiating faults. More specific guidance for my assessment was based on ONR PSA TAG 30 (Ref. 4) sub-sections relevant to Level 2 PSA models, in particular Table A.1-3.

453. In my assessment of Level 2 PSA, I collaborated with the SAA, Chemistry and Civil Engineering specialist inspectors from ONR to gain insights from their assessments and share mine. The engagement across these disciplines provided better understanding of the severe accident systems, methodology for source terms calculations and containment fragility analysis.

454. The Level 2 PSA Rev B report (Ref. 42) provides a summary of the discussion provided in historical international Level 2 PSA studies such as those for UK GDAs of UKEPR, UKAP1000, UKABWR and USNRC guidance in NUREG-2122 (Ref. 9) on the definition of LRF. This review by the RP concluded that there is no standard definition of the LRF. Therefore, a conservative definition of the LRF was adopted for UK HPR1000 wherein all the releases have been grouped under LRF, without differentiating between the large and non-large releases. This resulted in a conservative approach whereby the RP grouped accident sequences which claim success for filtered containment venting and containment sprays as LRF. To understand the importance of this modelling approach, my TSC used the RP's Level 2 PSA model and assigned these same accident sequences as non-LRF (i.e. for successful filtered containment venting and late failures with containment spray operational). The TSC's analysis showed that LRF was reduced by 5%. This result showed the effectiveness of the containment venting and sprays, but by modelling these systems in the conservative manner that was chosen, the RP did not gain insight into the importance of these two systems for the Level 2 PSA results. For the purpose of GDA, as the overall releases are captured through the LRF, I am satisfied this can be considered a gap in the modelling approach. I am content that the further refinement of the LRF definition to separate it from non-LRF can be undertaken as part of ongoing development in the site-specific stage of any UK HPR1000 project. Hence, I am satisfied that the RP's approach on LRF is adequate for GDA.

455. The fragility curve for the containment building is an important input to the Level 2 PSA. The TSC and I worked with the ONR Civil Engineering Inspector to perform a focussed assessment of the supporting documentation on this topic with support of the ONR Civil Engineering TSC as the ultimate capacity analysis of the containment building is the basis for the fragility curve evaluation. The PSA TSC found gaps in the RP's analysis (Ref. 53) and provided feedback to me on these gaps, thus I raised questions in several RQs. The areas in the safety case where I found gaps that I identified in the RP's approaches for containment analysis were as follows:

- methodology for the fragility curves did not include treatment of epistemic and aleatory uncertainties;
- containment failure modes considered for the analysis; and
- application of the Latin hypercube sampling methodology

456. In discussions with the RP, I identified that these were gaps in the safety case that should be resolved during GDA, and thus I included them in RO-UKHPR1000-0047 (Ref. 57). In response to this RO, the RP submitted Ver. B of the Level 2 PSA (Ref. 42).

457. The RP's revised methodology for analysis of the fragility curve used in Ref. 52 incorporated the effect of epistemic and aleatory uncertainties. The failure probability of the containment building was shown to increase substantially, however, this only had a negligible impact on the LRF. Ref. 52 also included application of a Latin hypercube sampling methodology to the uncertainty analysis which is expected in RGP. I assessed these aspects of Ref. 52, and they compare favourably with RGP such as is listed in paragraph 452. I am content with the RP's approach on these Level 2 PSA topics including application of the containment fragility curve for the Level 2 PSA. However, I have noted that a gap relating to the details of the methodology for the ultimate capacity analysis for the containment, is identified through the Civil engineering assessment report (Ref. 89), which would in turn could affect the containment fragility. This matter is discussed in greater detail in the Civil engineering assessment report (Ref. 89).

458. The TSC and I reviewed the RP's integration of the hazards PSAs into the Level 2 PSA. One aspect I reviewed was the RP's use of boundary conditions for internal fire Level 2 PSA. I sampled the RP's use of boundary conditions (found in Table 4.10.2-2 of Level 2 PSA or Ref. 42) for a fire in the reactor building fire compartment BRX15A1ZFS. This compartment includes rooms which house Accumulator tanks & valves train A, RCV valves, SG1, RCP [RCS] 1, Containment Internal Filtration System (EVF) and Containment Cooling and Ventilation System (EVR) equipment and fans. The boundary condition used by the RP for this part of the analysis assumes the loss of all equipment in this fire compartment. I am satisfied that the RP has used appropriate boundary conditions which consistently capture the loss of components due to internal fire and propagated these from the Level 1 PSA model into the Level 2 PSA sequences. For the area that I sampled, I am content with the integration of the Level 2 modelling into the hazards PSA. Further assessment on the comparative risk insights from quantitative results of integration of hazards in LRF estimates is discussed in a later sub-section in this report when I discuss my assessment of the Level 2 PSA results.

459. The TSC and I reviewed the RP's analysis of the survivability of equipment in severe accident scenarios and compared this with RGP. The regulatory expectation based found in the PSA TAG is for a systematic review of all the components modelled in Level 2 PSA to justify the qualification and demonstrate survivability. In Ref. 42, the RP presented a systematic review of 996 components modelled in the Level 2 PSA and identified a small subset of 16 component groups which could experience the harsh environment during a severe accident scenario of extreme pressure, high temperature, and severe radiation conditions. I sampled the RP's sensitivity study in Ref. 42 for the

loss of the RIS [SIS] valves and the loss of the RIS [SIS] water filters due to severe accident conditions. The RP concluded that failure of these components during a severe accident increased the Level 2 PSA results significantly, and thus these components were justified for qualifying them for severe accident conditions of operation. The recommendations related to the equipment survivability are part of the ALARP demonstration for PSA report (Ref. 56) which I assess later in this report. In my opinion, the sample I reviewed of RP's analysis of the survivability of equipment in severe accident scenarios met regulatory expectations such as the PSA TAG (Ref. 4) and provides me with confidence that the rest of the analysis would likewise meet similar expectations.

460. The TSC and I reviewed the sensitivity of the assumptions made about the reliability of Passive Autocatalytic Recombiners (PARs) in the Level 2 PSA (Ref. 42). The RP stated that the PARs have been designed with adequate redundancy and operate in a completely passive manner with no dependency on control or activation signal and thus, the RP screened PARs from the Level 2 PSA model. The RP provided a sensitivity analysis case to understand how the Level 2 PSA LRF would be affected if the PARs were included in the Level 2 PSA. This sensitivity case used a pfd of 1 x 10^{-3} for the PARs, and the results showed a slight increase of 1.65% of the LRF. The actual failure rate of PARs is considered by the RP to be much lower than the pfd used in the sensitivity case, and thus even less of a contributor to the Level 2 PSA LRF than was calculated. I am content with the RP's decision to screen the PARs for explicitly inclusion in the Level 2 PSA, as the arguments were reasonable, and the sensitivity case demonstrated that if the PARs were included they would have limited effect on the Level 2 PSA results.

4.19.3 Strengths

461. The Level 2 PSA approach and scope generally compares favourably with RGP.

462. Detailed Level 2 PSA is carried out for the internal fire, internal flooding, and external hazards (excluding seismic). The RP's use of boundary conditions for Level 2 hazard PSA was a strength.

4.19.4 Outcomes

463. My assessment of the RP's submissions on Level 2 PSA approach and scope against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.19.5 Conclusions

464. I found the Level 2 PSA approach and scope to compare favourably with RGP such as Table A.1-3 of the PSA TAG and SAPs FA.11 and 12.

4.20 Level 2 PSA: Plant Damage States

4.20.1 Background

465. The Plant Damage State (PDS) analysis provides the linking between the end states of Level 1 PSA and the initiators in the Level 2 PSA. The linking is done with the help of defining the attributes of the end states and using the attributes to group various core damage sequences to model through the CETs of the Level 2 PSA.

4.20.2 Assessment

466. The Level 2 PSA Rev B (Ref. 42) presented a coherent picture of the linking of the core damage sequences Level 1 PSA to the PDS which is the starting point of Level 2 PSA event trees. I assessed the veracity of the PDSs presented in Level 2 PSA Rev B

(Ref.42). I raised several queries through RQ-UKHPR1000-1646 (Ref.66). The RP in the response to RQ-UKHPR1000-1646 provided a more structured representation of the criteria used in the binning of the CDF sequences into the PDSs along with the rationale. Additionally, I traced the use of the CDF sequences binned through the PDS in the Risk Spectrum model where the Level 1 PSA and Level 2 PSAs are linked through the features of the software. This response to the RQ and my assessment of the model provided me the necessary confidence on the veracity of the decisions made through the logic tree shown in the revised Level 2 PSA report.

4.20.3 Strengths

467. A reasonable set of PDS attributes have been identified and applied. The Level 2 PSA model includes detailed system models for systems designed to mitigate severe accidents, for example containment isolation systems. The features of the Risk Spectrum software are used in linking Level 1 and Level 2 PSA sequences ensuring no loss of frequency due to simplifications. Each PDS is represented by the end state of the Level 1 to Level 2 interface logic tree. The logic trees in the Level 2 PSA documentation are presented with the criteria and discussion to show how the core damage sequences from Level 1 PSA are reduced to a justified number of PDSs to be progressed through CETs. The CETs are clearly discussed in the documentation. Severe accident management operator actions are modelled in CETs. Fission product RCs are defined and assigned to the CET end states.

4.20.4 Outcomes

468. My assessment of the RP’s submissions on plant damage states against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.20.5 Conclusions

469. Overall based on my assessment Level 2 PSA on the topic plant damage states**,** I am content that the analyses for this topic meets ONR’s expectations for Level 2 PSA models for the UK HPR1000 in Table A.1-3 of TAG30 and SAPs FA.11 and 12.

4.21 Level 2 PSA: Phenomena Analysis

4.21.1 Background

470. On the topic of phenomena analysis for Level 2 PSA there is a strong link to the deterministically performed SAA (see SAA AR – Ref. 63). The key phenomena of severe accidents considered for deterministic safety analysis of UKHPR1000 are High Pressure Melt Ejection (HPME), DCH, hydrogen combustion, MCCI, steam explosion, containment overpressure, and re-criticality. The deterministic analysis of these phenomena is not within the scope of this AR, however, the RP used information obtained from the deterministic analysis of these phenomena in the Level 2 PSA. My assessment of the RP’s use of phenomena analysis in the Level 2 PSA is presented in the following paragraphs. I compared the RP’s analysis with RGP such as: IAEA SSG-4 (Ref. 8), the PSA TAG (Ref. 4) and SAPs FA.14 and FA.15 (Ref. 2).

4.21.2 Assessment

471. In my assessment of the Level 2 PSA Rev B (Ref.42), I focussed on the depth of the substantiative analysis supporting the identification of the various phenomena that impact severe accident scenarios. the PSA TAG (Ref. 4) expects that the Level 2 model should consider all potentially significant phenomena, and these should be subject to detailed analysis, considering the scenario and appropriate boundary conditions. The RP presented in Ref.42 its phenomena analysis by referring to relevant generic studies such as NUREG-1570 for SGTR/HLR analysis (Ref. 9) and a design-

specific study that was performed and reported for the hydrogen phenomena of UK-HPR1000 design.

472. The TSC and I reviewed the RP's phenomena analyses in Ref. 42 and found gaps compared with RGP on the hydrogen phenomena, in-vessel steam explosion, ex-vessel steam explosion, HPME, DCH, MCCI, long term containment overpressure, and induced SGTR/hot leg rupture (HLR). I raised several RQs, and the RP provided additional supporting analysis results for the modelling of these phenomena in the Level 2 PSA. The responses on all the phenomena were adequate except for SGTR/HLR supporting analysis. In my opinion, further justification was still necessary to substantiate the basis for the modelling. As a result the RP subsequently revised its initial response to RQ-UKHPR1000-1596 (Ref.66) with the addition of the sensitivity studies showing a ten-fold increase in the probability of the induced SGTR. The impact on of the induced SGTR on LRF was shown to be insignificant. Overall, I am content with the use of the Level 2 PSA supporting analysis for phenomena.

473. The TSC and I noted that the RP did not use bespoke analysis to support the Level 2 PSA modelling of HLR and SGTR, in the event of any delay in the opening of the SADVs in a severe accident scenario caused by either a LOOP or primary transient IE. The RP provided sensitivity analysis for this accident scenario which demonstrated that the LRF was not affected by using the generic analysis. Thus, I am content in the RP's use of generic analysis for these two areas of the Level 2 PSA phenomena analysis.

4.21.3 Strengths

474. The RP's phenomena analysis supporting Level 2 PSA modelling was detailed and contains thorough substantiation. The approaches used compared favourably with RGP.

4.21.4 Outcomes

475. My assessment of the RP's submissions on Level 2 PSA phenomena analysis against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.21.5 Conclusions

476. Overall based on my assessment Level 2 PSA on the topic phenomenon analysis, I am content that the analysis for this topic meets ONR's expectations for Level 2 PSA models for the UK HPR1000 in Table A.1-3 of TAG30 and SAPs FA.11 and 12.

4.22 Level 2 PSA: Containment Event Trees

4.22.1 Background

477. CETs represent the progression from plant damage states identified as output from Level 1 PSA to RCs (RCs are a group of accident progression sequences that would generate a similar source term to the environment). CETs are used in modelling Level 2 PSA in the Risk Spectrum software. The function events considered within the CETs are divided into different time stages as follows:

- T1: the stage before RPV failure;
- T2: the time of RPV failure; and
- T3: a significant length of time after RP failure.

4.22.2 Assessment

478. The TSC and I assessed the revised Level 2 PSA CETs and found gaps in the substantiation and documentation of the CETs compared with RGP such as the PSA TAG (Ref. 4) on the topics of:

- phenomenological uncertainty for the successful operation of IVR;
- re-criticality;
- reliability of the Containment Combustion Gas Control System (EUH [CCGCS]) system; and
- documentation of supporting information on the hydrogen combustion analysis leading to deflagration loads.

479. To seek more information regarding these gaps, I included several questions on these topics in RQs. The RP in its response to the RQs provided additional information, justifications, and sensitivity studies to answer the queries.

480. The RP referred to various other analyses performed to substantiate the EUH [CCGCS], assessment of criticality, assessment of EUH [CCGCS] by computational fluid dynamics (CFD) method, and sensitivity studies on key parameters of IVR analysis.

481. The RP submitted the Level 2 PSA version C (Ref. 52), and I reviewed the RP's revised documentation of the above areas. In particular I sampled the RP's substantiation of the branch point probabilities on the CETs and the reliabilities of the components modelled within containment systems such as the EUH [CCGCS] system. In the Level 2 PSA version C, I found the evidence and substantiation to be reasonable and adequate. Thus, I am content with the RP's CET modelling for GDA.

4.22.3 Strengths

482. The traceability of the supporting analysis provided through the various topics of the Level 2 PSA to interpret the CET branch points and probabilities was a strength in Ref. 52.

4.22.4 Outcomes

483. My assessment of the RP's submissions on CETs against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.22.5 Conclusions

484. Overall based on my assessment of the Level 2 PSA on the topic of CETs, I am content that the analysis for this topic meets ONR's expectations for Level 2 PSA models for the UK HPR1000 in Table A.1-3 of the PSA TAG and SAPs FA.11 and 12.

4.23 Level 2 PSA: Release Category and Source Term Analysis

4.23.1 Background

485. As stated previously, the CET sequences are assigned to various RCs. Each of the RCs are then analysed and source terms are assigned to each. The RC frequencies and source terms (measured in quantities of radionuclides) are then input into the Level 3 PSA calculations.

4.23.2 Assessment

486. The TSC and I assessed the Level 2 PSA (Ref. 42) treatment of the RCs and compared this with RGP such as the PSA TAG (Ref. 4). I observed that the RP has

undertaken a systematic and structured analysis and selection of RC attributes, developed mapping of the attributes to each of the RC, assigned accident sequences to the RCs, presented source terms for each RC, and calculated the frequency for each RC. While at a high level this analysis has been reasonably presented, I found the following areas where there were gaps in the RP's documentation of attributes used for defining the RCs:

- primary circuit pressure during severe accident scenarios leading to core damage;
- passive capture feature of releases within containment or outside containment based on release location;
- time of releases at the end of the CET sequences is typically influenced by conditions at the start of an accident; and
- initiation conditions used in high primary circuit pressure after an SBO compared with low primary pressure after a LB-LOCA.

487. I discussed these gaps in the documentation with the RP and raised questions in several RQs. The RP explained that the attributes were included in analysis, however they had not been documented in Ref. 42. The RP also presented further evidence and an improved documentation on these topics in the revised Level 2 PSA (Ref. 52). The RP explained that for the high primary pressure after an SBO compared with a low primary pressure after a LB-LOCA, both scenarios are assigned the same RC (RC201) in the analysis. I assessed the responses and note that the impact of SADVs opening on SBO scenario is the basis of the evidence presented. In addition, in the revised Level 2 PSA (Ref. 52), I found the documentation of these areas to be improved and thus the gaps I had found in the documentation of the RCs were closed. I am content in the RP's treatment of RCs for GDA.

488. The TSC and I assessed the RP's source term analysis in Ref. 42. For GDA, the source term analysis was primarily assessed by the ONR Chemistry specialist inspector (see Ref. 43) for ONR's detailed assessment of the source terms), although I assessed the treatment of source terms in the Level 2 PSA. I collaborated with the Chemistry inspector through several meetings during GDA. The ONR chemistry inspector concluded that the RP has developed an adequate source term for severe accidents, and the modelling work they have undertaken (using the code ASTEC) is also reasonable and conservative. The ONR chemistry inspector identified a shortfall which involved the assumptions made by the RP regarding the pH of the IRWST, which could result in an underestimate of volatile iodine, which is one of the more significant elements in terms of dose. The Chemistry inspector raised an Assessment Finding to close this gap.

4.23.3 Strengths

489. The Level 2 PSA Rev C (Ref. 52) has presented a clearly traceable and justified attribute list for the RCs.

4.23.4 Outcomes

490. My assessment of the RP's submissions on release category and source term analysis against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.23.5 Conclusions

491. Overall based on my assessment of the Level 2 PSA Ver. B (Ref. 42) and Ver. C (Ref. 52) on the topics of release category and source term analysis, I am content that the analyses for these topics meet ONR's expectations for Level 2 PSA models for the UK HPR1000 in Table A.1-3 of TAG30 and SAPs FA.11 and 12.

4.24 Level 2 PSA: Overall Results

4.24.1 Background

492. The CET sequences are used to quantify the sequence frequencies. The sequences in the CETs are assigned to various RCs. These RC frequencies are carried forward as input to the Level 3 PSA. The overall results of Level 2 PSA Rev B (Ref. 42) are reported in terms of LRF and RC frequencies.

4.24.2 Assessment

493. The TSC and I assessed the results of the Level 2 PSA and risk insights against expectations of the PSA TAG. In the Level 2 PSA report Rev B (Ref. 42) the overall contribution of the all the hazards (excluding seismic) presented as a summation with the internal event PSA results are discussed.

Table 8: LRF of different types of Initiating Events (Ref. 42)

Initiating Event type	LRF (1/ry)	Contribution (%)
Internal Event	6.05 x 10^{-8}	68.52
Internal Fire	1.51 x 10^{-8}	17.10
Internal Flooding	1.34 x 10^{-9}	1.52
External Hazards (excluding seismic initiators)	5.28 x 10^{-9}	5.98
External Flooding	6.03 x 10^{-9}	6.83
Total	8.83 x 10^{-8}	100

494. Similarly, based on the reported results for CDF, I have populated a summation of the CDF for different initiators to make a comparison against relative contributions for LRF.

Table 9: CDF from different types of Initiating Events

Initiating Event type	Point estimate CDF (1/ry)	Reference	Contribution (%)
Internal event	3.85 x 10^{-7}	Ref. 36	50.39%
Internal fire	3.47 x 10^{-7}	Ref. 48	45.42%
Internal flooding	4.65 x 10^{-9}	Ref. 46	0.61%
External hazards (excluding Seismic initiators)	2.11 x 10^{-8}	Ref. 41	2.76%
External Flooding	6.03 x 10^{-9}	Ref. 40	0.79%
Total	7.64 x 10^{-7}		100%

495. Based on the two tables reported above, I have reviewed the relative quantitative values in the internal flooding and external hazards in the Level 1 PSA (CDF) and Level 2 PSA (LRF) aggregation. The percentages are similar across both the tables. This appears reasonable. However, the fire IEs contribute about 18.37% of the Level 2 PSA LRF aggregation, while it is 45.69% for the Level 1 PSA CDF aggregation.

496. Review of the Level 2 PSA results shows that the difference of contribution of fire events to the aggregated CDF and LRF to be reasonable. This difference arises mainly due to different RCs which are present in the Level 2 PSA for internal events in comparison to internal fire PSA. In the internal events Level 2 PSA the LRF is due

mainly to RC503 (T3 stage, long-term containment rupture due to MCCI with spray), RC504 (T3 stage, long-term containment rupture due to MCCI without spray), RC 205 (T1 stage, containment overpressure in early stage), and RC 501 (T3 stage, no vessel failure, no long-term containment overpressure failure due to the success of EUF). Whereas in internal fire Level 2 PSA has a contribution from only RC504, RC501 and RC205. The absence of some of the sequences in the internal fire PSA is reasonable as such sequences are logically impossible.

497. Review of the Level 2 PSA results shows that the dominant contributors to LRF are reported in the component importance tables (T-4.11.2-1 of Ref. 42) followed by a discussion. The results indicate that risk significant components are the DEL chillers, the 380V transformers of the emergency power distribution system, the DVL [EDSBVS] fans and the RPS software. CCFs for these components effectively lead to multiple mitigating system failures and hence contribute significantly to LRF. The results and the discussion in the Level 2 PSA Rev B (Ref. 42) to explain the contribution, is reasonable.

498. I have considered the impact of variations in the design references for Level 1 and Level 2 PSA on the results. The Level 1 PSAs for internal events, internal fire, internal flood, external flooding, and external hazards (excluding seismic) are all performed using the same design reference: DR2.1. In contrast, the Level 2 PSA has assumed design details from the earlier DR1 to model internal fires, internal floods and external hazards. However, I am satisfied that the design changes from DR1 to DR2.1 relevant to hazards are small variations in the design and are not likely to have a significant impact on severe accident phenomena or CET progression modelling for hazards initiators. Therefore, I consider LRF from hazards is reasonably calculated and aggregated for Step 4 of GDA. Although the DAC is against DR3, my detailed assessment was of the Level 2 PSA based on earlier DRs. My detailed assessment of the Level 2 PSA from DR2.1 has provided me with confidence that the actual LRF of the DR3 should be similar or slightly lower than that reported for earlier DRs.

499. In Tables 8 and 9 seismic risk is missing from the Level 2 PSA results. This remains an important omission as there is an area of unknown risk in the Level 2 PSA for GDA and requires tracking by ONR through to resolution. This matter is captured in Assessment Finding AF-UKHPR1000-0185.

500. I have also considered the impact of the severe accident management guidelines (SAMGs) and emergency operating procedures (EOPs) on the results of Level 2 PSA. It is noted that in the analysis submitted for GDA the SAMGs and EOPs of the reference plant FCG3 were assumed to apply. In my opinion the use of reference plant details for EOPs and SAMGs is reasonable for GDA.

501. Overall, the results provide the insights desirable from Level 2 PSA, and provide confidence on the modelling of severe accident mitigation systems in the Level 2 PSA. I am content with the insights presented for the Level 2 PSA for GDA.

4.24.3 Strengths

502. The use of Risk spectrum for the integrated Level 1 and 2 analysis provides a clear way forward to the use of the PSA towards PSA applications post-GDA.

4.24.4 Outcomes

503. As a result of the Level 2 PSA not including seismic hazards, the licensee will need to complete a site-specific seismic PSA including Level 2 PSA aspects.

4.24.5 Conclusion

504. Overall based on my assessment of Level 2 PSA results and ALARP, I am content that Level 2 PSA for internal events, and hazards (excluding seismic) for HPR1000 meets ONR's expectations for Level 2 PSA models in Table A.1-3 of TAG30 and SAPs FA.11 and 12 for GDA. Notwithstanding this conclusion, the matter discussed in paragraphs 499 and 503 is captured by the Assessment Finding AF-UKHPR1000-0185.

4.25 Level 3 PSA

4.25.1 Introduction to Level 3 PSA

505. The RP has submitted a Level 3 PSA report (Ref. 44) to summarise the results of the L3 PSA model for individual and societal risk and compare the results against the Targets 7-9 of the ONR SAPs (Ref. 2). Level 3 PSA presents the consequences of radionuclide release during accident conditions from a nuclear facility including analysis of the release of radionuclides and their transfer through the environment with risks to the public from off-site releases.

506. The RP also submitted a Level 3 PSA Methodology (Ref. 25) and compared it with Refs 8, 90 and 18. The RP claimed that this methodology conforms with the referenced RGP as well as Level 3 PSAs performed recently for previous GDAs in the UK.

507. The RP used the PC-COSYMA software for all dispersion and dose calculations in the Level 3 PSA.

508. The Level 3 PSA included inputs from the internal events Level 1 PSA (Ref. 36), SFP PSA (Ref. 37) and the Level 2 PSA (Ref. 42). In addition, it included inputs from outside PSA such as the waste route and the fault schedule. The RP examined the fault schedule and the waste route safety case and identified several accident scenarios that were screened out of the Level 1 PSA, Level 2 PSA or SFP PSA. These additional inputs were included in the Level 3 PSA analysis.

4.25.2 Justification of the Level 3 PSA Codes and Approaches

509. The RP's chosen Level 3 PSA software code is somewhat dated, and has limitations. I discussed these limitations in detail with the RP in a number of meetings. Subsequently, I raised RQ-UKHPR1000-0424 (Ref. 66) to address the lack of justification for these gaps and limitations of the software and to gain confidence in the RP's choice of software for the Level 3 PSA. The RP submitted Ref. 91 to further address the limitations of the software package.

510. Ref. 91 notes the following limitations of PC-COSYMA and approaches:

- Doses and individual risk can only be calculated for adults.
- Gaussian atmospheric dispersion model is dated and less sophisticated than modern approaches.
- Population data is from the 2001 UK census.
- Agricultural data is from the 2003 EDINA database.
- The maximum meteorological sample size is only 144.
- The number of radionuclide release phases is limited to six one-hour phases.
- Separate calculation of early and late societal health effects.
- Single particle size.
- Single set of location factors.
- Erroneously high numbers of late health effects in individual grids.
- Old MS-DOS-based user interface.

511. The RP presented justification for each one of the identified limitations, as well as a comparison of the code with ONR guidance outlined in the PSA TAG (Ref. 4). I

sampled a few of these justifications, and my assessment of these is summarised in the following paragraphs.

512. The most potentially risk-important limitation of PC-COSYMA is the fact that results can only be calculated for adults. ONR SAPs (Ref. 2), paragraph 751 states that 'the analysis should identify the hypothetical person at most risk overall'. It is likely that this person would not be an adult, but an infant. Thus, this limitation in the code is important because the total internal dose to an individual will depend on the combination of the dose coefficient (which increase with decreasing age for inhalation and ingestion) and habit data such as breathing rates and food consumptions rates which usually decrease with decreasing age. As the total dose is the sum of internal and external dose (cloudshine and groundshine), the amount of time spent outdoors is another differentiator between candidate groups for the representative person selection (i.e. the person representing the group for whom the dose or individual risk assessment is performed).

513. To address this limitation of the code, the RP proposed to follow the recommendations outlined from the International Commission on Radiological Protection (ICRP) in Ref. 92. Ref. 92 recommends against using overly conservative assumptions in Level 3 PSA. The RP described how using an infant as the recommended person would mean using several combinations of conservative assumptions (e.g. children spend more time outside, it is assumed children only eat local food, the child would be constantly assumed to be present at the side boundary, etc). Thus, to make a balanced analysis that avoids overly conservative approaches, the RP proposed to use child/infant dose assessments only for Target 8. Thus, for Target 8, the RP used dose scaling factors from the ICRP which were applied to the calculated adult inhalation and ingestion doses, and a sensitivity study estimated the difference between the base case adult dose and an infant. For assessments against Target 7, the RP did not use child/infant doses. For Target 9 the risk factors are already population averaged and since it is the risk to the population as a whole that is being assessed, the adult specific results are proposed to be used.

514. Following a discussion with ONR Radiological Consequences specialist inspectors, I was able to conclude the RP's proposal is proportionate and reasonable. I consider it to not be proportionate to encourage the RP to perform the overly conservative methodology across all three Targets. The Level 3 PSA is already somewhat conservative and thus, I am content that the solution proposed by the RP is adequate for GDA.

515. A second justification for limitations in the PC-COSYMA code that I sampled was the use of population data from the 2001 UK census. This limitation is due to the age of the software, and that the most recent UK census data that was available at its development was from the 2001 census. The 2011 census data is now available but the code did not automatically include this new information.

516. The RP proposed two options in Ref. 91 for addressing this limitation. The first option would entail recreating a new population datafile using the updated census data. This was found by the RP to not be a trivial task and would require significant time to enter all the new data manually into a format suitable for PC-COSYMA. The second option was simpler where the RP proposed to apply a uniform growth factor to reflect the growth in UK population between 2001 and 2018. This could be used in sensitivity studies to investigate the effect of population growth scenarios over the lifetime of the NPP. The RP decided to use the second, simpler approach for GDA because it was less labour intensive and could be used almost up until the present (2018).

517. I assessed this line of reasoning and found that the RP's proposal did not take account of the UK updated ratio of urban to rural area population. Therefore, the urban population is likely underestimated, whereas the rural area population is over

estimated. The RP provided a sensitivity study in Section 3.3.2 of Ref. 44 which concluded that the mean number of early and late fatalities increases with the population growth but the conditional probability of over 100 fatalities remains stable.

518. I also discussed this proposal with ONR Radiological Consequences specialist inspectors and was able to conclude that the RP's proposal is proportionate and reasonable. I found that it would not be proportionate to encourage the RP to manually update the ratio of urban to rural population in the Level 3 PSA database and found the RP's sensitivity studies including data up until 2018 increased my confidence. Thus, for GDA I find this proposal to be adequate, however, I expect that the Level 3 PSA should be updated with accurate population data post-GDA as a part of normal business.

4.25.2.1 Level 3 PSA Methodology

519. The TSC and I reviewed the Level 3 methodology (Ref. 25) and found that, it generally compared favourably to RGP approaches such as IAEA SSS No. GSG-10, IAEA TECDOC-1914 (Ref. 8), NEA/CSNI/R(2018)1 (Ref. 90) and ASME/ANS-RA-S-1.3-2017 (Ref. 18). However, I identified a shortfall in the RP's Level 3 methodology which relates to the treatment of thirteen RCs which do not have a specific source term calculated for them. Instead, the RP assumed conservatively that for this group of RCs the top facility dose band for Target 8 (>1 Sv) is the consequence. I present my assessment of this shortfall in the following paragraphs.

520. During routine interactions, the RP stated that it had taken this approach due to the amount of extra work that would be required if customised and RC specific source terms for the group of thirteen had been derived. For GDA, the RP decided that it would be more proportionate to conservatively assign a dose consequence, rather than specifically calculate them.

521. In my opinion, although I agree with the RP's general principle that this conservative approach will not result in optimistic results of the Level 3 PSA, I also find that this approach has resulted in a distortion to the Level 3 PSA results. Comparing the results of Level 3 PSA against SAP Targets is one important use for a Level 3 PSA, however, understanding of risk-important systems and accident sequences is a secondary important purpose. In my opinion, the RP's decision to conservatively treat this group of thirteen RCs has led to a Level 3 PSA wherein there is a potential masking of the normal risk-important information that would usually arise from the results. By using this approach, the risk profile of the design has been distorted and it is less useful than it would have been had bespoke source terms been used for the group of thirteen RCs.

522. Thus, in my opinion, I find that the Level 3 PSA is adequate for GDA, but I would expect it to be updated with bespoke source terms for all RCs as a part of normal business post-GDA.

523. Overall, I found that the Level 3 PSA approaches and methodology largely met regulatory expectations as compared with RGP. For GDA I am content that this methodology should enable the RP to perform Level 3 PSA analysis and meet its objectives.

4.25.2.2 Level 3 PSA Results

524. The following table shows the Level 3 PSA for the SAPs Targets 7 through 9.

Table 10: Level 3 PSA Results for Target 7

Release Category ID	Release Category Type	Frequency (/ry)	Mean Individual Risk at Distance		
			0.4 km	1.0 km	1.5 km
RC_IE_W01	Waste Route PIEs	8.59x10^{-05}	1.44x10^{-12}	5.26x10^{-13}	3.38x10^{-13}
RC_IE_W02		9.12x10^{-04}	5.83x10^{-11}	2.22x10^{-11}	1.52x10^{-11}
RC_IE_01	DBC PIEs	2.03x10^{-04}	7.37x10^{-12}	2.69x10^{-12}	1.73x10^{-12}
RC_L1_P01		1.86x10^{-01}	1.14x10^{-07}	3.77x10^{-08}	2.29x10^{-8}
RC_SFL1_02	Level 1 PSA Success Sequences (SFP)	8.18x10^{-03}	2.50x10^{-09}	7.67x10^{-10}	4.61x10^{-10}
SFP_RC01		5.99x10^{-05}	2.62x10^{-12}	1.07x10^{-12}	7.23x10^{-13}
SFP_RC03		1.27x10^{-07}	1.11x10^{-09}	3.67x10^{-10}	2.25x10^{-10}
SFP_RC02		1.24x10^{-09}	9.97x10^{-17}	4.03x10^{-17}	2.79x10^{-17}
SFP_RC03		1.70x10^{-12}	3.19x10^{-14}	1.11x10^{-14}	6.94x10^{-15}
RC_L1_S03	Level 1 PSA Success Sequences (Reactor Core)	2.87x10^{-08}	3.27x10^{-13}	1.44x10^{-13}	9.80x10^{-14}
RC_L1_S02		6.07x10^{-06}	1.15x10^{-12}	4.34x10^{-13}	2.73x10^{-13}
RC_L1_L01		2.27x10^{-5}	5.18x10^{-10}	2.35x10^{-10}	1.59x10^{-10}
RC_L1_L02		3.89x10^{-09}	2.40x10^{-11}	8.17x10^{-12}	5.06x10^{-12}
RC_L1_S01		1.49x10^{-03}	1.96x10^{-10}	6.53x10^{-11}	4.21x10^{-11}
RC_L1_M01		6.54x10^{-05}	1.19x10^{-11}	3.80x10^{-12}	2.29x10^{-12}
RC_L1_P01		8.93x10^{-07}	5.48x10^{-13}	1.81x10^{-13}	1.10x10^{-13}
RC101	Level 2 PSA (with Source Terms)	2.67x10^{-07}	5.18x10^{-11}	2.04x10^{-11}	1.31x10^{-11}
RC102		4.90x10^{-08}	2.90x10^{-11}	1.00x10^{-11}	6.34x10^{-12}
RC201		3.25x10^{-09}	3.48x10^{-10}	1.84x10^{-10}	1.28x10^{-10}
RC501		1.29x10^{-08}	5.83x10^{-11}	2.03x10^{-11}	1.22x10^{-11}
RC502		8.74x10^{-10}	8.40x10^{-11}	5.25x10^{-11}	3.88x10^{-11}
RC601		3.05x10^{-09}	3.42x10^{-10}	1.90x10^{-10}	1.33x10^{-10}
RC503	Level 2 PSA (without Source Terms)	2.04x10^{-08}	2.04x10^{-08}	2.04x10^{-08}	2.04x10^{-08}
RC202		1.24x10^{-10}	1.24x10^{-10}	1.24x10^{-10}	1.24x10^{-10}
RC203		2.71x10^{-11}	2.71x10^{-11}	2.71x10^{-11}	2.71x10^{-11}
RC204		1.21x10^{-09}	1.21x10^{-09}	1.21x10^{-09}	1.21x10^{-09}
RC205		1.83x10^{-08}	1.83x10^{-08}	1.83x10^{-08}	1.83x10^{-08}
RC302		5.88x10^{-10}	5.88x10^{-10}	5.88x10^{-10}	5.88x10^{-10}
RC401		2.56x10^{-13}	2.56x10^{-13}	2.56x10^{-13}	2.56x10^{-13}
RC402		1.64x10^{-10}	1.64x10^{-10}	1.64x10^{-10}	1.64x10^{-10}
RC504		1.87x10^{-08}	1.87x10^{-08}	1.87x10^{-08}	1.87x10^{-08}
RC602		2.08x10^{-09}	2.08x10^{-09}	2.08x10^{-09}	2.08x10^{-09}

Release Category ID	Release Category Type	Frequency (/ry)	Mean Individual Risk at Distance		
			0.4 km	1.0 km	1.5 km
RC701		$5.68\text{x}10^{-09}$	$5.68\text{x}10^{-09}$	$5.68\text{x}10^{-09}$	$5.68\text{x}10^{-09}$
SFP_RC05		$6.65\text{x}10^{-09}$	$6.65\text{x}10^{-09}$	$6.65\text{x}10^{-09}$	$6.65\text{x}10^{-09}$
Summated Individual Risk (/ry)			$1.93\text{x}10^{-07}$	$1.14\text{x}10^{-07}$	$9.80\text{x}10^{-08}$

525. The Level 3 PSA results show the summated risk of the UK HPR1000 design is below the Target 7 BSO. The release category type ‘Level 2 PSA (without source terms)’ dominates the risk, which is to be expected based on my assessment in paragraph 522 of this report.

526. In addition, for Target 7, the RP performed a sensitivity case to look at the difference if scaling factors were used to estimate the dose to a child or infant and found the total individual risk (/ry) to be very similar for adults, children, and infants. The RP explained this is likely a result of using the conservative source terms for the group of RCs as previously discussed.

527. As the RP has demonstrated, the Level 3 PSA results are less than the SAPs Target 7 BSO, and thus I am content that the RP has demonstrated that the individual risk to people off the site from accidents is low.

Table 11: Level 3 PSA Results for Target 8

Facility Dose Band	Dose Range (mSv)	Dose Band Total Frequency (/ry)	BSO (mSv)	BSL (mSv)	Percentage of BSO
1	0.1-1	$2.27\text{x}10^{-05}$	$1.00\text{x}10^{-02}$	1.00	0.23%
2	1-10	0	$1.00\text{x}10^{-03}$	$1.0\text{x}10^{-01}$	0
3	10-100	$2.67\text{x}10^{-07}$	$1.00\text{x}10^{-04}$	$1.0\text{x}10^{-02}$	0.27%
4	100-1000	$1.93\text{x}10^{-07}$	$1.00\text{x}10^{-05}$	$1.0\text{x}10^{-03}$	1.93%
5	>1000	$8.11\text{x}10^{-08}$	$1.00\text{x}10^{-06}$	$1.0\text{x}10^{-04}$	8.11%

528. For Target 8, the RP’s results showed that the frequency dose target BSOs for accidents on an individual facility to any person off the site have been met. In addition, the RP noted that no single RC category or type dominated the results. The RC group ‘Level 2 PSA (without source terms) again dominates the results, but a balanced risk profile is maintained regardless.

Table 12: Level 3 PSA Results for Target 9

Release Category Type	Release Category ID	Conditional Probability of 100 or more Total Fatalities	Frequency of 100 or more Fatalities	Conditional Probability of 100 or more Late Fatalities	Frequency of 100 or more Late Fatalities
Level 1 PSA Success Sequences (SFP)	SFP_RC03	1.00	1.27x10^{-07}	0.66	8.38x10^{-08}
	SFP_RC04	1.00	1.70x10^{-12}	0.76	1.30x10^{-12}
Level 1 PSA Success Sequences (Reactor Core)	RC_L1_L02	1.00	3.89x10^{-09}	0.82	3.19x10^{-09}
Level 2 PSA (with Source Terms)	RC101	0	0	0	0
	RC102	0.19	9.18x10^{-09}	0.19	9.18x10^{-09}
	RC201	1.00	3.25x10^{-09}	0.90	2.91x10^{-09}
	RC501	1.00	1.29x10^{-08}	0.65	8.41x10^{-09}
	RC502	1.00	8.74x10^{-10}	0.91	7.95x10^{-10}
	RC601	1.00	3.05x10^{-09}	0.90	2.75x10^{-09}
Level 2 PSA (without Source Terms)	RC503	1.00	2.04x10^{-08}	1.00	2.04x10^{-08}
	RC202	1.00	1.24x10^{-10}	1.99	1.24x10^{-10}
	RC203	1.00	2.71x10^{-11}	1.00	2.71x10^{-11}
	RC204	1.00	1.21x10^{-09}	1.00	1.21x10^{-09}
	RC205	1.00	1.83x10^{-08}	1.00	1.83x10^{-08}
	RC302	1.00	5.88x10^{-10}	1.00	5.88x10^{-10}
	RC401	1.00	2.56x10^{-13}	1.00	2.56x10^{-13}
	RC402	1.00	1.64x10^{-10}	1.00	1.64x10^{-10}
	RC504	1.00	1.87x10^{-08}	1.00	1.87x10^{-08}
	RC602	1.00	2.08x10^{-09}	1.00	2.08x10^{-09}
	RC701	1.00	5.68x10^{-09}	1.00	5.68x10^{-09}
	SFP_RC05	1.00	6.65x10^{-09}	1.00	6.65x10^{-09}
Summed Frequency (/ry)			2.34x10^{-07}	—	1.85x10^{-07}

529. The RP demonstrated that the overall frequency of 100 fatalities is lower than the Target 9 BSL but above the BSO for all parts of the PSA, including hazards, but not including seismic. This result is based on the PSAs for DR2.1 and DR1 as described earlier in this report. In this demonstration, the RP noted that RC SFP_RC03 (32 fuel assemblies damaged and DWL runs successfully) dominated the total risk. The Level 3 PSA results for this RC alone are noted to be 1.27x10^{-7}, compared with the total risk of 2.34x10^{-7} for all accidents. The RP argued that this RC was modelled very

conservatively, and thus its real level of risk is likely to be much lower than calculated in the PSA.

530. RC SFP_RC03 is modelled with three large areas of conservatism. The first conservatism is that the accident sequence in the SFP PSA (Ref. 37) models a dropped load of a transfer cask over the hoisting pit and assumes as a bounding case that all 32 assemblies in the cask are damaged and that all of the radioactive material will be released into the fuel building. The RP claims that this assumption was used due to the SFP PSA being modelled on DR2.1 and thus did not include impact limiters. In DR2.2, after a modification (Ref. 86) has been implemented to the design, this accident sequence is removed from the PSA as the consequences will be negligible if a dropped load occurred.

531. The RP claimed that the second conservatism is that the assumption that all radioactive material will be released into the fuel building was a conservative assumption as most of the fuel route for this accident is over water and any dropped load would result in water contamination, but little release into the fuel building atmosphere.

532. The RP claimed that the third conservatism is that the maximum bounding source term was used for this RC, instead of a bespoke source term. The RP claimed that if the bespoke source term and this conservatism removed, the RC would not be significant for assessments against Target 9.

533. I have assessed these claims and arguments and judge them to be reasonable. Although the combined Level 3 PSA showed results slightly higher than the BSO for Target 9, in my opinion, if some conservatisms were removed, the level of risk would be less than the BSO. In addition, if risks from seismic hazards were included, I would not expect the risk to rise significantly as the RP demonstrated adequately that the risks are expected to be low from seismic hazards (see sub-section 4.18 of this report).

534. Aside from Target 9, and considering a more holistic view, I found that the Level 3 PSA results show that the risk from the UK HPR1000 is low. The subsequent modifications made during GDA reduce the risk further. From the PSA perspective, and for matters within the scope of PSA, the final design of the UK HPR1000 achieves a level of risk consistent with RGP for a modern plant and unless they are easily achievable, my expectation is that further modifications are likely to be grossly disproportionate.

4.25.2.3 Level 3 PSA ONR Comparison Analysis

535. The TSC performed a comparison analysis (Ref. 93) to study the effect of an alternative calculation method on the Level 3 PSA results. The purpose of this study was to provide confidence to ONR that the RP's Level 3 PSA results were reasonable. For this purpose, the TSC used PACE which is a more recently developed software tool compared to PC-COSYMA. While PACE is capable of utilising a more advanced dispersion model, it was decided that the built-in Gaussian plume model (ADEPT) should be used for a better comparability.

536. There were three main considerations guiding the RC selection for the verification calculations – availability of source term data, significant frequency contribution and significant radiological effects. In addition, the SFP RCs were not considered due to the SFP design modification (Ref. 86) that is expected to eliminate the SFP as a significant release contributor. Thus, RC501 and RC601 were selected as both being a significant frequency contributor (1.29×10^{-8} and 3.09×10^{-9} respectively) while having high radiological consequences. RC501 models containment failures due to overpressure with the EUF failed open. RC601 models containment bypass following SGTR.

537. The results of the comparison analysis provided confidence that the RP's Level 3 PSA was adequate for GDA and that SAP Targets 7 and 8 BSOs are met and SAP Target 9 BSL is met.

4.25.3 Strengths

538. All of the known limitations of PC-COSYMA were addressed. The RP provided sensitivity cases for some of the significant limitations, and these demonstrated that the limitations do not significantly affect the Level 3 PSA results.

4.25.4 Outcomes

539. I identified a gap where bespoke source term analysis should be performed for the thirteen RCs which were assigned conservative bounding source terms. I would expect a licensee to update the Level 3 PSA with this information in the site-specific stage.

4.25.5 Conclusion

540. In my assessment I find that the RP has used approaches and methods that compare favourably with RGP. Where there were differences, the RP demonstrated how they would address the differences adequately. The overall results demonstrate that the overall level of risk is less than the BSO for SAP Targets 7 and 8 and close to the BSO for SAP Target 9.

541. In addition, my TSC's comparative analysis provided confidence that the RP's Level 3 PSA was adequate for GDA and that SAP Targets 7-9 are met.

4.26 Worker Dose Analysis Report (Targets 5 & 6)

4.26.1 Introduction to Worker Dose Analysis Report (Targets 5 & 6)

542. The RP submitted a report (Ref. 46) to calculate the individual risk of death to any person on the site due to exposure to ionising radiation from on-site accidents (Target 5), and the frequency of any single accident in the facility which could give doses to a worker on site (Target 6).

543. Whilst the Level 1, Level 2 and Level 3 PSA models do not directly estimate these risks, the RP has used insights and outputs from the various PSA models to compare with SAP Targets 5 & 6. Targets 5 & 6 are concerned with on-site dose to workers, rather than Targets 7-9 which are concerned with off-site dose to the public. Analysis of Targets 5 & 6 is discussed in the PCSR Chapter 14 (Ref. 3), along with the PSA. It was decided for GDA that this report would be in the scope of the assessment for PSA as outlined in my assessment plan (Ref. 5)

544. The RP used the results of the PSA, combined with the hazard analysis, DBA and SAA to address the risks to workers. The RP's approach was explained in Ref. 54.

4.26.2 Worker Dose Analysis Methodology

545. The RP's approach to demonstrate that risks to workers on-site from accidents has been reduced to ALARP used information from a wide variety in the safety case. The RP selected potential accident sequences from the PSA, waste and SFP PIE lists, and additional sequences from other sources wherein it could be possible that a worker could receive a dose. This initial list was then grouped and screened to combine accidents with similar consequences into a group. The RP then analysed the accident sequences to find where certain categories of workers could potentially receive a dose after the accidents. Frequencies were assigned to the accident scenarios, and potential doses were calculated for the scenarios for each category of worker. Finally,

occupancy factors for workers were calculated to arrive at the final results to compare against Targets 5 & 6.

546. The initial list of potential accident sequences reviewed the following areas of the safety case:

- all Level 1 PSA sequences (including hazard PSA) without core damage but with radioactive release;
- all Level 2 PSA sequences (including hazard PSA) with core damage grouped into RCs;
- all SFP PSA accident sequences with and without spent fuel damage;
- all waste route PIEs; and
- any other accident sequences not identified in the PSA such as sequences included in assessment against Target 4.

547. To identify accident sequences from the above list whereby a potential dose to workers could arise, the RP used the following principles for selection and grouping:

- Accident sequences requiring workers to perform on-site mitigation operations.
- Accident sequences with radiological material released to atmosphere inside the nuclear island buildings, radioactive waste treatment building (BWX) or BMX.
- Accident sequences with radiological material released to systems that normally contain low or negligible radioactivity.
- Accident sequences with loss or degradation of shielding effectiveness.
- For accident sequences wherein the likely worker dose is in excess of 2000 mSv, the detailed calculation of the dose was not performed.
- Grouping was performed on the basis of causal or functional similarity, as well as quantity of radioactive release and resulting working dose. Grouping is further performed based on similar location.

548. The RP's method to calculate doses was explained in Ref. 54 and used typical methods and software that is well known to the industry. The RP then used these estimated doses and calculated the estimated risk by combining the dose consequence with the frequency of the accident scenario, the occupancy factor and a dose conversion factor for the radionuclide inhaled or type of radiation exposure.

549. I assessed the methodology and found it to be reasonable and logical. The RP used previous GDA reports that were in the public domain, and thus this approach is similar to other GDA approaches to address SAP Targets 5 & 6. In my opinion, the methodology is fit for purpose and adequate for GDA.

4.26.3 Worker Dose Assessment Results

550. The following tables are the RP's worker dose assessment results against SAP Targets 5 and 6.

Table 13: Summary of Results for SAP Target 5 - Generic Worker

Accident Group	Risk (/ry)	% of Total
Level 1 PSA PIEs (including RCCA and reactor coolant pump seizure)	2.10×10^{-7}	46.36
Fuel Route PIEs	1.39×10^{-7}	30.68
Spent Fuel Pool Level Drop Accidents	7.37×10^{-8}	16.27
Auxiliary System PIEs	4.39×10^{-9}	0.97

Accident Group	Risk (/ry)	% of Total
Waste Route PIEs	2.30×10^{-8}	5.08
Level 1 PSA (internal hazard fire and flooding events)	1.92×10^{-9}	0.42
Level 1 PSA (external hazard events)	6.04×10^{-10}	0.10
Level 2 PSA	8.38×10^{-10}	0.18
Total:	4.53×10^{-7}	100

Table 14: Summary of Results for SAP Target 5 - MCR Worker

Accident Group	Risk (/ry)	% of Total
Level 1 PSA PIEs (including RCCA and reactor coolant pump seizure)	1.23×10^{-8}	65.3
Fast Core Damage accidents LB-LOCA	3.77×10^{-9}	19.9
Auxiliary System PIEs	1.81×10^{-9}	9.6
Level 2 PSA	8.77×10^{-10}	4.6
Fuel Route PIEs	7.20×10^{-11}	0.4
Level 1 PSA (internal hazard fire and flooding events)	1.35×10^{-11}	0.1
Total:	1.89×10^{-8}	100

551. The SAP Target 5 results show that the risk to MCR workers is less than for generic workers, and in addition, the total risk is less than the SAP Target 5 BSO. I find that these results demonstrate that risks to on-site workers are low enough such that it would be disproportionate to expect the RP to perform further analysis or modifications to the design to lower these risks further. Thus, the RP's claim that these risks have been reduced to ALARP is adequate for GDA.

Table 15: Summary of Results for SAP Target 6 - Results Below BSO

Accident	Frequency (/ry)	% of Target 6 BSO
TEG pipeline failure in BNX	8.42×10^{-5}	84.20
SFP level drops to +8.78 m – internal fire hazards	6.76×10^{-4}	67.60
MSLB	6.29×10^{-4}	62.90
ATWS	5.20×10^{-5}	52.01
TEG delay beds failure in BNX	2.98×10^{-4}	29.80
SFP level drops to +8.78 m – internal events	2.92×10^{-4}	29.20
Feedwater line break	2.65×10^{-5}	26.52
RCV volume control tank failure	1.95×10^{-4}	19.50
RPE tank or pipeline failure in BNX	1.69×10^{-4}	16.93

Accident	Frequency (/ry)	% of Target 6 BSO
IB-LOCA	1.35×10^{-5}	13.51
LB-LOCA	2.39×10^{-6}	2.39
Level 2 PSA sequences	1.47×10^{-7}	1.47
SFP level drops to +8.78 m – internal flooding hazards	7.92×10^{-7}	0.08
SFP level drops to +8.78 m – external hazards	3.72×10^{-7}	0.04

Table 16: Summary of Results for SAP Target 6 - Results Above BSO

Accident	Dose (mSv)	Frequency (/ry)	% of Target 6 BSL
Spectrum of RCCA ejection accidents	2.75×10^{2}	1.00×10^{-4}	10
Spent fuel assembly drop	2.19×10^{2}	5.59×10^{-5}	6
RHR system break outside containment	1.04×10^{2}	1.00×10^{-4}	1

552. The RP's results for SAP Target 6 show that for the majority of accident scenarios, the results are below the SAP Target 6 BSO. For three accident scenarios, the risk is above the BSO (but below the BSL) and the RP provided further ALARP justification for these three scenarios. I sampled the justification for dropped loads and the RCCA ejection accidents. My assessment for these scenarios is in the following paragraphs.

553. For the dropped fuel assembly accident, the RP argued that this accident is a result of the DR2.1 fuel handling equipment in the SFP PSA and due to design changes since that time the accident sequence no longer will be credible. As the RP has implemented a modification (Ref. 86) included in DR3 which should result in this accident sequence becoming highly unlikely, in my opinion the RP's arguments are sound and adequate for GDA.

554. For the RCCA ejection accident, the RP argues that the actual dose consequences for this scenario are conservative in the analysis and could be lowered via simple administrative rules such as restricting access to the containment airlock after the initiating event. The analysis assumed the worker would linger in the high radiation zone for a significantly long period of time, but it is unlikely that this would occur due to standard rules regarding signage and workers not lingering in these areas in nuclear plants. I found that this line of reasoning to be reasonable and thus adequate for GDA.

555. In my opinion, I found that the approaches used by the RP met my expectations compared with RGP. I also found that the results clearly showed that the risks have been reduced to ALARP. Where ALARP justifications were made for risks that were above the BSO, but below the BSL I found that the RP's arguments were reasonable and adequate for GDA.

Table 17: Summary of Results for Doses to Fuel Building Workers from Accidents

Accident	Dose (mSv)	Frequency (/ry)
SB-LOCA	1.46	4.58×10^{-3}
LB-LOCA	1.01×10^{1}	2.39×10^{-6}
MSLB	4.71	6.29×10^{-4}
SFP water level drop to +8.78m	6.67	9.69×10^{-4}
Spent fuel assembly dropped into SFP	2.01×10^{2}	5.59×10^{-5}
Spent fuel assembly dropped into transfer pit	2.19×10^{2}	5.59×10^{-5}
Spent fuel assembly dropped into reactor cavity pool	1.26×10^{2}	5.59×10^{-5}
Spent fuel assembly dropped into core internal pool	1.27×10^{2}	5.59×10^{-5}
Failure of volume control tank (VCT) in fuel building	5.34	4.18×10^{-4}
RCCA Ejection Accident	3.19×10^{1}	1.00×10^{-4}

556. Table 17 presents a summary of the RP's estimated doses for fuel building workers from accidents. These are included in the generic worker categorisation in the previous tables. It can be observed that for all of the accidents listed, the workers doses are all in line with the Target 6 expectations, as many of the accidents potentially affecting workers in the fuel building are either <2 mSv or less than the applicable BSO. The four events which are above the BSO are for the four dropped spent fuel assembly accidents. It is noted that these events are 6% of the BSL for Target 8 in the appropriate dose category.

557. The RP notes in Ref. 46 that these accidents are all due to the overhead crane design. In Modification-94 (Ref. 86) this polar crane design has been proposed to be eliminated from the design and replaced with a gantry crane. I did not assess this modification in detail, but the RP claims that new crane design will eliminate many of the PIEs associated with the polar crane dropped loads. I found the RP's arguments reasonable, and it is logical that many of the dropped load PIEs would not be physically possible with the new type of crane. In addition, although these PIEs have higher dose-frequency results than the BSO in Target 6, they are still significantly below the BSL.

558. Thus, as a subset of the generic worker faults, I found that the fuel building worker dose assessment against Targets 5 & 6 was clear and provided a systematic and thorough analysis of the results for fuel building workers.

4.26.4 Strengths

559. The RP performed a systematic and thorough analysis to understand the level of risk arising from the design for on-site workers.

560. The RP's approach ensured that a wide selection of risks was included, not just from the PSA.

4.26.5 Outcomes

561. My assessment of the RP's submissions on worker dose assessment calculations against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.26.6 Conclusion

562. The RP's demonstration that the level of risk arising from the design to on-site workers was ALARP is adequate for GDA. I found the approach to be reasonable, broad, and thorough. A licensee will need to review this analysis during detailed design and when the operation of the facility is better understood.

4.27 Overall Conclusions from the PSA

563. This sub-section presents my detailed conclusions of the GDA review of the UK HPR1000 PSA when compared against relevant expectations in Table A1-5 of ONR's PSA TAG (Ref. 4). Section 5 of this report presents a summary of these conclusions. My judgement is based on the significance of the outcomes of my review and the potential impact on the risk profile of the RP's sensitivity analyses, and qualitative or quantitative information from the PSA. I have considered the following:

- the adequacy of the PSA documentation;
- whether it is believed that all aspects of the PSA have been subject to sufficient level of independent review by the RP;
- whether the PSA has a credible and defensible basis;
- whether the PSA reflects the design of the UK HPR1000 submitted for GDA;
- the adequacy of the process in place to ensure that the PSA assumptions regarding design and operation of the UK HPR1000 are captured in the development of future procedures, policies and strategies, design, design modifications, etc;
- whether the PSA has enabled a judgement to be made as to the acceptability of the overall risk of the facility against ONR's SAP Targets; and
- whether the PSA has been effectively used to demonstrate that a balanced design has been achieved and that the risk associated with the design and operation of the UK HPR1000 is ALARP.

564. The UK HPR1000 PSA and the responses to the supporting ROs and RQs broadly meet the expectations of ONR's PSA TAG (Ref. 4).

565. The UK HPR1000 PSA has a credible and defensible basis. There is clarity regarding the differences between the UK HPR1000 design reflected in the PSA and the design of the UK HPR1000 submitted for GDA.

566. The UK HPR1000 PSA is built on a number of assumptions based on the design documentation available at the time when the PSA was developed. The majority of these assumptions have been adequately substantiated during GDA. For the remainder, it is important that adequate substantiation is provided when detailed information becomes available. The PSA will need to be revised to reflect the detailed design, site-specific characteristics, and operational matters (such as procedures, EMIT schedule, refuelling outage strategy, etc). This is considered part of normal business for the site-specific stage.

567. The UK HPR1000 PSA submitted in GDA enables a comparison to be made against ONR's SAP Targets. The results of the PSA show that the risk is low and that a balanced design has been achieved. The RP has used these results to argue that the risks have been reduced to ALARP, and I am content with the RP's use of the PSA to make this claim.

568. The PSA chapter of the PCSR presents an adequate summary of the detailed PSA submissions assessed during GDA and provides a route map to the detailed PSA documentation.

569. In sub-section 2.4 I listed the standards and criteria I have used during my assessment to judge whether the UK HPR1000 PSA submission appropriately addressed regulatory expectations and has been carried out adequately with respect to modern standards.

570. I am able to conclude that the UK HPR1000 PSA has been carried out adequately with respect to these standards to enable a meaningful GDA to be completed.

4.28 Demonstration that Relevant Risks Have Been Reduced to ALARP

571. The RP submitted Ref. 94 to demonstrate that the PSA has been used to risk inform the design, and that it would be disproportionate to further reduce the risk. I assessed this report and found significant gaps in the ALARP demonstration for PSA in that the RP had not undertaken a systematic review of the PSA and had not demonstrated use of the PSA to inform potential modifications identified from elsewhere in the safety case. Thus, I raised RO-UKHPR1000-0043 (Ref. 57) to ensure that the RP addressed these gaps during GDA.

572. In response to this RO, the RP updated Ref. 94 substantially and submitted Ref. 56 to supersede it.

573. The revised approach included the following steps:

- The RP’s process started by comparing their PSA procedures against RGP and OPEX.
- The next step was to review the quantification results of the PSA models in order to derive risk insights.
- The risk insights that were identified were systematically reviewed to understand potential plant design weaknesses, and design improvement options, or PSA modelling improvement options.
- The RP identified how the risk could be reduced by each potential improvement, either in the design or the PSA model. The results of this step were stated to be reviewed from other topic area staff to ensure that a holistic review is performed.
- For all changes that proceed through the screening exercise, the RP then documented how the changes would be implemented, and then judged whether or not they are reasonably practicable.
- The final step was to review the final results of the exercise and to judge whether or not further risk reduction options exist, and then put those through the process again if needed.

574. After performing the above approach, the RP submitted its analysis of the PSA results in Ref. 56. The RP stated that it would be disproportionate to further reduce the risk and provided justification for this statement through analysis of the Level 1 PSA, hazards PSA, Level 2 PSA, SFP PSA and the FCG3 seismic PSA. For this justification, the RP analysed nearly 100 different case studies total including some from each of the different PSAs.

575. The RP documented many different studies of ways that the level of risk can be reduced, including further analysis of:

- PSA results which indicate that the design should be modified to be more reliable; and
- PSA design assumptions which are potentially conservative.

576. I find that in Ref. 56, the RP has developed and documented a detailed and systematic process for using PSA to identify design improvements that reduce the risk of UK HPR1000 design to ALARP. The process uses the PSA results themselves to identify potential design improvements and uses the PSA to inform potential improvements identified from other disciplines. This is consistent with my expectations and RGP.

577. In my opinion, the RP's approach for demonstrating that the risks have been reduced to ALARP for PSA is adequate and systematic and able to identify areas of risk reduction both in the design as identified by the PSA, and in the PSA model itself. The first step of the process references Refs 8 and 17 and the RP stated that these were used to develop the approach. These comparison references are what I expected the RP to use as they are well understood to be RGP for PSA methods, including optimisation and reducing the risk to ALARP

578. I sampled some of the RP's analysis of the ALARP demonstration. In the following paragraphs I have presented a summary of my sampling assessment.

579. My first sample was an example of where PSA results indicate that design modification should be performed to increase the reliability of the plant. In this sample, the Level 1 PSA results clearly showed that the loss of the DVL [EDSBVS] HVAC system was a very high contributor to the overall level of risk. The results showed that if the DVL [EDSBVS] HVAC system diversity was modified such that each train's normal supply fans were diverse, the internal events Level 1 CDF will drop by approximately 25%. This is related to Modification-35 (Ref. 78) of which the RP analysed the probabilistic impact in Ref. 6. I found that the RP followed their methodology to understand and demonstrate the level of risk arising from this part of the design; they recognised that design change would lower the level of risk; and this contributed towards justification for modification M-35, which was accepted as a design change for GDA.

580. I sampled an analysis of a PSA design assumption with an identified conservatism, in the DVL [EDSBVS] system modelling. The PSA model assumed that a failure in the closed position of any HVAC damper would directly and immediately result in loss of cooling for the entire related division of DVL [EDSBVS], cascading to all loads of that division. The RP identified this modelling as a potentially conservative design assumption as it is unlikely that a loss of fresh air intake would immediately result in failure of DVL [EDSBVS] cooling. The RP analysed the change in the PSA model if this conservatism was removed. The results were that the CDF decreased by approximately 10%. I found that the RP followed their methodology to identify and assess this design assumption. The RP stated that they would carry this model change into the next version of the PSA.

581. I sampled the analysis for a PSA assumption whereby the IVR system is assumed to be 100% effective. The RP performed sensitivity calculations by modifying this assumption so that the IVR was effective in 90% and 99% of all scenarios. It was determined that the Level 2 PSA results (LRF) was affected by this assumption, but only by a small amount (~6% increase for the 90% effectiveness). In the optioneering evaluation for this assumption, it was decided to perform more analysis after GDA to ensure that the assumption of 100% effectiveness of the IVR could be maintained in the model. I found that the RP followed their methodology to identify and analyse this assumption. It was clear how important this assumption was and what the RP was planning on doing as a result of this analysis.

582. For the analysis sample that I chose, the RP has provided adequate analysis, substantiation, and documentation to demonstrate that the PSA has been used to understand if the level of risk from the design is ALARP. The scope and breadth of the analysis was substantial and adequate for GDA. I found that the demonstration was suitable and sufficient for use in the UK HPR1000 safety case and met my expectation for GDA.

583. As noted above, the RP will need to implement all of the identified changes into future versions of the PSA model. This is part of normal business for a licensee to be undertaken after GDA.

4.28.1 Strengths

584. The RP has adequately used the PSA to demonstrate that risks have been reduced to ALARP. The PSA results are low, compare favourably with the SAPs Targets, and also demonstrate that the risks are balanced.

4.28.2 Outcomes

585. My assessment of the RP's submissions on the demonstration that the risks have been reduced to ALARP for PSA against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.28.3 Conclusion

586. In my opinion, the RP has developed and documented a detailed process for using the PSA and results in a systematic and comprehensive way to identify potential options for design improvement to reduce the risk of the generic UK HPR1000 design to ALARP.

587. I find that the RP has used the process developed to systematically and thoroughly use the PSA model and results to identify insights and vulnerabilities of the generic UK HPR1000 design.

588. Thus, the demonstration that risks have been reduced to ALARP is adequate for GDA from a PSA perspective.

4.29 Consolidated Safety Case

589. The evolution of the PSA documents (including all PSA models and reports discussed in this assessment report) through GDA is related to the evolution of the design for GDA. Based on ONR feedback and also on independent review of the design to meet the expectations of reducing risks to ALARP the design reference during GDA has progressed from DR1 through DR2.1, DR2.2 and finally DR3. The final PCSR submission is based on DR3. A comprehensive assessment of various PSA documents was conducted on a sampling basis through DR2.1 related deliverables such as Level 1 and 2 PSA for internal events, internal fire, internal flooding, and other hazards PSA. Several RQs and ROs were raised, and the RP provided the responses to meet the expectations of ONR on the PSA topic.

590. In Chapter 14 of the PCSR the relevant updates to the PSAs were progressed to meet the expectations of ONR to consolidate all the RQ and RO responses into the safety case.

591. To inform my judgement on the adequacy of the RP's consolidation, I assessed a sample of the following final documentation:

- PCSR Chapter 14 (Ref. 3)
- Level 2 PSA, Rev C (Ref. 52)
- Internal Fire PSA, Rev C (Ref. 51)
- Level 1 PSA, Rev C (Ref. 55)
- ALARP demonstration report Rev D (Ref. 56)

592. My assessment of PCSR Chapter 14 was on the consolidation of the results and insights from the PSA. I have sampled a few topics such as the Plant Damage state groups and code for POS A and B reported in the Chapter 14 Table T-14.5-4 and

results of external hazards to CDF reported in Table T-14.9-1 and found these to be aligned to the latest updates of the PSA documents. I am content that the reporting of the information is all aligned with latest versions of the PSA documentation. I reviewed Chapter 14 and found that it met my regulatory expectations. I have presented some examples of specific samples of my assessment in the following paragraphs.

593. I assessed for the inclusion of the responses provided in RQ-UKHPR1000-1595, 1596, 1625, 1646 and 1647 into the Level 2 PSA, Ver. C (Ref. 52). I sampled specific topics within the documentation such as:

- Inclusion of evidence and justification on the PDS attributes in sub-section 4.1.3 of Ref. 52 (a response in RQ-UKHPR1000-1646);
- Inclusion of the details regarding calculation consideration and sensitivity in the source term analysis in sub-section 4.9.2 (a response to RQ-UKHPR1000-1595; and
- The inclusion of the evidence related to hydrogen phenomenon analysis in sub-section 4.3.5 (a response to RQ-UKHPR1000-1596).

594. Based on my assessment I am content with the consolidation of the safety case in Level 2 PSA, Rev C (Ref. 52), and with the PCSR Chapter 14.

595. I assessed for the inclusion of the response provided in RQ-UKHPR1000-1687 into the Internal fire, Rev C (Rev. 51). I sampled specific topics within the documentation such as:

- the description the approach to obtain the CDF of the multi-compartment fires (response to query 11(a) and (b) of RQ-UKHPR1000-1687) is embedded in Chapter 14.3.5;
- the sensitivity result for the use of Bin 4 for Main control board initiating event frequency (response to query 3 of RQ-UKHPR1000-1687) is embedded in a new Chapter 18.4; and
- the appropriate treatment of junction boxes aligned with FAQ-13-0006 and reporting (in response to query 4 of RQ-UKHPR1000-1687) in the report has now been made in Chapter 14.1.1.3 and further details in Chapter 14.2.1 to 14.2.18.

596. Based on my assessment I am content with the consolidation of the safety case in internal fire PSA, Rev C (Rev. 51).

597. I assessed Level 1 PSA, Rev C (Ref. 55) for consolidation of the DR3 into the PSA model. I sampled a few modifications and some of the supporting analysis for incorporation into the documentation or the model where appropriate. I am content with the consolidation.

598. The ALARP demonstration report (Ref. 56) has already been discussed in my assessment on ALARP and the resolution of the matters identified in RO-UKHPR1000-0043. I am therefore content of the consolidation of the safety case through Rev D of the ALARP demonstration through PSA.

4.29.1 Strengths

599. The licensee has a systematic process to capture the updates necessary, arising from the RQ and RO responses in the consolidation of the safety case.

600. Chapter 14 of the PCSR met my regulatory expectations.

4.29.2 Outcomes

601. My assessment of the RP’s submissions on the consolidated safety case Chapter 14 against the expectations of the ONR SAPs and PSA TAG has found no significant concerns for the purposes of GDA.

4.29.3 Conclusion

602. Overall, I am content with Chapter 14 of the PCSR, and with the consolidation of the safety case through PCSR Chapter 14 and other associated PSA documentation.

4.30 Comparison with Standards, Guidance and Relevant Good Practice

603. I have used the RGP, standards and guidance explained in sub-section 2.4.3 of this report to compare with the RP’s submissions on PSA.

604. In my opinion, the RP has performed the PSA analysis well compared with this RGP. In each of the individual sub-sections above, where applicable, I have discussed this in more detail.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

605. This report presents the findings of my PSA assessment of the generic UK HPR1000 design as part of the GDA process.

606. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- I am satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for PSA. I consider that, from a PSA viewpoint, the UK HPR1000 design is suitable for construction in the UK subject to future permissions and permits beings secured.
- The UK HPR1000 PSA and the responses to the supporting ROs and RQs broadly meet the expectations of ONR's PSA TAG (Ref. 4) and SAPs FA.10, FA.11, FA.12, FA.13 and FA.14.
- I raised two Assessment Findings as I identified gaps in the RP's Seismic PSA and the consideration of C&I and software in the RP's submissions that should be addressed but need site-specific and finalised design information in order to address them fully.

607. Based on my assessment, I have concluded that the UK HPR1000 PSA methods, scope, completeness, justification and quality of the documentation, and the clarity of the substantiation, broadly meets the expectations of ONR's PSA TAG and is adequate to support the PCSR.

608. The UK HPR1000 PSA has a credible and defensible basis and allows for comparison against Targets 7, 8 and 9 contained in ONR's SAPs. Comparison of the results of the UK HPR1000 PSA to Targets 7 and 8 show that the estimated level of risk is below the BSO. Comparison of the results of the UK HPR1000 PSA to Target 9 shows that the estimated level of risk is well below the BSL. However, the level of risk is slightly above the BSO for Target 9.

609. The PSA has been used adequately during GDA to ensure that risks are being managed towards an ALARP position as the design continues through GDA and into the site-specific stage. The PSA has been used to identify ALARP improvements which have been incorporated into the GDA design reference and to calculate the risk significance of these changes to the design. My assessment has not found any major areas of the plant design for which additional ALARP analysis was needed in GDA or where alternative design features were required.

610. The scope and content of the PSA is adequate for GDA. However the PSA needs to be revised beyond GDA to reflect the detailed design and address the Assessment Findings identified by my review, include site-specific characteristics and operational matters and to allow for these aspects to be risk informed. In addition, I have identified multiple minor shortfalls which I would recommend the licensee considers to strengthen its safety case submissions but these are not significant enough for ONR to track.

611. The core damage frequency for internal events Level 1 PSA was low ($3.85\text{x}10^{-7}$ /ry). The large release frequency for Level 2 PSA was also low ($6.05\text{x}10^{-8}$ /ry).

612. From the PSA perspective, and for matters within the scope of PSA, the final design of the UK HPR1000 achieves a level of risk consistent with RGP for a modern plant and unless they are easily achievable, my expectation is that further modifications are likely to be grossly disproportionate.

613. 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 PSA perspective.

5.2 Recommendations

614. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From a PSA perspective, ONR should grant a DAC for the generic UK HPR1000 design.
- **Recommendation 2**: The two 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. http://www.onr.org.uk/saps/saps2014.pdf

3. *Pre-Construction Safety Report Chapter 14 Probabilistic Safety Assessment,* GHX00620014KPGB02GN, Rev. F, CGN, CM9 2019/283519

4. Technical Assessment Guides

   Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), NS-TAST-GD-005, Rev. 11, November 2020, ONR

   Probabilistic Safety Analysis, NS-TAST-GD-030, Rev. 7, June 2019, ONR

   Validation of Computer Codes and Calculation Methods, NS-TAST-GD-042, Rev. 5, September 2020, ONR

   Civil Engineering, NS-TAST-GD-017 Revision 4. ONR. November 2020
   Essential Services, NS-TAST-GD-019 Revision 5. ONR. July 2019

   Guidance on Mechanics of Assessment, NS-TAST-GD-096, Revision 4, ONR, May 2020
   http://www.onr.org.uk/operational/tech_asst_guides/index.htm

5. *GDA Step 4 Assessment Plan of PSA topic for the UK HPR1000 Reactor.* ONR-GDA-UKHPR1000-AP-19-001. Revision 1. February 2020. ONR. CM9 Ref. 2020/374731

6. *Impact Analysis on Internal Events Level 1 and Level 2 PSA,* GHX00650155DOZJ02GN, Rev. A, January 2021, CGN, CM9 2021/8887

7. *WENRA Safety Reference Levels for Existing Reactors 2020,* February 2021, WENRA, https://www.wenra.eu/sites/default/files/publications/wenra_safety_reference_level_for_existing_reactors_2020.pdf

8. IAEA Guidance

   Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, SSG-3, 2010, IAEA

   Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, 2000, IAEA

   Prospective Radiological Environmental Impact Assessment for Facilities and Activities, Safety Standards Series No. GSG-10, 2018*,* IAEA

   Case Study on Assessment of Radiological Environmental Impact from Potential Exposure, IAEA-TECDOC-1914, 2020, IAEA

   Case Study on Assessment of Radiological Environmental Impact from Potential Exposure, SSG-4, 2010, IAEA

   Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1, Rev. 1, 2016, IAEA

   Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA TECDOC-1804, 2016, IAEA

   Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3, Rev. 1, 1999, IAEA

9. USNRC guidance

Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, NUREG/CR-6268, Rev. 1, September 2007, Idaho National Laboratory

Control of Heavy Loads at Nuclear Power Plants, NUREG-0612, 1980, USNRC

A Survey of Crane Operating Experience at US Nuclear Power Plants from 1986 through 2002, NUREG-1774, 2003, USNRC

Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plant, NUREG-1738, 2001, USNRC

Accident Sequence Evaluation Program: Human Reliability Analysis Procedure, NUREG/CR-4772, 1987, USRNC

Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278, 1983, USNRC

The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883, 2005, USNRC

Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928, 2015, USNRC

Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process, NUREG/CR-1829, 2008, USNRC

Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, 1994, USNRC

Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, NUREG/CR-7007, 2008, USNRC

EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Final Report, NUREG/CR-6850, EPRI 1011989, 2005, USNRC

Fire Dynamics Tools (FDTs) Quantitative Fire Hazard Analysis Methods for the USNRC Fire Protection Inspection Program, NUREG-1805, 2004, USNRC

Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database: United States Fire Event Experience Through 2009, NUREG-2169, January 2015, USNRC

Refining and Characterizing Heat Release Rates from Electrical Enclosures during Fire (RACHELLE-FIRE), Volume 1: Peak Heat Release Rates and Effect of Obstructed Plume, NUREG-2178, EPRI 3002005578, 2016, USNRC

Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications, Volume 4: Fire-Induced Vulnerability Evaluation, NUREG-1824, May 2007, USNRC

Cable Heat Release, Ignition, and Spread in Tray Installations During Fire (CHRISTIFIRE), Phase 1: Horizontal Trays, NUREG/CR-7010 Vol. 1, 2012, USNRC

Joint Assessment of Cable Damage and Quantification of Effects from Fire (JACQUE-FIRE), Volume 1: Phenomena Identification and Ranking Table (PIRT) Exercise for Nuclear Power Plant Fire-Induced Electrical Circuit Failure, NUREG/CR-7150, Volume 1, October 2012, USNRC

Joint Assessment of Cable Damage and Quantification of Effects from Fire (JACQUE-FIRE) Volume 2: Expert Elicitation Exercise for Nuclear Power Plant Fire-Induced Electrical Circuit Failure, NUREG/CR-7150, Volume 2, May 2014, USNRC

Cable Tray Ignition, FAQ 16-0011, Revision 1, 2016, USNRC

Hot Work/Transient Fire Frequency Influence Factors, FAQ 12-0064, 2013, USNRC

Clarifications on Treatment of Sensitive Electronics, FAQ 13-0004, 2013, USNRC

Modelling Junction Box Scenarios in a Fire PRA, FAQ 13-006, 2013, USNRC

Cable Fires Special Cases: Self Ignition and Caused by Welding and Cutting, FAQ 13-0005, 2013, USNRC

US NRC. Glossary of Risk-Related Terms in Support of Risk-Informed Decision-making. NUREG -2122, 2013, USNRC

Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment, EPRI, EPRI Report 1019194, 2014, USNRC

http://www.nrc.gov

10. *International standard for electrical, electronic and programmable electronic safety related systems*, IEC 61508, Edition 2, 2010, IEC

11. *Standard data element types with associated classification scheme*, IEC 61360, 2017, IEC

12. *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF),* IEC 62340, 2007, IEC

13. *Guidance for Post Fire Safe Shutdown Circuit Analysis,* NEI 00-01, Revision 4, *September* 2016, NEI

14. *PWR Spent Fuel Pool Risk Assessment Integration Framework and Pilot Plant Application*, 3002002691, 2014, EPRI

15. *Seismic Probabilistic Risk Assessment Implementation Guide*, 3002000709, 2013, EPRI

16. *Methodology for Developing Seismic Fragilities*, TR-103959, 1994, EPRI

17. *Standard for Level 1/Large Early Release Frequency PRA for NPP Applications*, ASME/ANS RA-S, 2018, ASME

18. *Standard for Radiological Accident Offsite Consequences Analysis (Level 3 PRA) to Support Nuclear Installations Applications,* ASME/ANS RA-S-1.3-2017,July 2017, ASME

19. *Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), RA-S-1.2-2014,* 2017, ASME

20. *Requirements for Low Power and Shutdown PRA,* 58.22-2014, 2017, ASME

21. *Methodology for PIE Identification*, GHX00100008DOZJ03GN, Rev. H, January 2019, CGN, CM9 Ref. 2019/26887

22. *Methodology of Internal Event Level 1 PSA,* GHX00650027DOZJ02GN, Rev. B, March 2020, CGN, CM9 2020/99201

23. *Methodology of Human Reliability Analysis*, GHX00650030DOZJ02GN, Rev. B, March 2020, CGN, CM9 2020/82774

24. *Methodology of Spent Fuel Pool PSA,* GHX00650029DOZJ02GN, Rev. A, May 2018, CGN, CM9 2018/180090

25. *Methodology of Level 3 PSA,* GHX00650004DOHB02GN, Rev. D, November 2020, CGN, CM9 2020/312677

26. *Methodology of Internal Flooding PSA,* GHX00650031DOZJ02GN, Rev. A, May 2018, CGN, CM9 2018/180088

27. *Methodology of External Hazards PSA,* GHX00650032DOZJ02GN, Rev. A, May 2018, CGN, CM9 2018/180086

28. *Methodology of Internal Fire PSA*, Rev. A, CGN, May 2018, CM9 2018/180081

29. *Methodology of Internal Events Level 1 PSA, GHX00650027DOZJ02GN,* Rev A, CM9 2018/139577

30. *Methodology for the modelling of Computer Based I&C System Reliability in the PSA*, GHX00650003DIYK02GN, CGN, CM9 2020/130942

31. *Methodology of Level 2 PSA,* GHX00650028DOZJ02GN, Rev. A, May 2018, CGN, CM9 2018/180093

32. *Methodology of Seismic PSA,* GHX00650128DOZJ02GN, Rev. B, July 2019, CGN, CM9 2019/226157

33. *Initiating Event Grouping and Frequency Analysis of Internal Events Level 1 PSA,* GHX00650145DOZJ02GN, Rev. D, September 2020, CGN, CM9 2020/259692

34. *Applicability Analysis of Initiating Event Analysis Methodology for Internal Events Level 1 PSA*, GHX00650154DOZJ02GN, Rev. A, June 2020, CGN, CM9 Ref. 2020/199705

35. *PSA Data Analysis Report*, GHX00650015DOZJ02GN, Rev. F, January 2020, CGN, CM9 2020/14143

36. *Internal Events Level 1 PSA,* GHX00650001DOZJ02GN, Rev. B, April 2020, CGN, CM9 2020/112233

37. *Spent Fuel Pool Level 1 PSA,* GHX00650120DOZJ02GN, Rev. A, March 2020, CGN, CM9 2020/97821

38. *Human Reliability Analysis for Internal Events Level 1 PSA*, GHX00650089DIKX02GN, Rev. C, April 2020, CGN, CM9 2020/112299

39. *UK HPR1000 - Internal Flooding Level 1 PSA,* GHX00650004DOZJ02GN, Rev. C, May 2019, CGN, CM9 2019/143881

40. *External Flooding Level 1 PSA,* GHX00650141DOZJ02GN*,* Rev. A, May 2020, CGN, CM9 2020/163047

41. *External Hazards Level 1 PSA Report (and model),* GHX00650007DOZJ02GN*,* Rev C, December 2020, CGN, CM9 2020/322030

42. *Level 2 PSA*, GHX00650140DOZJ02GN, Rev. B, September 2020, CM9, CGN, 2020/289966

43. *Step 4 Chemistry Step Assessment of the UK HPR1000 Reactor,* ONR-NR-AR-21-02, January 2022, ONR, CM9 2021/41488

44. *Level 3 PSA Report,* GHX00650002DOHB02GN, Rev. A, January 2021, CGN, CM9 2021/8460

45. *Risk Insights of Seismic PSA for UK HPR1000,* GHX00650142DOZJ02GN, Rev A, May 2020,CGN, CM9 2020/161966

46. *Worker Risk Assessment Report (Target 5 and 6),* GHX00530012DNFP02GN, Rev. B, CGN, November 2020, CM9 2020/315804

47. *Level 1 Internal Fire PSA (Model),* Rev A, CGN, CM9 2019/138002

48. *Internal Fire Level 1 Probabilistic Safety Assessment,* GHX00650005DOZJ02GN, Rev. B, December 2020, CGN, CM9 2020/322621

49. *Internal Flooding Level 1 PSA, GHX00650004DOZJ02GN,* Rev D, October 2020, CGN CM9 2020/313752

50. *Level 2 PSA,* GHX00650002DOZJ02GN, Rev. A, November 2018, CGN, CM9 Ref. 2018/378858

51. *Internal Fire Level 1 PSA,* GHX00650005DOZJ02GN, Rev. C, July 2021, CGN, CM9 2021/58829

52. *Level 2 PSA (Model),* Rev. C, July 2021, CGN, CM9 2021/51695

53. *ONR-395 UK HPR1000 PSA Review - TSC Final Report,* Rev. A, July 2021, Jacobsen Analytics, CM9 2021/71433

54. *Worker Risk Assessment Methodology for Radiation Protection Targets 5 and 6*, GHX00100037DNFP03GN, Rev. C, September 2020, CGN, CM9 2020/289456

55. *Internal Events Level 1 PSA,* GHX00650001DOZJ02GN, Ver. C, July 2021, CGN, CM9 2021/58822

56. ALARP Demonstration Report for PSA, GHX00100057KPGB03GN, Rev D, January 2021, CGN, CM9 2021/2778

57. *UK HPR1000 – Regulatory Observation (RO) Tracking Sheet, January 2020,* ONR, CM9 2020/8667

58. *Step 4 Management for Safety and Quality Assurance of the UK HPR1000 Reactor,* ONR-NR-AR-21-003, Rev. 8, January 2022, CM9 2021/42541

59. *Fault Studies Step 4 Assessment Report for the UK HPR1000 Reactor,* ONR-NR-21-014, January 2022, ONR, CM9 2021/44803

60. *Decoupling LOCA Criteria for Fuel*, FS1-0046539, Rev. 2, March 2020, Framatome, CM9 2020/79659

61. *LB-LOCA Safety Case Clarification and Core Assessment Report*, GHX00600007DRRL02GN, Rev. C, June 2021, CGN, CM9 2021/46979

62. *Large Break – Loss of Coolant Accident (Up to Double-Ended Break)*, GHX00600004DRAF02GN, Rev. C, November 2019, CGN, CM9 2019/352765

63. *Severe Accident Analysis Step 4 Assessment Report for the UK HPR1000 Reactor,* ONR-NR-21-008, January 2022, ONR, CM9 2021/49781

64. *Spent Fuel Interim Storage Step 4 Assessment Report for the UK HPR1000 Reactor,* ONR-NR-21-017, January 2022, ONR, 2021/51327

65. *GDA Step 3 Assessment Note - PSA*, ONR-NR-AN-19-011, Rev. 1, January 2020, ONR, CM9 2019/337900

66. *UK HPR1000 – Regulatory Query (RQ) Tracking Sheet,* January 2020, ONR, CM9 Ref. 2020/8662

67. *RPV Head Drop Analysis Report,* GHX00100012DPLX44GN, Rev. E, February 2021, CGN, CM9 2021/17447

68. *Fuel and Core Step 4 Assessment Report for UK HPR1000 GDA*, ONR-NR-AR-21-021, Rev. A, ONR, CM9 2021/23724

69. Detailed Accident Sequence Analysis for LOOP and IB LOCA, GHX00650168DOZJ02GN, Rev. A, January 2021, CGN, CM9 2021/8487

70. *MCLs Failure Consequence Analysis Report*, GHX44700002DPZS03GN, Rev. D, November 2020, CGN, CM9 2020/309256

71. *EMIT Consistency Analysis,* GHX42EMT004DOYX45GN, Rev. A, September 2020, CGN, CM9 2020/289528

72. *EMIT Strategy Implementation Report,* GHX42EMT005DOYX45GN, Rev. A, December 2020, CM9, CGN, 2021/233

73. *Emergency Feedwater System Analysis for Level 1 PSA,* GHX00650059DOZJ02GN, Ver. C, March 2020, CGN, CM9 2020/116860

74. *Pre-Construction Safety Report Chapter 13,* HPR-GDA-PCS-0013, Rev. F, September 2021, CGN, CM9 2021/48479

75. *EHR - Containment Heat Removal System Design Manual, Chapter 6, Operation and Maintenance,* GHX17EHR006DNHX45GN, Rev. D, July 2021, CM9 2021/53522

76. *Step 4 Structural Integrity Assessment Report of the UK HPR1000 Reactor*, ONR-NR-AR-21-016*,* Rev. A, ONR CM9 2021/52300

77. *Optioneering of the EHR [CHRS] Related to Inadvertent Reactor Pit Flooding*, GHX00100002DNHX45GN, Rev. C, December 2020, CGN, CM9 2020/320736

78. *Cat1-HVAC Systems Diversity Modification, MOD-35,* HPR-GDA-LETT-0070, Rev. A, October 2020, CGN, CM9 2020/304342

79. *Step 4 Human Factors Assessment Report for the UK HPR1000 Reactor, ONR-NR-AR-21-013,* Rev. A., ONR CM9 2021/54151

80. *HRA Summary Report,* GHX00100183DIKX03GN, Rev. A, May 2021, CGN, CM9 2021/43592

81. *Modelling of a Typical C&I Function Reliability in the PSA*, GHX00650004DIYK02GN, Rev. A, August 2020, CGN, CM9 2020/232678

82. *Examination, Maintenance, Inspection and Testing (EMIT) Windows,* GHX42EMT002DOYX45GN, Rev. D, January 2021, CGN, CM9 2021/8441

83. *Examination, Maintenance, Inspection and Testing (EMIT) Strategy,* GHX42EMT001DOYX45GN, Rev. D, March 2021, CGN, CM9 2021/28205

84. *Optioneering Report M35-GHTCN000127-B-Cat1-HVAC Systems Diversity Modification*, HPR-GDA-LETT-0070 – 2, Rev. A, October 2020, CGN, CM9 2020/304341

85. *PIE List of UK HPR1000 of Internal Event (Except for Loss of Support System)*, GHX00100110DOZJ03GN, Rev. H, May 2021, CGN, CM9 2021/43558

86. *The Delivery of UK HPR1000 GDA Design Modification - Category 2 "Modifications of the BFX to Adopt Gantry Crane for Fuel Handling (M94-GHTCN00203-A),* HPR-GDA-LETT-0114, Rev. A, June 2021, CGN, CM9 2021/44825

87. *External Hazards Level 1 PSA, GDA-REC-CGN-003840 - GHX00650007DOZJ02GN,* Rev B, February 2019, CGN, CM9 2019/59095

88. OECD/NEA, *"Use and Development of Probabilistic Safety assessment: an Overview of the Situation at the End of 2010*", NEA/CSNI/R(2012)11, December 2012, www.oecd-nea.org

89. *Civil Engineering Step 4 Assessment Report for the UK HPR1000 Reactor,* ONR-NR-AR-21-018, Rev. A, January 2022, ONR, CM9 2021/57205

90. *Status of Practice for Level 3 Probabilistic Safety Assessment,* NEA/CSNI/R(2018)1*,* NEA, 2018, www.oecd-nea.org

91. *Level 3 PSA Software Qualification Report,* GHX00650003DOHB02GN, Rev. A, April 2020, CGN, CM9 2020/126190

92. *Assessing Dose of the Representative Person for the Purpose of the Radiation Protection of the Public,* ICRP Publication 101a Annex ICRP 36(3), ICRP, 2006

93. *UK HPR1000 PSA Assessment – TSC Final Report – Appendix H – Level 3 PSA Assessment,* August 2021, Jacobsen Analytics, CM9 2021/64533

94. *ALARP Demonstration Report for Probabilistic Safety Assessment,* GHX00100057KPGB03GN, Rev. A, October 2019, CGN, CM9 2019/310135

95. *UK HPR1000 Generic Site Report*, GHX00100091DOZJ03GN, Rev. B, September 2020, CGN, CM9 2020/286714

96. *An Improvement of LOOP Event Mitigation*, M-56-GHTCN000146, HPR-GDA-LETT-0083, Rev. A, November 2020, CGN, CM9 2020/306795

97. *UK HPR1000 Design Reference Report,* NE15BW-X-GL-0000-000047, Rev. I, September 2021, CGN, CM9 2021/68330

Annex 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No	SAP Title	Description
FA.10	Need for PSA	Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis.
FA.11	Validity of PSA	PSA should reflect the current design and operation of the facility or site.
FA.12	Scope and Extent of PSA	PSA should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults.
FA.13	Adequate Representation of PSA	The PSA model should provide an adequate representation of the facility and/or site.
FA.14	Use of PSA	PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities.
AV.1	Theoretical Models	Theoretical models should adequately represent the facility and site.
AV.2	Calculation Methods	Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place.
AV.3	Use of Data	The data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.
AV.4	Computer Models	Computer models and datasets used in support of the safety analysis should be developed, maintained and applied in accordance with quality management procedures.
AV.5	Documentation	Documentation should be provided to facilitate review of the adequacy of the analytical models and data.

SAP No	SAP Title	Description
AV.6	Sensitivity Studies	Studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.
AV.7	Data Collection	Data should be collected throughout the operating life of the facility to check or update the safety analysis.
AV.8	Update and Review	The safety analysis should be updated where necessary, and reviewed periodically.

Annex 2

Assessment Findings

Number	Assessment Finding	Report Section
AF-UKHPR1000-0104	The licensee shall, as part of detailed design, undertake PSA analysis to demonstrate the risk from C&I failures. This analysis should explicitly include C&I hardware and software failures in the PSA models and should include both Level 1 and 2 PSA for all categories of initiating events and plant operating states.	4.10.2
AF-UKHPR1000-0185	The licensee shall, as part of site-specific and detailed design activities, undertake PSA analysis to demonstrate the risk from seismic events. This should include both Level 1 and 2 PSA for all categories of initiating events and plant operating states.	4.18.2