Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Probabilistic Safety Analysis Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-019
Revision 0
10 November 2011

COPYRIGHT

First published December 2011

For published documents, the electronic copy on the ONR website remains the most current publically available version and copying or printing renders this document uncontrolled.

PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Directorate (ND) or the Nuclear Installations Inspectorate (NII) should be taken as references to ONR.

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process and the submissions made by EDF and AREVA relating to the UK EPR^{TM} reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires EDF and AREVA to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the EDF and AREVA UK EPR^{TM} reactor.

EXECUTIVE SUMMARY

This report presents the findings of the Probabilistic Safety Analysis (PSA) assessment of the UK EPR undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the November 2009 Pre-construction Safety Report (PCSR) and supporting documentation submitted by EDF and AREVA during Step 4.

This assessment has followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by EDF and AREVA were examined, in Step 3 the arguments that underpin those claims were examined.

The scope of the Step 4 assessment was to review the safety aspects of the UK EPR reactor in greater detail, by examining the evidence supporting arguments and claims made in the safety documentation, building on the assessment already carried out for Steps 2 and 3, and to make a judgement on the adequacy of the PSA information contained within the PCSR and Supporting Documentation.

It is seldom possible, or necessary, to assess a safety case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic specific or generic weaknesses in the safety case. To identify the sampling for the PSA an assessment plan for Step 4 was set-out in advance.

During GDA Step 3 I concluded that EDF and AREVA had produced a large, modern standards PSA and that the techniques and methodologies that they had used were acceptable in principle. My assessment in GDA Step 4 has focussed on establishing the evidence supporting the PSA model and the results that this model has produced. For PSA "evidence" has been broadly interpreted as being the detailed implementation of the methods and techniques together with the numerical data and parameters used to quantify the PSA.

In addition to carrying out an assessment of the UK EPR PSA, I have undertaken assessment work in support of other technical areas, most notably reviewing updated PSA submissions produced by EDF and AREVA to incorporate additional Control and Instrumentation (C&I) engineering in the form of a Non Computerised Safety System.

A number of items have been agreed with EDF and AREVA as being outside the scope of the GDA process and hence have not been included in my assessment; they are simply noted in the report as needing to be addressed post GDA.

From my assessment I have concluded that:

- EDF and AREVA have provided large, modern standards PSA as part of their overall GDA submission.
- The scope of the PSA includes internal faults, internal and external hazards, all operating states and reasonable allowances for maintenance and test. It also includes all significant sources of radioactivity.
- The PSA is an adequate representation of the design described in the GDA submissions and there is good evidence that the PSA has been used to inform the development of the design.
- Major modifications to the C&I provisions have been adequately incorporated into the UK EPR PSA.
- Integration of the Level 1 and Level 2 PSA models is a strength of the analysis.

- The PSA results presented by EDF and AREVA meet the Basic Safety Objectives (BSO) of Targets 7, 8 and 9 from Numerical Target NT.1 of the Safety Assessment Principles (SAP).
- The UK EPR PSA provides sufficient information at this stage in the project to conclude that all of the significant risks have been identified.

There are, however, some limitations identified in this assessment report as findings, and many of them point to the need for the PSA to develop into a suitable operational support tool. One such a limitation is the asymmetry of the PSA model, for example all of the Loss of Coolant Accidents (LOCA) are assumed to occur in one of the loops - at a summed frequency covering all loops - to simplify the model. Whilst this will not invalidate high level numerical results, it can lead to distortion of PSA insights for operational purposes and will ultimately need to be addressed so that the PSA provides an appropriate tool to support operation of a potential EPR in the UK.

Other limitations are associated with lack of design detail available at this stage of the process, and the need for clear documentation of the analysis and the assumptions that have been made which need to be carried into the future design and operation of a UK EPR.

Overall, based on the sample undertaken in accordance with Nuclear Directorate (ND) procedures, I have concluded that an acceptable case has been made for the UK EPR PSA submitted as part of the PCSR. Based on the scope of information supplied for GDA I am broadly satisfied that the UK EPR reactor is suitable for construction in the UK.

Finally, as already mentioned above, in some areas the lack of detailed information available at this stage has limited the extent of my assessment. As a result ND will need additional information to underpin my conclusion and these are identified as Assessment Findings to be carried forward as normal regulatory business. These are listed in Annex 1.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ASEP	Accident Sequence Evaluation Program
ASN	Autorité de Sûreté Nucléaire (French nuclear safety authority)
ATWS	Anticipated Transient without SCRAM (Reactor Shutdown)
BMS	(Nuclear Directorate) Business Management System
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
C&I	Control and Instrumentation
CCF	Common Cause Failure
CCWS	Component Cooling Water System
CDES	Core Damage End State
CDF	Core Damage Frequency
CET	Containment Event Tree
DBE	Design Basis Earthquake
DDT	Deflagration to Detonation Transition
DG	Diesel Generator
DNB	Departure from Nucleate Boling
DNBR	Departure from Nucleate Boling Ratio
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EMIT	Examination, Maintenance, Inspection and Testing
EFWS	Emergency Feedwater System
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute (USA)
EPS	Electrical Power System
ESWS	Essential Service Water System
EUR	European Utilities Requirements
f/d	failures per demand
FMEA	Failure Modes and Effects Analysis
GDA	Generic Design Assessment
HCLPF	High Confidence of Low Probability of Failure
HFE	Human Failure Event
HRA	Human Reliability Analysis

LIST OF ABBREVIATIONS

HSE	The Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning
IAEA	The International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IE	Initiating Event
IRWST	In-containment Refuelling Water Storage Tank
ISLOCA	Interfacing System LOCA
JAC	Fire fighting water supply system
LERF	Large Early Release Frequency
LHSI	Low Head Safety Injection
LOCA	Loss Of Coolant Accident
LOCC	Loss Of Cooling Chain
LOOP	Loos Of Offsite Power
LUHS	Loss of Ultimate Heat Sink
LWR	Light Water Reactor
MAAP	Modular Accident Analysis Programme
MCS	Minimal Cut Set
MGL	Multiple Greek Letter
MFW	Main Feedwater (System)
MHSI	Medium Head Safety Injection
MLOCA	Medium LOCA
MOV	Motor Operated Valve
MDEP	Multi-national Design Evaluation Programme
NCSS	Non Computerised Safety System
ND	The (HSE) Nuclear Directorate
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
NT	Numerical Target (in SAPs)
OECD	Organisation for Economic Cooperation and Development
OL3	Olkiluoto 3 – EPR under construction in Finland
OSSA	Operating Strategy for Severe Accident
PCSR	Pre-construction Safety Report
PGA	Peak Ground Acceleration
POS	Plant Operating State

LIST OF ABBREVIATIONS

POSR	Pre Operational Safety Report
PS	Protection System
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report
PWR	Pressurised Water Reactor
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RGA	Risk Gap Analysis
RI	Regulatory Issue
RIA	Regulatory Issue Action
RO	Regulatory Observation
SA	Severe Accident
SAP	Safety Assessment Principles
SBO	Station Blackout
SEL	Seismic Equipment List
SFAIRP	So Far As Is Reasonably Practicable
SGTR	Steam Generator Tube Rupture
SIS	Safety Injection and Residual Heat Removal System
SLB	Steam Line Break
SMA	Seismic Margins Assessment
SME	Seismic Margins Earthquake
SOKC	State Of Knowledge Correlation
SSC	System, Structure and Component
SSER	Safety, Security and Environmental Report
SSS	Start-up and Shutdown System
STUK	The Finish Nuclear Safety Authority
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
TSC	Technical Support Contractor
US NRC	Nuclear Regulatory Commission (United States of America)
WENRA	The Western European Nuclear Regulators’ Association

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1 This report presents the findings of the Probabilistic Safety Analysis (PSA) assessment of the UK EPR PCSR (Ref. 1) and supporting documentation provided by EDF and AREVA under the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. Assessment was undertaken of the November 2009 Pre-Construction Safety Report (PCSR) and the supporting evidentiary information derived from the Submission Master List (Ref. 2). The approach taken was to assess the principal submission, i.e. the PCSR, and then undertake assessment of the relevant documentation sourced from the Submission Master List on a sampling basis in accordance with the requirements of ND Business Management System (BMS) procedure AST/001 (Ref. 3). The Safety Assessment Principles (SAP) (Ref. 4) have been used as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 During the PSA assessment a number of Technical Queries (TQ) and Regulatory Observations (RO) were issued and the responses made by EDF and AREVA assessed.

3 A number of items have been agreed with EDF and AREVA as being outside the scope of the GDA process and hence have not been included in this assessment; they are simply noted in the report as needing to be addressed post GDA.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR PSA

4 The intended assessment strategy for Step 4 for the PSA topic area was set out in an assessment plan (Ref. 5) that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below.

2.1 Assessment Plan

5 Assessment within the Nuclear Directorate (ND) is undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 3). AST/001 sets down the process of assessment within ND and explains the process associated with sampling of safety case documentation. The SAPs (Ref. 4) have been used as the basis for the assessment of the PSA associated with the UK EPR design. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

6 The assessment has been conducted in accordance with ND's Business Management System and in line with ND policy; a targeted and structured sampling has been used to improve the overall efficiency of the PSA assessment process.

2.2 Standards and Criteria

7 The main standards and criteria used are HSE's Safety Assessment Principles (SAP) (Ref. 4); SAPs FA.10 to FA.14 and Numerical Targets NT.1 (Targets 7 to 9) and NT.2 are the relevant parts of that document. Also of importance are relevant parts of the International Atomic Energy Agency (IAEA) standards (Ref. 6) and the Western European Nuclear Regulators Association (WENRA) reference levels (Ref. 7).

8 The above PSA related SAPs, IAEA standards and WENRA reference levels are embodied and enlarged on in ND's Technical Assessment Guide (TAG) on PSA (Ref. 8) and it is this guide that provides the principal means for assessing the PSA in practice.

2.3 Assessment Scope

9 The objective of the GDA Step 4 assessment has been to review the safety aspects of the proposed reactor designs in a more detailed way by examining the evidence supporting arguments and claims made in the EDF and AREVA safety documentation. GDA Step 4 builds on the assessment already carried out for GDA Steps 2 and 3 with the objective of making a judgement on the adequacy of the PSA contained within the PCSR and Supporting Documentation.

10 For PSA "evidence" is broadly interpreted as being:

- the detailed implementation of the methods and techniques; and
- the data and parameters used to quantify the PSA.

It is not always a simple matter to disentangle the methods from the data, judgements and implementation, so some degree of overlap between the GDA Step 3 and GDA Step 4 assessments is inevitable.

11 The overall bases for assessment in GDA Step 4 were the PSA elements of:

- (i) the update to the Submission / PCSR / Supporting Documentation, (ii) the Design Reference that relates to the Submission / PCSR as set out in UK EPR GDA Project Instruction UKEPR/I/002;

- Design Change Submissions – which were proposed by EDF and AREVA that were incorporated within the GDA scope by agreement with HSE.

12 The main PSA documents sampled during the GDA Step 4 assessment are listed in Table 1 and all PSA related matters that have been resolved during the GDA process are suitably dealt with in the relevant sections of the consolidated PCSR (Ref. 61) and its supporting documents.

2.3.1 Findings from GDA Step 3

13 The GDA Step 3 assessment report (Ref. 9) concluded that EDF and AREVA had produced a large, modern standard PSA supporting the PCSR submitted to ND and that these documents cover all of the areas expected in the scope of a Nuclear Power Plant (NPP) PSA. For the most part the methods and techniques used by EDF and AREVA were considered acceptable in principle, though further assessment of the implementation of these methods was undertaken in GDA Step 4.

14 Although the PSA model is large, the documentation available for GDA Step 3 had some shortfalls in terms of an auditable trail to the supporting evidence for the claims and arguments in the reports. This evidence trail has been addressed in GDA Step 4 with many of the Technical Queries (TQ) raised during the GDA Step 3 review of the PSA aimed at identifying the information and answers to questions needed for GDA Step 4.

2.3.2 Additional Areas for GDA Step 4 PSA Assessment

15 For the most part the PSA areas, or topics, assessed in GDA Step 4 are broadly the same as those in GDA Step 3, but the level of detail has been more focussed on establishing the evidence supporting the PSA and its results. One area that is new to the GDA Step 4 assessment is Level 3 PSA. In reality Level 3 PSA is concerned with the offsite impact of accidents and has greater relevance in relation to a site specific rather than generic safety case. Nevertheless we have provided a high level assessment of EDF and AREVA's Level 3 PSA submission.

16 As well as the detailed review of all the technical areas of the PSA, during GDA Step 4 ND's PSA assessment team has undertaken a limited Risk Gap Analysis (RGA) (Ref. 10). RGA is an independent analysis of the UK EPR PSA focussing on the potential impact of assessment findings. Its principal function is to help prioritise the Assessment Findings which are actions on a future Nuclear Site Licensee for improvements in the PSA as the project goes from a more detailed design phase through to construction and ultimate operation. The RGA is not intended to produce credible, alternative PSA results, and it is unsuitable for such a purpose.

17 The items for RGA evaluation were identified during the GDA reviews of the individual technical areas in the PSA focussing on the Assessment Findings. A preliminary screening of these items for further RGA evaluation was undertaken based on qualitative judgements and / or existing quantitative information derived from the PSA or other sources such as different data bases.

18 The screened in items were retained for further RGA evaluation, mostly quantitative. In some cases, because of the gaps of information in the current PSA documentation and / or the need to simplify the analysis, RGA quantification was necessarily based on assumptions. For some RGA cases it was not possible to identify a meaningful quantitative evaluation. Where there are insights from the RGA, they are included in the relevant part of Section 4 below.

2.3.3 Use of Technical Support Contractors

19 Technical Support Contractors (TSC) have been used to provide technical advice to ND and this advice has been used to inform the regulatory judgement. In the PSA area TSCs provided support for:

- Level 1 PSA topics – scope, data, accident sequence modelling, systems modelling, hazards analysis, integration of human failure events and quantification. (Refs 11 to 20, Refs 75 and 76).
- Level 2 PSA – modelling of core damage sequences and probabilistic containment response (Ref. 21). Advice on suitability of RiskSpectrum® as a Level 2 PSA code (Ref. 22).
- Level 3 PSA – offsite consequence modelling (Ref. 23).

2.3.4 Cross-cutting Topics

20 A number of topics are by their nature ‘cross-cutting’ (eg PSA, Management of Safety and Quality Assurance) however in addition to these the Assessment Unit Heads have identified the following ‘cross-cutting’ sub-topics:

- Severe Accidents.
- Categorisation and Classification.
- Limits and Conditions and Examination, Maintenance, Inspection and Testing (EMIT).

21 In these three cases advice has been provided to the topic leads for these areas.

2.3.5 Integration with other Assessment Topics

22 The nature of PSA means that there are interactions with other technical areas since aspects of the assessment in those areas constitute inputs to the PSA assessment. For the UK EPR PSA assessment the key inputs were:

- Human Factors: undertook the Human Reliability Analysis (HRA) assessment.
- Fault Studies: provided input to the assessment of the Level 1 PSA success criteria.
- Severe Accident Analysis: provided confirmatory analysis for the Level 2 PSA.
- Control and Instrumentation (C&I): provided input on reliability of protection systems.
- Civil Engineering / External Hazards: provided input to the assessment of the Seismic Margins Assessment regarding definition of earthquake/s magnitude/s and frequency/ies, and fragilities of structures.
- Radiological Protection: undertook the assessment of the Level 3 PSA.
- Structural Integrity: provided an input on large Loss of Coolant Accident (LOCA) frequency.

23 A key, iterative interaction was between PSA and C&I since the PSA assessment of the C&I modelling and related analyses was an input to the C&I assessment. This PSA input was useful in assessing the design changes proposed by EDF and AREVA (Refs 24 and 25) in response to Regulatory Issue RI-UKEPR-002 (Ref. 26).

24 The cases examined in the Severe Accident confirmatory analyses (Ref. 27) were selected taking account of the Level 2 PSA assessment.

25 In addition to the above, there were frequent, informal interactions between PSA and other technical areas, such as Mechanical, Electrical Engineering, Internal Hazards and Chemistry.

26 The PSA was also used as input into Regulatory Observation RO-UKEPR-55 (Ref. 28) on GDA Design Basis Limits and Development of Plant Operating Limits and Maintenance Schedules. The RO response review is reported in the Cross-cutting Topics Assessment Report (Ref. 29). It should be noted that subsequent revision of the PCSR (Ref. 61) has identified that Sub-chapter 18.2 does not include a definitive list of test frequencies. Instead, these have been considered as out of scope items in GDA (see Section 2.3.6).

2.3.6 Out of Scope Items

27 The following items have been agreed with EDF and AREVA as being outside the scope of GDA (Ref. 74).

- Final updates of detailed GDA PSA documentation (in line with the last GDA PSA update) will be performed after GDA (on the grounds that GDA submissions – see Table 1 - provided sufficient information and the Living Status document (Ref. 30) together with the PSA Log book tracks all required changes and commitments for future updates).
- Development of processes to consider PSA insights for any future use of the PSA beyond GDA (see Section 4.19).
- Any requirement on the PSA modelling that needs detailed design information or site specific data beyond the scope of GDA (see Section 4.19).
- Failure Modes and Effects Analysis (FMEA) for initiating event analysis (see Section 4.4).
- Test frequencies of key components (see Section 4.10).

3 EDF AND AREVA'S SAFETY CASE

28 The PSA for the UK EPR is described in Chapter 15 of the PCSR (Ref. 1) and its supporting references. The PSA is noted as a contribution to a key objective ensuring that the risk of release of radioactive products to the environment is reduced to As Low As Reasonably Practicable (ALARP).

29 The PSA has been carried out at Level 1, 2 and 3. The Level 1 PSA considers both internal events (Sub-chapter 15.1) and internal and external hazards (Sub-chapter 15.2) that, together with total or partial failure of protection or mitigation measures, can lead to core damage, and evaluates the resulting Core Damage Frequency (CDF). Other end points that do not result in core damage but may lead to potential releases, including those relating to the spent fuel pool, are included.

30 The Level 1 PSA analysis includes consideration of all non-power operating states and an allowance for plant unavailability due to maintenance is modelled in the PSA.

31 Initiating faults have been derived using the method proposed by the IAEA (Ref. 31) which includes the use of past PSAs, operational feedback data and, for new systems, FMEAs.

32 Event trees are used to model the accident sequence progression and provide estimates of CDF from each initiating event group. In each event tree sequence the safety functions are addressed by "top or function events" which call on specific human actions and fault trees to estimate the failure probability of the frontline and support systems in the specific circumstances for that sequence.

33 Thermal-hydraulic and neutronic parameters, initial conditions, set-points that underpin the success criteria for the top or function events in the sequences are generally based on best-estimate data.

34 The PSA considers random individual component failures, components which fail as a result of the initiating fault, common cause failures (involving both components and signals), pre-fault human errors and human errors occurring during the course of fault sequences (including potential dependencies between separate human activities). The component reliability data used in the PSA has been derived mainly from French and German operational experience. Human Reliability Analysis for Level 1 is largely assumption based and uses the ASEP methodology (Ref. 32) for quantification.

35 Common Cause Failure (CCF) is modelled in the fault trees using Multiple Greek Letter (MGL) parameters derived from the CCF beta factors in the European Utility Requirements (EUR) document (Ref. 33).

36 Control and instrumentation is modelled in the PSA using a compact model. In response to RI-UK EPR-002, EDF and AREVA have provided enhanced design for the UK EPR C&I by inclusion of an additional Non Computerised Safety System (NCSS). The PSA has been completely reworked to include the new system and a new version of the PSA model was submitted during the course of GDA Step 4.

37 Uncertainty analyses using a Monte-Carlo methodology are performed to derive confidence levels for the PSA results. The analyses take into account uncertainties in reliability data and initiating event frequencies by inputting these parameters as probability distributions. The sensitivity of the PSA results to major assumptions and expert judgments is also considered. Overall conclusions of the PSA analysis, including uncertainties, sensitivity analysis are presented in Sub-chapter 15.7 (Ref. 1).

38 The objective of the Level 2 PSA (Sub-chapter 15.4 of Ref. 1) is to assess the response of the containment and its related systems to potential loads and to assess the characteristics of radiological releases from core damage accidents. The Level 2 PSA calculates the probability, composition, magnitude, and timing of fission product releases from the plant and assigns Level 2 fault sequences into Release Categories. The analysis relies on a combination of deterministic and probabilistic considerations.

39 Integration of the Level 1 and Level 2 analyses is carried out by defining Core Damage End States (CDES) with each Level 1 core damage sequence being gathered into the appropriate CDES. The CDES from Level 1 provide the “initiating events” for the Level 2 analysis. The integration of Levels 1 and 2 PSA in this way enables logical information from the Level 1 PSA to be retained and propagated through the Level 2 PSA and avoids the need to define intermediate Plant Damage States.

40 The Level 2 PSA is supported by detailed phenomenological evaluations including: induced Reactor Coolant System (RCS) rupture and Steam Generator Tube Rupture (SGTR), fuel coolant interaction (in and ex vessel), hydrogen generation and ignition, in vessel corium quench, direct containment heating, vessel rocketing and long term containment challenges such as molten core concrete interaction.

41 Further supporting evaluations for Level 2 PSA are included: containment fragility evaluation, HRA (using the SPAR-H method, Ref. 54) and equipment and system survivability.

42 The PSA is physically large, and contains 168 event trees for the Level 1 PSA and a further 128 for the propagation into Level 2 PSA. The PSA quantification for both Level 1 and Level 2 is carried out using RiskSpectrum® Professional software, version 2.10.04. This software suite has been developed by the Swedish company RELCON. It enables the modelling of fault trees to be integrated with the event tree modelling. The code models sequence dependencies automatically.

43 Off-site consequences are analysed by the Level 3 PSA (Sub-chapter 15.5) to determine both individual and societal risk to the public.

44 The Initiating Events analysed in the Level 3 PSA were drawn from three sources; (i) those events modelled in the Level 1 PSA, (ii) those considered in the Design Basis Analysis, and (iii) additional Initiating Events whose consequences would be within the design basis identified by an expert review of the design and operating practices.

45 Individual risk is considered against five dose bands corresponding to those in SAPs numerical Target 8. Analysis of results from the Level 1 and Level 2 PSA and DBA was used to establish representative release types for each band in terms of origin and radiological characteristics of the release. This was done using conservative assumptions to calculate doses in each case in order to assign the dose band.

46 Societal risk is considered by screening the results of the Level 2 PSA to identify those releases likely to result in 100 or more eventual deaths. This screening was based on previous accident consequence assessments of UK power stations. The frequency of each of the releases identified is then summed to yield an overall frequency for comparison with the target

47 PSA results are reported against a number of targets and a range of these are presented in Table 3.

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR PSA

48 The Step 4 PSA assessment has followed the PSA strategy described in Section 2 of this report and has been undertaken with the assistance of Technical Support Contractors who have carried out their work under direction and supervision by ND.

49 For each of the relevant 'assessment expectations' in the tables contained in T/AST/030 (Ref. 8), a view on the adequacy or otherwise of the submitted documentation, including any appropriate TQ and RO responses, has been taken. In cases where limitations and / or potential findings have emerged there has been dialogue with EDF and AREVA in an effort to resolve the problem or identify if further information could be provided within the GDA timeframe.

50 The GDA Step 3 PSA assessment identified a number of areas where the depth of information was simply not visible and / or the reference trail to such information had not been identified in sufficient detail. These shortfalls generally led to the issue of TQs and the responses to these TQs have often been accompanied with new, purpose written reports from EDF and AREVA. These reports are included in Table 1

51 In some limited cases the nature of the shortfall between the PSA and ND's expectations was such that Regulatory Observations (Ref. 34 and Ref. 35) have been issued and these are listed below together with the sub-section number of this report where they are discussed:

- RO-UKEPR-16 – Preventative Maintenance – 4.2, 4.7 &4.11.
- RO-UKEPR-18 – Fire suppression modelling 4.13.
- RO-UKEPR-29 – Inclusion of 2A LOCA - 4.2.
- RO-UKEPR-47 – C&I modelling – 4.7.
- RO-UKEPR-68 – PSA documentation & configuration control - 4.5, 4.6 & 4.7.

52 Details of the assessment and the conclusions and findings are given in Sections 4.1 to 4.19 below and for future convenience the appropriate reference numbers of the T/AST/030 expectations tables are included in the headings.

53 Table 2 provides a brief overall summary of findings in terms of the PSA SAPs, and annex 1 summarises the actual findings that need to be addressed as part of normal regulatory business post GDA.

4.1 Approaches and Methodologies (A1-1.1)

4.1.1 Assessment

54 The PSA approach using linked fault and event trees is the most widely used modern PSA technique and is acceptable in principle.

55 The PSA contains asymmetric assumptions. For example all of the LOCAs are assumed to occur in one of the loops (at a summed frequency covering all loops) to simplify the model. Whilst this will not invalidate high level numerical results, such as Core Damage Frequency, it can lead to distortion of PSA insights for operational purposes and will ultimately need to be addressed so that the PSA provides an appropriate tool to support operation of a potential EPR in the UK. This is not a barrier to GDA confirmation or PCSR acceptance, but it is something that a potential utility would need to address in future licensing stages.

4.1.2 Strengths

- The overall modelling approach is sound.
- PSA modelling software is state of the art.

4.1.3 Findings

> ***Assessment Finding AF-UKEPR-PSA-001:*** *The licensee shall develop the UK EPR PSA into a fully symmetric model.*

4.1.4 Conclusions

- I consider that the approach and methodologies used for the PSA are adequate for GDA. However the PSA will eventually need to be made symmetric in order to support operation of an EPR in the UK.

4.2 PSA Scope (A1-1.2)

4.2.1 Assessment

56 The scope of the PSA includes internal faults, internal hazards, and external hazards. The PSA considers all modes of operation including low power and shutdown and refuelling. The Plant Operating States (POS) are described in the PCSR (15.1) and are summarised below:

- States A and B, the plant is assumed to be at full power (i.e. 4500 MWth), with all systems available, all controls in operation, and the core thermal power being removed via the steam generators.
- State Ca is representative of cold shutdown with the residual heat removal system in operation for reactor cooling. The reactor is pressurised and full of water.
- State Cb is representative of 3/4 loop operation (usually called mid-loop operation), with the reactor pressure vessel head in place.
- State D represents 3/4loop operation with the reactor pressure vessel head removed. As the vessel head is open, the secondary side systems cannot be used for residual heat removal.
- State E is representative of core loading and unloading operations.

57 All sources of radioactivity are included in the PSA documentation. The sources of radioactive releases are:

- the reactor core;
- the spent fuel storage pool;
- the spent fuel handling facilities; and
- the radioactive waste storage tanks.

58 The last three sources are not considered in the Level 1 PSA, which confines itself to “core damage” but are considered in the overall PSA, feeding into Level 2 and 3 which is satisfactory.

59 PCSR Chapter 15.0 states: *“The whole set of internal events is addressed in all PSA levels. Concerning internal hazards, fire, and flooding are addressed in all PSA levels,*

whereas missile and dropped loads are qualitatively analysed. Concerning external hazards only those leading to the loss of ultimate heat sink (LUHS) are effectively addressed in all PSA levels. The other external hazards have not been included due to their low occurrence frequency and consequences." This is acceptable, providing the justification is adequate (see Section 4.13).

60 Section 1.3 of the PSA (Ref. 36) indicates that initiating faults due to intentional mal-operation or sabotage are not considered in the PSA. Also, a malicious event such as an intentional aircraft crash is not considered. This is consistent with ND expectations.

61 PCSR Sub-chapter 15.1 (Ref. 1) indicates that the Level 1 PSA covers all reactor operational modes, from operation at full power to refuelling shutdown with at least one fuel element in the reactor vessel.

62 The risks from internal hazards were not assessed quantitatively (considered negligible) for shutdown states (CA, CB, D and E). It is argued by EDF and AREVA that fire and flooding events would be detected with a higher probability and this together with the longer grace periods will lead to more reliable measures to cope with internal fire or flooding events. Whilst the likelihood of detecting an internal hazard may be higher, it is also likely that activities during shutdown operating states may increase the frequency of internal hazards and there will be more safety equipment unavailable during such states; so higher detection rates can not simply be assumed to provide a more reliable response without doing any supporting analysis. This type of analysis is particularly valuable in informing the procedures to be followed during shutdown states.

63 The GDA Step 3 assessment report noted that EDF and AREVA had included 2A LOCA (large double guillotine failure of primary circuit cooling loops) in response to RO-UKEPR-29. This was a suitable response to the issue and the justification of the initiating event frequency was provided during the course of GDA Step 4 (see comment in Section 4.9.1).

64 Also in GDA Step 3 EDF and AREVA amended the PSA baseline results to include contributions from unavailability due to preventative maintenance in response to RO-UKEPR-16. The way in which such contributions have been included in the PSA model has been assessed in GDA Step 4 (see Section 4.11) and found to be acceptable.

65 The potential contribution to the risk from internal fire and flood during shutdown states was investigated in the Risk Gap Analysis using information from the US EPR PSA (Ref. 37). As expected this revealed only a small potential contribution to the overall risk. This however does not diminish the need to carry out a proper analysis to inform procedures to be followed during shutdown states to keep the risk ALARP.

4.2.2 Strengths

- The overall scope of the PSA includes all modes of operation, all significant sources of radioactivity and includes consideration of internal and external hazards and maintenance activities.

4.2.3 Findings

Assessment Finding AF-UKEPR-PSA-002: *The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.*

4.2.4 Conclusions

- The scope of the PSA is adequate to allow reasonably complete estimates of the risk to be calculated and this is adequate for GDA. However the PSA for shutdown operating states needs to include appropriate consideration of internal hazards to support operation of an EPR in the UK.

4.3 Computer Codes and Inputs (A1-1.4)

4.3.1 Assessment

66 The PSA has been modelled using the RiskSpectrum® linked event and fault tree program. This is one of the leading PSA software suites in the world and is used extensively for existing UK reactor PSAs. During MDEP discussions (see Section 4.20) we received advice from the Finnish nuclear safety authority, STUK, who had encountered some problems regarding Level 2 PSA modelling: a) suitability of using a Level 1 PSA code for Level 2 PSA and b) potential quantification errors. Although the UK EPR PSA was a separate study based on the US EPR analysis rather than on the Okiluoto-3 (OL3) PSA, and therefore thought unlikely to have these problems, work was commissioned from a TSC to examine these points (Ref. 22).

67 In terms of using a Level 1 PSA model, the problem does not really arise as the RiskSpectrum® model has been specifically developed to deal with both Level 1 and Level 2 PSA, and integration of these models is in fact a major strength of the UK EPR PSA. In terms of quantification the concern centred on modelling of mutually exclusive events leading to the same consequence which, if not taken into consideration by the modeller, can underestimate the risk. The UK EPR model was reviewed to identify such events and to examine their significance on the results. This work identified only one instance where there was a potential problem - Release Category 203 for shutdown state C - which could be underestimated by about 20%. This release category contributed less than 0.5% to the large release frequency, so the impact on the results was entirely negligible. The most recent version of the PSA model has been corrected by EDF and AREVA.

68 The deterministic accident progression analysis in the Level 2 PSA is based on calculations performed using the Modular Accident Analysis Program (MAAP) version 4.0.7. (Refs 38 to 40). This is an Electric Power Research Institute (EPRI) code and is the most widely used severe accident progression code by the nuclear industry internationally. It represents many years of severe accident research and has been benchmarked against numerous separate effects tests, actual plant data, other detailed code analysis, and integral experiments. The code deals with accident progression and source term analysis.

69 The implementation of the MAAP4 code within the UK EPR PSA has been assessed during GDA Step 4 (see Section 4.17). Its use is considered appropriate and it has been used correctly by EDF and AREVA.

70 The thermal hydraulic calculations for the PSA success criteria have been performed mainly with the code CATHARE. For Anticipated Transients Without Scram (ATWS) and Steam Line Breaks (SLB) the codes MANTA / SMART / FLICA have been used. The use of these codes has been assessed by ND (Ref. 41) and they are considered satisfactory.

4.3.2 Strengths

- The RiskSpectrum® computer code used for both the Level 1 and Level 2 PSA is acceptable.
- The use of MAAP for deterministic accident progression is adequately supported by a variety of benchmarks with an acknowledgement of any apparent shortcomings.

4.3.3 Findings

- There are no findings in this section.

4.3.4 Conclusions

- My conclusion is that the computer codes selected to support the PSA and used for the PSA modelling itself are adequate.

4.4 Identification and Grouping of Initiating Events (IE) (A1-2.1)

4.4.1 Assessment

71 During GDA Step 3 a more detailed (GDA Step 4 level) review of the Initiating Event analysis was undertaken to identify a full range of initiators. This review involved consideration of the documentation provided in support of the PCSR together with examination of supporting evidence at AREVA's offices. Following this review EDF and AREVA provided a specific submission on IE analysis (Ref. 42) to consolidate the work done on IE derivation and grouping and address questions raised during the GDA Step 3 review.

72 The basis for IE derivation is given in PCSR subchapter 15.1 and describes a systematic and exhaustive search for potential initiating events following the guidance in IAEA-TECDOC-719 (Ref. 31). The process included the following elements:

- engineering evaluation or technical study of plant (see PCSR Chapter 14 'Design Basis Analysis');
- previous PSAs;
- lists of IEs such as NUREG/CR 3862;
- analysis of operating experience for actual plant; and
- FMEA of EPR systems.

73 The guidance in IAEA-TECDOC-719 is consistent with the requirements of T/AST/030 and is acceptable.

74 The GDA Step 3 review noted a difference in the definition of IEs in various parts of the GDA submissions. This has been resolved and the IAEA definition (Ref. 31) is now used consistently and this definition is in line with T/AST/030 expectations.

75 The PCSR together with the specific IE submission (Ref. 42) provides information that:

- Gives clarity on the process used to identify and define IEs leading to a systematic and comprehensive identification of initiating faults.
- Identifies the source documents used and shows the applicability of the information.
- Identifies the applicability of the IEs to each Plant Operating State (POS).

- Considers consequential IEs (such as Steam Generator Tube Rupture, SGTR).
- Identifies characteristics (causes and impact on plant) of each initiating event.
- Shows that each IE group is represented by the most onerous fault.

76 In addition, the assessment has not identified any instances where the definition of IE groups or the grouping process could mask plant vulnerabilities.

77 There are a number of IEs identified related to plant systems (Ref. 42) that are not yet included in the PSA (e.g. Loss of ventilation/room coolers – Heating, Ventilation and Air Conditioning, HVAC) due to lack of design detail. This is inevitable at this stage and these contributions will need to be included, when more information becomes available. This is important because it will also enable insights from the PSA to be considered in the detailed design (see Section 4.19).

78 The impact of the absence of the HVAC in the PSA is discussed further in Section 4.6.

4.4.2 Strengths

- The process for identification of Initiating Events conforms to current PSA standards and practice and is judged adequate to identify the important IEs for the UK EPR design.
- The list of IE groups is reasonable and there is adequate information describing how the IEs were grouped.

4.4.3 Findings

Assessment Finding AF-UKEPR-PSA-003: *The licensee shall provide FMEAs to support derivation of initiating events (out of scope for GDA – see Section 2.3.6).*

Assessment Finding AF-UKEPR-PSA-004: *The licensee shall ensure that those IEs related to plant systems that are not yet included due to lack of design detail are incorporated into the PSA as more information becomes available.*

4.4.4 Conclusions

- The process for establishing the list of IEs and the list itself are judged adequate for GDA, though the FMEAs supporting IE derivation were out of scope. These FMEAs will need to be submitted as part of a site licensing PCSR.

4.5 Accident Sequence Development – Success Criteria (A1-2.2)

4.5.1 Assessment

79 A high level review of ‘Success Criteria’ against the expectations in T/AST/030 (Ref. 8) was conducted during GDA Step 3. This review raised general concerns in the following areas:

- Traceability of the success criteria to the supporting analyses.
- Justification of timing for operator actions.
- Extent of conservatisms in the success criteria analysis for the PSA.

- Limited discussion of the thermal-hydraulic and neutronic analysis performed to support the success criteria development.
- Information provided in the PSA was insufficient to allow identification of the specific analysis supporting each success criteria claim.

80 For the assessment of the UK EPR PSA “Success Criteria” the same event groups have been selected as those selected for the assessment of the event trees reported in Section 4.6. The example Initiating Event Groups are:

- Medium Break Loss of Coolant Accident (MLOCA);
- Internal Fire in the Switchgear Building of the Turbine Island;
- Loss of Ultimate Heat Sink (LUHS);
- ATWS with Loss of Main Feed Water;
- Small Steam Line Break (SLB) with induced Steam Generator Tube Rupture (SGTR) and
- Loss of Cooling Chain during Shutdown State D (LOCC).

81 The above selection provided a good representation of all the types of Initiating Events that can occur in the UK EPR.

82 There had been some concerns with document trails and references in GDA Step 3, so to support the GDA Step 4 assessment EDF and AREVA were requested to develop Route-maps connecting the success criteria in the selected event trees to the specific calculations carried out to justify these, and to provide all the supporting documentation. The Routemaps proved valuable (see below) and the Level 1 PSA detailed documentation will be updated accordingly.

83 The information in the Routemaps helped to establish that for each initiating fault group, the safety functions, the systems which can perform each of the functions, and any need for operator intervention, are identified and the link from the Level 1 PSA report (Ref. 36) to the PSA support studies (Ref. 43) will be formalised when the former is updated.

84 The source and methods used for the derivation of success criteria are presented in a sufficiently clear way in the PSA (Ref. 36) and the PSA support studies (Ref. 43). The primary deficiencies in the cross referencing between success criteria in the main PSA report (Ref. 36) and supporting calculations in the support studies (Ref. 43) were alleviated by the Routemap provided by EDF and AREVA.

85 There were several deviations in success criteria between the documentation and the PSA model. These deviations are only partly traced in the original model logbook (Ref. 44) which was intended to capture the developments between the PSA report and the 2009 version of the PSA model. In general the rationale for the modifications is not transparent. These difficulties were one of the contributory factors in the issue of RO-UKEPR-68.

86 RO-UKEPR-68 noted that the logbook did not contain enough information, or an adequate reference trail, to act as a bridge between the original documentation and the suite of “new” documents supporting the current model and results.

87 In response to the RO, EDF and AREVA provided:

- A “living” status document for the current PSA configuration which includes for each report and file, the title, identification number, version number and date.

- An enhanced Model logbook that had all of the changes with the rationale for each change identified and the reference to the correct report in the status document.
- A PSA Updating Procedure describing the process in place to control model revisions.

88 The response to RO-UKEPR-68 is acceptable and is judged to provide a good basis for the control of future PSA development. The timescale of the RO actions and deliverables was such that the GDA Step 4 assessment of the success criteria and events trees (see Section 4.6) had to proceed in parallel with rather than wait for the RO deliverables

89 The success criteria for each safety function for each initiating fault group are clearly stated and include: minimum equipment requirements and mission times, details of the specific operator actions required, although in several cases the starting point for manual action (i.e. the time at which the operator cue will occur) is missing.

90 The assessment of a representative subset of thermal-hydraulic, neutronics and other supporting analyses showed no significant modelling or numerical errors, although there were some editorial discrepancies.

91 Normally in PSA studies the temperature criterion for core damage is 1200^{o}C for hot rod cladding. To simplify the calculations so that hot rod calculations which depend on factors such as fuel management and burn up are not needed, EDF and AREVA have used an average rod cladding decoupling criterion of 600^{o}C based on an assumed hot rod temperature of 900^{o}C (Ref.43).

92 The justification of the decoupling temperature of 600^{o}C does not explicitly cover all phenomena. However there is a significant margin of 300^{o}C in the calculations and phenomena such as exothermic oxidation are unlikely to challenge that margin. This view is in line with the Fault Studies assessment (Ref. 41) and overall it is judged that the decoupling temperature is adequate for GDA PSA purposes. Nevertheless it is worthwhile confirming, by analysis, that the use of the decoupling criterion is not challenged by phenomena such as Departure from Nucleate Boling (DNB) or exothermic oxidation.

93 Core damage is also assumed to occur if the reactor cooling system pressure is not stabilised, the core remains critical or decay heat removal fails.

94 Section 3.2.3.2 of Ref. 36 states that the validation of success criteria is based on the study of transients using realistic assumptions. The success criteria for partial cool down were, however, based on the success criteria made for the EPR basic design report and the supporting analyses for the Initiating Event ”Loss of coolant chain” are adapted from the support studies for the Final Safety Analysis Report (FSAR) of the Finnish EPR (Okiluoto-3, OL3) (Ref.43) , so may be conservative.

95 The support studies documented in Ref.43 are on a best estimate basis, which is good, but they are performed for OL3. This is acceptable only if the relevant design and operational features embodied in the support studies are incorporated into UK EPR design and operational practices, including Emergency Operating Procedures (EOP). Any departures from this would need to be properly justified.

96 There are explicit calculations for most of the initiating events. For LUHS and SLB there are, however, no explicit calculations but analysis from other Initiating Events has been used in a reasonable and traceable manner, so it is acceptable.

97 Justification of operator actions is said to be contained in HRA-Notebook (Ref. 45) but in some cases the derivation of grace times is not traceable or consistent. For manual start of the Low Head Safety Injection (LHSI), there are different claims on the grace period of

60 minutes in the PSA support studies (Ref. 43) and 120 minutes in the PSA report (Ref. 36) that are not fully justified. As far as numerical estimates go there is only a ~25% difference between the probability of failure calculated for a grace period of 60 mins and that for 120mins and this is not significant in terms of the PSA results. Nevertheless the documentation needs to be made consistent and the grace periods confirmed so that appropriate procedures can be developed.

98 The success criteria for the MLOCA are not properly aligned. The size range for MLOCA is set at 45-100cm^2, but the analysis in the PSA support studies (Ref. 43) is carried out for an 80cm^2 break. It is quite likely that there will be no difference in the success criteria in terms of the required systems responses, nevertheless the analysis should properly bound the group. In addition to providing further evidence on the accident progression and mitigation requirements, EDF and AREVA also provided sensitivity calculations which showed that even if all of the 45-100cm^2 LOCAs were allocated to a higher >100cm^2 LOCA group the impact on CDF would be less than 1%. These calculations are now included in chapter 15.7 of the PCSR (Ref. 1).

99 The thermal hydraulic-analyses are documented in the sense that relevant trend plots are presented and described in an adequate way. The model descriptions and validation reports of the used codes are not part of the PSA assessment and are covered in Ref. 41.

100 For the most part traceability between the success criteria and the underlying analysis is given in the updated Routemap (provided in response to TQs) and the HRA Notebook (Ref. 45). However in the case of ATWS the Routemap is not sufficient because the cited reference (Ref. 46) does not provide any of the required calculations or other derivations. Ultimately a subsidiary reference (Ref. 47) was located which provides the ATWS information. The difficulty in establishing adequate traceability in this case reinforces the need for proper consolidation of the documentation.

101 Following a screening exercise the Risk Gap Analysis for success criteria focussed on three areas:

- Potential mismatch between the thermal power assumed in the OL3 success criteria, 4300MWth and that of 4500MWth quoted for the UK EPR. The impact on CDF was investigated using LUHS as an example and although the impact was small, across a wider range of faults it could be more significant.
- The second area related to the justification of the decoupling criteria. Here the ATWS with loss of main feed faults was used as an example, as the supporting calculations do not consider the unfavourable impact of the potential trip of all the Reactor Coolant Pumps (RCP) on Departure from Nucleate Boling Ratio (DNBR). Here the potential impact was judged to be moderate.
- The system function “containment heat removal” is missing in some event trees. The pressure increase without cooling in the containment is considered acceptable for more than 24h. However, the failure of this function is relevant for long term faults that are not currently included in the UK EPR PSA (see Section 4.15). If all the affected sequences were conservatively assumed to lead to core damage, this would have a moderate impact on the risk.

4.5.2 Strengths

- The success criteria for each safety function for each initiating fault group are stated and include: minimum equipment requirements and mission times, details of the specific operator actions required.
- The assessment of a representative subset of thermal-hydraulic, neutronics and other supporting analyses showed no significant modelling or numerical errors, with only editorial discrepancies.

4.5.3 Findings

Assessment Finding AF-UKEPR-PSA-005: *The licensee shall ensure that all of the success criteria underpinning the UK EPR PSA should be best estimate.*

Assessment Finding AF-UKEPR-PSA-006: *The licensee shall ensure that the design and operational assumptions used in the non UK EPR studies (Ref. 43) are adhered to and confirmed for the UK EPR, or alternatives justified.*

Assessment Finding AF-UKEPR-PSA-007: *The licensee shall provide and implement a procedure to ensure that for Phase 2 of the UK EPR project clear traceability and alignment of the success criteria in the PSA supporting documentation is maintained by adherence to a suitable Living PSA control process (out of scope for GDA - see Section 2.3.6). RO-UKEPR-68 is relevant here.*

Assessment Finding AF-UKEPR-PSA-008: *The licensee shall ensure that the PSA documentation for the UK EPR PSA contains clear and explicit links between the grace periods for human action and the supporting analysis and the timing of cues for those actions.*

Assessment Finding AF-UKEPR-PSA-009: *The licensee shall ensure that in the development of best estimate success criteria noted in AF-UKEPR-PSA-005 all of the relevant phenomena are shown to be bounded, and that the success sequence end points are justified as real successes, not simply time bound because there has been no failure in 24 hr.*

4.5.4 Conclusions

- I have had some concerns with traceability and alignment of the success criteria and have required additional information to be provided during the course of the assessment. I consider that it is important that the PSA supporting documentation is consolidated, properly referenced and traceable within the overall suite of PSA documents (RO-UKEPR-68 is relevant here).
- The underlying analysis supporting the success criteria for the example sequences examined was judged to be adequate, though there are some gaps in the documentation. I do not consider that these documentation gaps have any significant impact on the overall risk calculated for the UK EPR. The difficulty in establishing the sources of information underlines the importance of consolidating the PSA and its supporting documentation.

4.6 Accident Sequence Development – Event Sequence Modelling (A1-2.3)

4.6.1 Assessment

102 My GDA Step 3 assessment for accident sequence development and event sequence modelling was carried out at a general level. For Step 4 assessment I have focussed in more detail on a selection of example event trees in addition to reviewing the responses to the questions raised during GDA Step 3.

103 Seven specific accident sequence analyses (event trees) were selected for detailed review:

- Medium break LOCA (45 and 100cm²) (PBM2_AB).
- Internal Fire in the Turbine Island Switchgear Building (IH F SWGB_AB).
- Loss of Ultimate Heat Sink (LUHS_AB).
- Long Loss of Offsite Power (Long LOOP) (LOOPL-AB).
- Steam Line Break (SLB) with Induced Steam Generator Tube Rupture (SGTR) (SLB_SO_SGTR_AB).
- Anticipated Transient Without Scram (ATWS) flowing a Loss of Feedwater (WS_LMF_A).
- Loss of Cooling Chain during shutdown (LOCC7_D).

104 These accident sequence analyses were selected for detailed review based on one or more of the following considerations:

- Contained sequences which significantly contributed to the overall core damage frequency (CDF).
- Included success criteria chosen for detailed thermal hydraulic review (see Section 4.5).
- Included systems chosen for detailed systems review.
- Contributed to a review of a diverse set of initiator types (i.e. internal event, internal hazard, external hazard).
- Included sequences initiated during shutdown operations.
- Contained classes of sequences found to be important in prior PSAs.
- Included support system initiators.

105 The main discussion of the accident sequence analyses is contained Chapters 4 and 6 of the detailed PSA report (Ref. 36) and Section 5 of PCSR Subchapter 15.1 (Ref. 1). Subchapter 6.3 of Ref. 36 presents the accident sequence analyses for each Initiating Event group. For example, 6.3.1 presents the analysis for the LOCA group. Each subsection within subchapter 6.3 generally describes the IE group characteristics and presents the overall assumption pertaining to the sequence analysis for the IE group.

106 For each specific IE within the group the characteristics of the IE are presented by EDF and AREVA followed by a discussion of the functional response of the plant to the occurrence of the IE. The principal functional safety requirements to prevent core damage and the success criteria (functional and systemic) are presented and discussed. The signals that are generated during the event sequence are presented along with the systems that are automatically actuated. The manual actions that are (or may be) required during the sequence progression are discussed, along with an estimate of the

time period available to perform the action. The inclusion of the event characteristics by EDF and AREVA is in line with ND expectations.

107 The overall modelling approach is judged to be sound and state-of-the-art PSA modelling software (RiskSpectrum®) has been used for the analysis. The accident sequence (event tree) analysis appears to be comprehensive. For each initiating event (fault) group, the safety functions, the systems which can perform each of the functions, and any need for operator intervention, are provided in the success criteria table associated with each IE group contained in the accident sequence quantification section (e.g. see Table 6.3.1-1 in Ref. 36).

108 The general assumptions relating to all event tree development are identified. Additional more detailed assumptions are provided for individual initiators.

109 As noted in Section 4.5, EDF and AREVA had provided route maps for the selected sequences connecting the success criteria in the selected event trees with specific calculations. Nevertheless the detailed assessment of the event trees was complicated by the main PSA documentation (Ref. 36) not being aligned with the PSA model. For example the main PSA reference (Ref. 36) does not refer to the thermal hydraulic analyses (Ref. 43) that support the model and does not identify which analyses support which event trees. The PCSR chapters in Issue 2 do not do this either.

110 Furthermore the log book of model updates and changes provided with the model was not sufficiently detailed to act as a bridge between the main PSA reference (Ref. 36) and the PCSR and the PSA model. There were no other reports or status documents which provided the links and reference or evidence trail between major document updates.

111 In dialogue with EDF and AREVA it was clear that they had all of this information, but it was not systematically documented within the GDA submissions in a way that was visible to us or other prospective UK users of the PSA.

112 Similar difficulties were emerging regarding the assessment of systems (see Section 4.7) and success criteria (see Section 4.5) and as a consequence RO-UKEPR-68 was issued. The response to RO-UKEPR-68 is discussed in Section 4.5.

113 EDF and AREVA's response to RO-UKEPR-68 (see Section 4.5) is acceptable and is judged to provide a good basis for the control of future PSA development. The timescale of the RO actions and deliverables was such that the GDA Step 4 assessment of the events trees and success criteria (see Section 4.5) had to proceed in parallel rather than wait for the RO deliverables.

114 The Initiating Event analysis assessment in Section 4.4 noted, amongst other things, that the failure of HVAC was not included in the PSA. Similarly during the accident sequence assessment EDF and AREVA confirmed that loss of HVAC during other accident sequences was also not included (for the same reasons as in 4.4). EDF and AREVA have provided some indication of the potential impact of inclusion of HVAC based on the French EPR, Flamanville 3 study of up to a 6% increase in the CDF.

115 Additionally, the compressed air system is not yet included in the PSA model. Further development of the support systems modelling will be needed as more detailed design information becomes available (see Sections 4.4 and 4.19).

116 During the assessment questions were raised on the potential multiple demands made on safety valves. EDF and AREVA confirmed that the PSA support studies (Ref. 43) had multiple opening and closing of such valves, but that the reliability data used in the model did not cover this. EDF and AREVA also pointed to there being significant conservatism (up to a factor of 100) in the model data compared to more recent analysis of French and

German operating experience indicating no negative impact on the overall PSA results from multiple demands. Although this is encouraging, in terms of the results, the PSA should properly model the demands on the valves and use the realistic data described by EDF and AREVA.

117 A high level comparison of the event tree modelling and success criteria between the UK EPR PSA and US EPR PSA for all the events selected for detail review has been carried out during GDA Step 4. This review indicates that there are differences in the assumed mitigation measures, event sequence progression and success criteria between the two analyses. The existence of these differences, of course, does not mean either analysis is wrong, only that different assumptions and strategies have been used and EDF and AREVA were able to explain the differences. Further collaborative international EPR PSA comparison work from a Regulators' perspective is planned, (see Section 4.20) and findings from this work will inform any future regulatory assessment of the EPR in the UK.

118 The omission of HVAC has been considered in the Risk Gap Analysis, noting that EDF and AREVA's estimate base on Flamanville 3 indicates a small impact. The US EPR study indicates a strong influence on the risk from the HVAC and depending on the assumptions used on "room heat up" the risk impact could be moderate. The room heat up assumptions are dependent on ambient conditions, and the US assumptions may be overly harsh for a UK environment. Again depending on assumptions made, the US study indicates a high importance for operator recovery of HVAC.

4.6.2 Strengths

- Overall modelling approach is sound.
- Accident sequence (event tree) analysis appears to be comprehensive and we have not identified anything that casts doubt on the ability of the event trees to calculate sequence failure probabilities correctly.
- General assumptions relating to all event tree development are identified.
- The response to RO-UKEPR-68 provides a good basis for the control of future PSA development.

4.6.3 Findings

Assessment Finding AF-UKEPR-PSA-010: *The licensee shall ensure that the detailed Level 1 PSA document (Ref. 36) (out of scope for GDA – see Section 2.3.6) is updated so that it is fully consistent with the current PSA model (Ref. 71).*

Assessment Finding AF-UKEPR-PSA-011: *The licensee shall ensure that the process for maintaining and developing the PSA model configuration and supporting document trail (see RO-UKEPR-68 discussion) is retained post GDA, or an equivalent process put in its place. (Out of scope for GDA – see Section 2.3.6)*

Assessment Finding AF-UKEPR-PSA-012: *The licensee shall ensure that all the support systems (e.g. HVAC) are incorporated into the PSA, both as potential initiators (see 4.4) and their role during accident sequences. The role of the operator in HVAC recovery should be examined closely.*

Assessment Finding AF-UKEPR-PSA-013: *The licensee shall ensure that future development of the PSA properly accounts for multiple demands on safety valves and should make use of current best estimate reliability data.*

> ***Assessment Finding AF-UKEPR-PSA-014:*** *The licensee shall provide and implement a consistent process to ensure capture of the assumptions that are currently dispersed throughout the PSA reports and its supporting documentation and gather them together in a single place within the PSA documents. This should be done in a systematic and traceable way, and the assumptions sentenced as part of a future PSA development (out of scope for GDA – see Section 2.3.6).*

4.6.4 Conclusions

- The event tree sequence modelling in the UK EPR PSA is adequate for GDA.
- Adherence to the PSA configuration and documentation control measures now in place for the UK EPR, or equivalents, should assist future PSA development and assessment of that development.
- The example differences between the UK EPR and US EPR were satisfactorily explained by EDF and AREVA. Collaborative international EPR PSA comparison work will be helpful for future regulatory assessment of the EPR in the UK.
- There is no apparent process to capture PSA assumptions that need to be reconciled with future operation or design development. This is a common theme in a number of PSA topic areas, and RO-UKEPR-68 process helps but does not deal with it entirely. PSA assumptions should be documented and captured in a systematic and traceable way, and ultimately all assumptions will need to be sentenced as part of a future PSA development and utilisation

4.7 System Analysis (A1-2.4)

4.7.1 Assessment

119 The UK EPR systems performing safety functions are modelled in the PSA by fault trees which are called upon, as needed, by the event trees for each fault group within the overall RiskSpectrum® model. A notable exception to this is the C&I which is represented by specific implementations of the “compact model” included in the individual system fault trees. Assessment of the PSA modelling of C&I is reported in Sub-section 4.7.5 below, and the current subsection concentrates on the other systems.

120 During the GDA Step 3 PSA assessment there were general systems analysis findings that led to the issue of a number of TQs. In addition to assessing the responses to these TQs, my GDA Step 4 assessment has focussed in more detail on the fault tree analysis of example systems.

121 A sample comprising five systems was selected to be reviewed in detail: Essential Service Water System (ESWS), Component Cooling Water System (CCWS), Electrical Power System (EPS), Safety Injection and Residual Heat Removal System (SIS), and Emergency Feedwater System (EFWS). These systems were selected as they represent potentially important frontline and support systems.

122 Each system analysis appendix contains the system description, system boundaries, system interfaces, system dependencies, connected systems, operational restrictions, testing and maintenance, description of the fault trees, definition of the safety function, tables of top events, tables of success criteria, assumptions, limitations, common cause failures, component data, human failure events, and house events.

123 My GDA Step 4 review revisited general expectations for the five selected systems and in many cases there were no additional comments. However the example system analysis

appendices did not provide specific information regarding component failure modes contributing to system failure. The missing component failure mode descriptions are primarily a documentation issue and it is true that a comprehensive list of basic events, including failure modes, and intermediate events (i.e. gates) is included in the PSA model in an easily accessible form.

124 For the EPS, CCWS, ESWS, EFWS, and SIS systems, the level of detail in the fault trees was generally acceptable in terms of realism, treatment of dependencies, and data. However, the correctness of the fault trees was difficult to judge due to apparent inconsistencies between the PSA model and the system analysis appendices which often required written or oral explanations from EDF and AREVA to resolve. This issue is a documentation issue since the inconsistencies are due to the update of the model while the documentation had not been fully updated.

125 The descriptions of the systems and their corresponding operation modes, normal configuration, configuration(s) following reactor trip, and configuration for non-power states are considered to be acceptable for each of the five systems.

126 Based on the system boundaries, which can be inferred from the system diagrams, no gaps or overlaps were identified for the ESWS, CCW, SIS, and EFWS systems. For the electrical power system, the inclusion of diesel generators and their support equipment was not clear initially, but the data report (Ref. 48) and TQ responses satisfactorily addressed these points.

127 The system analysis appendices provide tables for system success criteria under differing conditions, as defined by different top events, which are generally consistent with the success criteria tables in Section 6.3 of the PSA (Ref. 36). All of the inconsistencies noted were due to the PSA model update and were addressed through TQ responses.

128 The five detailed systems are treated very similarly regarding testing and maintenance activities in the system appendices (Ref. 36), but these are not up to date due to the fact that the model and PCSR were changed in response to RO-UKEPR-16 (see Section 4.11). Other than the need for consistent documentation we have no testing and maintenance issues as modelled in the UK EPR PSA.

129 Fault tree modelling assumptions for each specific system are described in Section 2.2 of each system analysis appendix. The assumptions are generally well described, but a few of the assumptions required additional support from TQ responses.

130 The ESWS, CCW, EPS, SIS, and EFWS system analysis appendices provide adequate explanation of the fault tree logic to facilitate a general understanding, although this will improve considerably when the documentation is consolidated (this will include relevant TQ responses being incorporated) to be aligned with the PSA model.

131 Each system analysis appendix discusses common cause failure events and all of the example systems reviewed in GDA Step 4 conform to the general approach used for the analysis of common cause failures in this PSA.

132 Construction of the fault tree logic in the PSA model appears generally adequate, and we have found no actual errors, although it was noted that failure of the In-containment Refuelling Water Storage Tank (IRWST) was not included in the SIS fault tree.

133 A number of the points that have arisen during the GDA Step 4 fault tree analysis assessment have been PSA documentation and configuration matters rather than technical problems with the modelling. The assessment of the accident sequence analysis (event trees) reported in Section 4.6 was similarly affected, leading to the issue of RO-UKEPR-68.

134 EDF and AREVA’s positive response to RO-UKEPR-68 (see Section 4.5) provides confidence in the modelling and the way in which changes are controlled.

135 The RGA for this particular area has indicated that non inclusion of the IRWST failure has a low potential impact on the risks.

4.7.2 Strengths

- Construction of the fault tree logic in the PSA model appears adequate, and we have found no actual errors.
- System descriptions are comprehensive.
- The descriptive text for fault tree gates and basic events is clear and consistent.
- The general approach to the inclusion of pre-initiator human failure events appears to be comprehensive.
- CCF has been included in a consistent manner.

4.7.3 Findings

Assessment Finding AF-UKEPR-PSA-010: *The licensee shall ensure that the detailed Level 1 PSA document (Ref. 36) (out of scope for GDA – see Section 2.3.6) is updated so that it is fully consistent with the current PSA model (Ref. 71).*

Assessment Finding AF-UKEPR-PSA-011: *The licensee shall ensure that the process for maintaining and developing the PSA model configuration and supporting document trail (see RO-UKEPR-68 discussion) is retained post GDA, or an equivalent process put in its place (out of scope for GDA – see Section 2.3.6).*

4.7.4 Conclusions

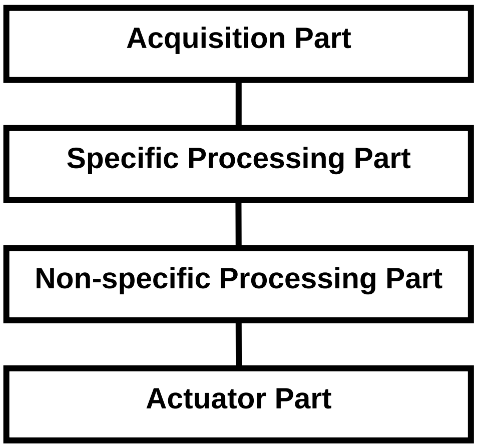
- The inconsistency between the model and documentation (mainly Ref. 36) resulted in a number of queries being raised during my assessment work which required an iterative process to resolve. Nevertheless, I consider that the system fault trees included in the PSA model provide an adequate representation of the systems performing the required safety functions for the range of initiating events included in the PSA.

4.7.5 Control and Instrumentation (C&I)

4.7.5.1 Assessment

136 In Step 3 PSA support was given to the C&I assessment. This support was mainly focussed on a review of sensitivity studies that explored the potential risk impact of different levels of numerical reliability and independence of the C&I. In addition to these considerations, an assessment of the way in which C&I is modelled within the UK EPR PSA has also been undertaken in Step 4.

137 C&I is included using the compact model, shown below:



138 The compact model is described in the PCSR (15.1.3.4) but the description was high level and there were a number of assumptions and inputs to the compact model that were not covered in the PCSR text or the supporting documentation available during GDA Step 3. Consequently, RO-UKEPR-47 was raised to address these points.

139 It should be noted that EDF and AREVA had already given a commitment to change the C&I architecture in response to RI-UKEPR-002, via design changes CMF 14 (Ref. 24) and CMF 15 (Ref. 25). RO-UKEPR-47 required that not only should the PSA be updated to reflect those changes, but that the update should take account of other PSA related concerns on the modelling of C&I listed in the RO.

140 These PSA related concerns included:

- Base event descriptions in the RiskSpectrum® listing were not unique to individual base events.
- Some base events seemed to be undefined composite or module events and the contributions to these base events were not explicitly identified.
- There was no evidence that support systems for instrumentation had been considered.
- There was no justification for any of the numerical values for the instrumentation reliabilities quoted.
- The internal architecture (of acquisition part) was not described, or referenced.
- General, un-quantified claims seemed to be being made on operator recovery.

141 The work carried out by EDF and AREVA to address RI-UKEPR-002 including C&I design changes is reported in ND’s Step 4 C&I report (Ref. 49) and Cross-cutting topics report (Ref. 29). In support of this work EDF and AREVA have updated the PSA model to include additional engineering in the form of a Non Computerised Safety System (NCSS), designed to provide diverse back up to the computer based protection systems already in place. In this particular revision of the PSA, EDF and AREVA also included changes to address RO-UKEPR-47 and provided additional documentation (Refs 50 and 51) to support the PSA model. The changes to the model and documentation have been undertaken and recorded in line with the processes agreed in response to RO-UKEPR-68 (see Section 4.5).

142 The detailed changes to the logic model to include the NCSS in the PSA have been assessed and are considered to provide an appropriate representation of the protection systems such that the PSA results will reflect the correct residual failure combinations. Care has also been taken by EDF and AREVA to discriminate between those sequences in which operator actions are claimed to support the computer based C&I and those actions to support the NCSS.

143 The PSA results quoted in Section 3 include the NCSS contribution at 10^{-3} failures per demand (f/d) and numerical failure probabilities for the computerised protection that are in accordance with the requirements of international C&I standards such as those from the IAEA and IEC. These results are lower than the Basic Safety Objectives (BSO) for SAPs Targets 8 and 9 of NT1.

144 During the assessment of the incorporation of the NCSS into the PSA, the potential for dependencies between a C&I Initiating Event and the subsequent role of the C&I in the safety systems mitigating the fault was discussed. EDF and AREVA considered that this was most likely to be seen in the reactor trip fault and provided information indicating that there have been no spurious reactor trips due to computerised C&I failure. EDF and AREVA acknowledged the need to pursue this point in more detail as the design develops.

145 The response to RO-UKEPR-47 (Ref. 52) comprised a detailed consideration of each point, together with a specific supporting document (Ref. 50) which links to the PSA justification of the NCSS (Ref. 51). The changes to the PSA and the provision of new supporting documentation adequately address the majority of the points in the RO, though the supporting document (Ref. 50) acknowledges that the actuators are not modelled in the current PSA, but does accept that they need to be included when details of the design are developed.

146 Although I have not identified any specific weaknesses in the use of the compact model, it is not clear at this stage that it will prove flexible enough to support configuration control during operation.

147 EDF and AREVA were also asked if they could interrogate the PSA results to establish if there were situations in which a claim of better than 10^{-3} f/d for the C&I was required to meet the probabilistic targets where the Protection System (PS) was relying on a single parameter. This is a difficult task and instead of laborious searches through the cutset lists or development of post processing routines, EDF and AREVA elected to carry out a specific sensitivity study using the most up to date version of the PSA model (NCSS incorporated) as a baseline.

148 The sensitivity study was carried out by adding additional base events for the parameters in each compact model fault tree using that parameter, with a value of 10^{-3} f/d. This means that no situation will exist where a claim of better than 10^{-3} f/d is made where there is a single parameter. The results of this study are in line with the BSOs for SAPs Target 8 dose band 5 and SAPs Target 9.

149 The Risk Gap Analysis for the C&I modelling in the PSA has focussed on the potential for dependencies between C&I based initiating events and subsequent demands on the C&I in the accident sequences. Based on conservative assumptions in which the common logic parts of the compact model are set to failed, a moderate impact on the risk would be expected. The reliability values used for the instrumentation were also considered in the Risk Gap Analysis and in this instance there was only a small impact.

4.7.5.2 Strengths

- The C&I modelling in the PSA is clear and the compact model provides an adequate representation for the purposes of estimating numerical risks and gaining insights into the importance of the elements of the C&I.
- The design change to include the NCSS has been incorporated into the PSA model in an appropriate manner.

4.7.5.3 Findings

Assessment Finding AF-UKEPR-PSA-015: *The licensee shall ensure that the modelling of the C&I in the PSA is reviewed and if necessary amended as the details of the C&I systems evolve. This should include explicit consideration of C&I based Initiating Events (including spurious signals) and the potential dependencies between such initiators and the safety mitigation systems and potential dependencies between the cues for operator action and signals used for the automatic C&I.*

Assessment Finding AF-UKEPR-PSA-016: *The licensee shall ensure that future updates of the model explicitly include the actuators associated with the compact model, and also take account of any CCF related to the actuators.*

4.7.5.4 Conclusions

- The modelling of C&I in the UK EPR PSA, including the NCSS added as a design change in response to RI-UK EPR-002, is judged to be adequate for GDA, though it is recognised that there will be further development of C&I that will need to be incorporated into the PSA during post GDA phases.

4.8 Human Reliability Analysis (A1-2.5)

4.8.1 Assessment

150 ND’s assessment of the Human Reliability Analysis (HRA) is reported in the Human Factors assessment report (Ref. 53) so only a brief mention is made here. In essence the HRA is largely assumption based since there is a lack of task analysis, written procedures and detailed information on operating practices available for GDA.

151 The methodologies selected by EDF and AREVA are well known, they use ASEP (Ref. 32) for the Level 1 PSA and SPAR-H (Ref. 54) for the Level 2 PSA.

152 The HRA methods used require knowledge of when a cue for action would happen and time period within which the correct implementation of the action would be successful. These times are derived from the PSA support studies (Ref. 43) discussed in Section 4.5 of this assessment report. We have not identified any significant discrepancies in the timings though we have noted lack of justification in the differences found in the documentation, as noted in Section 4.5 for manual start of the Low Head Safety Injection (LHSI).

153 The numerical values calculated for use in the Level 1 PSA do not give cause for concern and are broadly conservative. Post fault Human Failure Events (HFE) seem to be modelled in the appropriate places in the fault and event trees (we have not identified any problems) but there is only limited discussion of the placement of HFEs particularly when they are modelled at the event tree level.

154 The inclusion of pre-initiating events HFEs is, however, incomplete. Calibration errors are assumed to be included in the failure data for the instrumentation. Only misalignment of manual valves is considered explicitly, motor operated and solenoid valves, automatically realigned on a system demand and manoeuvrable from the MCR are not considered.

155 For the Level 2 PSA, the Human Error Probabilities (HEP) for the Emergency Operating Procedure (EOP) actions, i.e. those that are taken by the operators at transition to the UK EPR severe accident guidance (OSSA) (Ref.72) but still under the guidance of the EOPs, are evaluated using the SPAR-H approach, which is different from the approach used for the Level 1 PSA HEPs. This introduces an inconsistency into the analysis. The significance of this inconsistency is not clear, though it is unlikely to affect the results for Large Early Release Frequency (LERF) and Large Release Frequency (LRF) significantly. Indeed EDF and AREVA’s report on key claims on operator reliability in the UK EPR PSA Level 2 (Ref. 55) indicates that the most important operator actions in respect of LRF or LERF are actually Level 1 actions, with the Level 2 action being much less significant.

156 Nevertheless, the SPAR-H model is being used outside of the context for which it was developed, which was for control room crew responses and the HEPs calculated in this way may be optimistic when compared to the values that would be calculated using the Level 1 PSA HRA method.

157 The Risk Gap Analysis for HRA has concentrated on the potential significance of dependencies between HFEs causing initiating events and those modelled in the response to such faults. A bounding sensitivity study to address potential dependencies between boron dilution initiating event and the recovery factor showed that the impact on the risk was small in this instance. However further work on human caused Initiating Events ought to pay attention to this type of dependency to minimise the impact on the risk.

4.8.2 Strengths

- All significant post fault HFEs have been identified and correctly modelled in the appropriate parts of the PSA.
- The numerical probabilities calculated for the post fault HFEs provide an adequate basis for risk estimates within GDA.

4.8.3 Findings

Assessment Finding AF-UKEPR-PSA-017: *The licensee shall ensure that substantiation for the HRA in the form of task analysis, procedures and training is provided to underpin the numerical HFE values used in the PSA. The substantiation should include further consideration of pre-initiating HFEs and the potential for HFE dependencies (pre & post fault).*

Assessment Finding AF-UKEPR-PSA-018: *The licensee shall ensure that Level 2 PSA sensitivities to individual and collective HEPs are used to provide insights into the development of the UK EPR severe accident guidance (OSSA).*

4.8.4 Conclusions

- The HRA in the UK EPR PSA is largely assumption based, with no underlying substantiation. The numerical probabilities used in the PSA are, however, judged adequate for purposes of risk estimates within GDA.
- The PSA will need to be updated in line with future analysis and substantiation of HFEs during later, post GDA, phases.

4.9 Initiating Event Frequencies (A1-2.6.1)

4.9.1 Assessment

158 The quantification of Initiating Events is reported in Chapter 15.1.4 of the PCSR which indicates the following process for evaluation of the frequencies of IEs:

- French or international operational experience feedback.
- Calculations of the failure probability of specific equipment using the component reliability database (Ref. 56).

159 The quantification method depends on the Initiating Event group.

- For frequent Initiating Events (i.e. those observed at least once in French plants), the operational experience of the 1300MWe Pressurised Water Reactor (PWR) series is preferred, possibly augmented on a case by case basis by operational experience from French 900MW stations.
- For Initiating Events not observed in French or international operational experience, the frequency is said to be generally assessed using expert judgement, although in practice no Initiating Event frequency other than RPV failure has been estimated in this way.
- For the Initiating Events resulting from component failure, the frequency is calculated from reliability data on the relevant component.

160 The majority of the data for similar plant designs has come from the French 1300 MW PWRs or the 900 MW PWRs.

161 LOCA frequencies were generally taken from NUREG/CR-6928 (February 2007). For large break LOCA, EDF and AREVA use a smaller break size cut-off than in NUREG/CR-6928 (6” rather than 7”) and since smaller pipes tend to have a larger frequency, it would indicate they ought to use a slightly higher frequency. This is only a very minor point given the low frequencies involved. There are similar issues with the medium LOCA frequencies but again these are not considered important.

162 Table 4 of Chapter 15.1.4 of the PCSR indicates that the IE frequencies for small break LOCAs for shutdown states CA, CB, D and E were taken from NUREG/CR-6928 even though this NUREG does not cover low power and shutdown IEs. The use of these values is, however, expected to be conservative since failure at low pressure will be less likely than at higher pressure.

163 The frequency of the 2A LOCA was estimated in line with paragraph 244 of the SAPs and judged to be reasonable by ND Structural Integrity assessors (Ref. 57).

164 Two of the IE frequencies (e.g. Loss of Condenser Vacuum and Loss of Offsite Power LOOP) are derived from the 1995 European Utility Requirements for Light Water Reactor (LWR) Nuclear Power Plants Document (Appendix 2.17A). These quantitative IE frequencies have been removed from the current (2001) version of the EUR document

which recommends use of a national database for IE frequencies. The loss of condenser event frequency in the EUR is conservative with respect to other databases (e.g. NUREG/CR-6928) and is claimed to be consistent with French operating experience, hence its use is adequate for GDA.

165 For LOOP the UK EPR project team intended to use a UK National Grid Company generic document to support the UK EPR LOOP frequency claim but was not able to reference this document as the analysis of LOOP frequency for existing UK plants was not considered by the National Grid Company to be necessarily representative of a future UK EPR grid connection scheme. Therefore the EUR data was used as an alternative, conservative approach for the LOOP frequency. Note that the possibility of house load operation is neglected for the UK EPR analysis, which adds further to the conservatism of the assumed frequency values.

166 The data set used for the ratio of short / long conditional LOOP, based on NUREG/CR-6890 in the current PSA, is much smaller (and thus more uncertain) than the data set used to determine the ratio of short / long IE LOOP. The conditional LOOP ratio is however conservative compared to the IE ratio.

167 For those situations where fault trees are identified as being the source for the IE frequency (see Table 4 of Chapter 15.1.4 of the PCSR), details have been provided via TQ responses which will be included in the next update to the detailed PSA (Ref. 36). The information provided is judged adequate.

168 The RGA for this particular area has confirmed the overall conservative nature of the treatment of the short / long conditional LOOP frequencies. Although conservative, the difference in short / long ratios for conditional LOOPs versus IEs should be corrected or justified in the future.

4.9.2 Strengths

- The derivation of Initiating Event frequencies is generally sound and clearly set out in the documentation.
- The use of a consolidated analysis for initiating faults and the derivation of their frequencies minimises the likelihood of errors.

4.9.3 Findings

Assessment Finding AF-UKEPR-PSA-019*: The licensee shall ensure that the generic LOOP frequency is confirmed to be bounding in comparison to a site specific value or demonstrate that a site specific frequency is acceptable in risk terms.*

Assessment Finding AF-UKEPR-PSA-020*: The licensee shall ensure that the PSA uses an appropriate LOOP frequency for the site and justified ratios used for long and short duration LOOP, both in terms of initiating event and conditional LOOP.*

4.9.4 Conclusions

- The use of the superseded EUR for UK LOOP is not ideal, however its use is limited and the impact on the PSA is conservative. Overall I consider that the IE frequencies developed for the UK EPR PSA are adequate for GDA.

4.10 Component Failure Rates (A1-2.6.2)

4.10.1 Assessment

169 The GDA Step 3 assessment identified a number of shortfalls in the documentation supporting the component failure rates used in the PSA. These shortfalls have been addressed by EDF and AREVA in their component data report (Ref. 56). This report provides comprehensive coverage of the data sources used and appropriate justification for use of each source. In general preference has been given to data derived from EDF operational experience.

170 The Step 4 assessment involved not only consideration of the documentation provided in support of the PCSR, but also examination of details of the methodology used and supporting evidence at EDF's offices.

171 For standby components EDF uses Q = α + λsTs/2 + λrTm

172 Where Q is overall failure probability, α is the demand failure probability (stress), λs is the time related failure rate between tests, Ts is the test interval. For components that need to start and run, λr is the failure to run rate and Tm the mission time.

173 EDF does not distinguish failures due to stress (α) from latent failures (λsTs/2), instead a parameter γ is used in EDF PSA, where γ= (α + λsTs/2) and is calculated from operating feedback as n/N where n is the number of failure events and N the number of demands. This is contrary to typical UK practice where it is generally assumed α is zero thus explicitly crediting the maximum benefit to the impact of test frequency on the failure probability. The idea behind this is that the maximum impact of changes to test intervals can be investigated using the PSA. In practice EDF have also used this assumption (Ref. 58) for such investigations.

174 EDF's test intervals are based on current practice and manufacturers recommendations and are implicitly taken into account in the operating feedback when γ is derived. It is accepted that the test intervals are implicitly included in the numerical values.

175 For the GDA PSA results it does not actually matter if the failure probabilities are directly entered into RiskSpectrum® or are calculated by the programme from equivalent λs and Ts. Ultimately the PSA is expected to be developed into a flexible operational tool and for a utility to show they have optimised the test intervals so that the risk is ALARP by explicitly using them (λs and Ts) in the RiskSpectrum® model. This is a relatively simple change to implement.

176 The actual test intervals underpinning the component failure probabilities based on EDF operating experience are out of scope for GDA (see Sections 2.3.5 and 2.3.6).

177 For component failure probabilities the Risk Gap Analysis has compared the values used for the most important components with those in NUREG/CR-6928. In all cases the values chosen by EDF and AREVA are similar or more conservative than the comparison set.

4.10.2 Strengths

- Much of the component failure data has been derived from EDF operational experience and the failure probabilities derived from this operating experience provide acceptable figures for use in the GDA PSA.

- The generic data sources used when there is no suitable operational experience data are adequately justified.
- The component boundaries for the database are clear and have been shown to match with those used in the PSA.
- A complete list of base events is included in the PSA model submitted with the documentation.

4.10.3 Findings

Assessment Finding AF-UKEPR-PSA-021: *The licensee shall ensure that the test intervals underpinning EDF derived component failure probabilities (out of scope for GDA – see Section 2.3.6) are provided consistently with EMIT programmes or alternatives justified.*

Assessment Finding AF-UKEPR-PSA-022: *The licensee shall ensure that the implicit rather than explicit inclusion of test intervals (Ts) are revisited for the data inputs to the Operational PSA post GDA.*

4.10.4 Conclusions

- The extensive use of direct operating experience to estimate component failure probabilities is welcome and the values used are adequate for GDA purposes. More explicit use of test interval data will almost certainly be needed to support future operation of an EPR in the UK. ND normally expects the data to be included in the PSA in terms of λs and Ts.

4.11 Unavailability Due to Test and Maintenance (A1-2.6.3)

4.11.1 Assessment

178 The GDA Step 3 PSA assessment report described RO-UKEPR-16 which was aimed at having maintenance unavailability included in the baseline PSA rather than as a sensitivity study. This arose because the SAPs require numerical PSA results that reflect all potential states, including maintenance outages, for comparison with the numerical targets. EDF and AREVA readily revised the PCSR and the results quoted within it to comply with the RO.

179 In GDA Step 4 further consideration has been given to the way in which the maintenance outages were included.

180 The maintenance scenario modelled in the PSA identifies a number of maintenance groups, for example group A is simultaneous maintenance lasting 28 days on one train of the ESWS, CCWS and the SIS/RHR. There is, however, no source quoted for the maintenance periods assumed in the PSA or link with EMIT requirements assessed in the Cross-cutting Topics report (Ref. 29).

181 Base events for maintenance are included in the PSA model and are included under the same OR gate as, for example, failure to run the pump for a fluid system with pumps, or failure to run the diesel for the emergency diesel generator system, thus ensuring that “maintenance” will be modelled as unavailable and will not contribute to success of the safety function. This is acceptable. In addition to looking at the average contribution of maintenance unavailability, the PCSR also reports on the “instantaneous” risk associated with each of the assumed maintenance groups and the results indicate relatively modest

(approximately a factor of 2) increases during those time periods, which satisfies the intent of SAPs NT2 in respect of test and maintenance unavailability.

4.11.2 Strengths

- Unavailability due to maintenance / test has been modelled in the PSA in the appropriate fault trees and allows for coincidence of some maintenance activities.

4.11.3 Findings

> ***Assessment Finding AF-UKEPR-PSA-023:*** *The licensee shall ensure that the basis for the time periods assumed for maintenance and test unavailabilities is justified and that those time periods, together with the "allowable" maintenance combinations assumed in the PSA are incorporated into the Technical Specifications and EMIT programmes, or alternative values / strategies justified.*

4.11.4 Conclusions

- Unavailability due to maintenance / test has been adequately modelled in the PSA.
- The instantaneous risk associated with maintenance outages satisfies SAPs NT 2.

4.12 Common Cause Failure (A1-2.6.4)

4.12.1 Assessment

182 Common Cause Failure (CCF) methodology is based on an extended beta factor method and data taken from a superseded EUR document (Ref. 33) although it is converted to a Multiple Greek Letter (MGL) method for use in RiskSpectrum®. The MGL formulation is an accepted PSA method.

183 As part of this Step 4 assessment, the conversion of the EUR beta factors into MGL parameters has been checked and found to be mathematically correct. In addition an assessment of the implementation of CCF modelling of each of the system fault tree analyses reviewed in Section 4.7 above shows correct implementation of the model.

184 The derived MGL parameter estimates are applied to all CCF groups irrespective of the component type constituting the group or for specific component failure modes. Hence, the CCF model for all component types and failure modes use the same parameter values. Consideration of responses to TQs raised during GDA Step 3 on this point established that the use of the global, generic parameters is sufficient to highlight significant CCF events and that in comparison with other CCF databases that do contain component and system specific parameters, such as US NRC's (Ref. 59), the values used in the UK EPR PSA are conservative. Hence the use of global CCF parameters does not undermine the GDA PSA results or the significance of CCF within those results. Component-type specific and failure mode specific parameter estimates are likely to enable a more discriminating analysis of the CCF contribution to the risk which could have implications for potential future operation of the plant.

185 Section 5.3.2.4 of the main PSA reference (Ref. 36) indicated that several specific Common Cause Failure probabilities were based on direct expert judgment without the expert judgement process being described or any indication of the uncertainties associated with that process. Further investigation (TQs) revealed only two potential expert judgement cases: mechanical blockage of the Rod Cluster Control Assemblies

(RCCA) and intersystem CCF between the Main Feedwater (MFW) system and the Start-up and Shutdown System (SSS). In the former case the value was a generic CCF factor – now superseded by an EDF database figure – and not an expert judgement, and in the latter case it is an explicit assumption rather than the result of an expert judgement process. In reality there are no cases that use formal expert judgement methods for direct CCF estimation, so the absence of a declared methodology is not an issue.

186 There was no general consideration of intersystem CCF in the PSA other than for the MFW and SSS meaning that failures of similar components in different systems are considered to be fully independent.

187 The documentation does not discuss uncertainties associated with the CCF parameters. This information is readily available for existing CCF databases, although not for the EUR beta factors. Given the use of conservative CCF factors, the lack of consideration of uncertainty will have only a minor effect and is not judged to be significant for GDA.

188 The PSA contains no discussion of assumptions made in regard to the defences against CCFs. TQ responses on this issue attempted to address the issue of CCF related assumptions, but did not successfully cover the need to capture CCF related assumptions for future development of testing, maintenance and operational strategies and procedures and strategies to maintain low CCFs during the completion of system designs.

189 Intersystem CCF is a difficult area to address within the Risk Gap Analysis as significant changes to the model structure would be required as well as trying to establish appropriate input values. Instead, as a representative example, a simple evaluation was performed by assuming high failure probabilities for all Motor Operated Valves (MOV). The associated cutset probabilities are not credible risk estimates but they do show the value of the PSA in identifying potentially important intersystem component groups where it is prudent to review CCF defences to help ensure intersystem CCFs do not have a significant impact.

4.12.2 Strengths

- The overall approach selected for the CCF basic event modelling within the system fault trees and analysis is adequate. Review of each of the system fault tree analysis reviewed in GDA Step 4 shows correct implementation of the model.
- The contribution of CCF to the PSA results had been adequately analysed for GDA.

4.12.3 Findings

Assessment Finding AF-UKEPR-PSA-024: *The licensee shall use the PSA to explore intersystem CCF effects and to inform the incorporation of appropriate defences (e.g. detailed design, procurement strategy and operational features such as test and maintenance). Where appropriate the intersystem CCFs should be included explicitly in the model.*

Assessment Finding AF-UKEPR-PSA-025: *The licensee shall ensure that the use of global CCF parameters in the PSA model are reviewed and where appropriate that the parameters are replaced with available system or component specific values.*

Assessment Finding AF-UKEPR-PSA-026: *The licensee shall ensure that CCF uncertainty is included in the PSA post GDA.*

> ***Assessment Finding AF-UKEPR-PSA-027:*** *The licensee shall provide and implement a procedure to ensure that CCF related assumptions are captured and used for future development of testing, maintenance strategies and completion of system designs post GDA (out of scope for GDA – see Section 2.3.6).*

4.12.4 Conclusions

- I judge the CCF modelling in the UK EPR PSA to be satisfactory, despite the fact that the global CCF parameters provide no discrimination between different CCF groups, for overall risk estimates within GDA.

4.13 Analysis of Hazards (A1-2.7)

4.13.1 Assessment

190 The PSA for internal and external hazards is reported in Sub-chapter 15.2 of the PCSR (Ref. 1). The analysis of hazards uses several sources to create the initial list of hazards as discussed in Sections 3.4.2 & 3.4.3 of the PSA (Ref. 36), including:

- French and German safety requirements;
- European Utility Requirements;
- French and international event experience;
- combinations of hazards (such as internal hazards due to external hazards);
- malevolent acts;
- the Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties;
- IAEA Safety Standards; and
- NUREG/CR-5042.

191 The use of these sources indicates that EDF and AREVA have striven to identify a complete list of internal and external hazards as a starting point for the analysis. The list of potential hazards is considered adequate.

192 The majority of external events are appropriately screened out on deterministic (i.e. no or limited impact on plant safety) or on probabilistic grounds. Animal infestation is excluded from the GDA.

193 Frazil ice, solid or fluid impurities released into the water from a ship (e.g. oil spill) and the effect of organic material on the water intake are included in the Loss of Ultimate Heat Sink (LUHS) initiating event and included in the RiskSpectrum® PSA model.

194 Accidental aircraft crashes are screened in for further analysis. This analysis is necessarily generic and uses a simplified approach using UK aircraft crash frequencies. The impact of aircraft on buildings is then considered and high level estimates of core damage frequency made. These estimates indicate insignificant contributions to the CDF. EDF and AREVA acknowledge the need for aircraft crash to be assessed using site specific data. The current analysis is judged to be adequate for GDA.

195 The seismic hazard has been addressed using a Seismic Margins Assessment (SMA) considered in a specific sub-section below.

196 In terms of internal hazards, missiles are screened out on the basis of analysis that demonstrates that physical barriers are such that only the system train which was the source of the missile is lost, hence the risk is bounded by the existing analysis of such failures – i.e. they have no consequential impacts.

197 Internal explosions have been excluded from the analysis and will be completed later in the licensing process when the detailed design studies have been completed. The PCSR makes reasonable qualitative arguments for exclusion of missiles, including those from turbine disintegration, from explicit analysis within the PSA model. In the latter case, EDF and AREVA acknowledge that site specific turbine missile risk needs to be considered.

198 The potential dependency between combinations of extreme weather events (snow and wind) and consequential LOOP was discussed during the assessment process. EDF and AREVA acknowledged the dependency and argued that the assessment of extreme weather conditions was highly site specific and that the revised frequencies they provided were suitable for a generic analysis. Although this only partly resolved the question, the Risk Gap Analysis indicated only a moderate impact on the risk even if a total dependency existed. EDF and AREVA's point that this type of analysis is really site specific was accepted.

199 Internal fire and internal flood (including pipe, tank, pump and valve leaks and breaks) are included in the PSA model and are considered individually below.

4.13.1.1 Strengths (Hazards General)

- The use of a wide range of sources demonstrates the use of a complete list of internal and external hazards to begin the analysis.
- Events are generally appropriately screened for further analysis.
- Further analyses of screened-in events are documented in an auditable manner and adequately address initiating faults and physical effects on the plant.

4.13.1.2 Findings

Assessment Finding AF-UKEPR-PSA-028: *The licensee shall ensure that the dependency between a LOOP and extreme weather events is taken into account and if necessary the PSA amended.*

Assessment Finding AF-UKEPR-PSA-029: *The licensee shall ensure that the generic loss of ultimate heat sink frequency is confirmed as bounding in comparison to a site specific value or demonstrate that a site specific frequency is acceptable in risk terms.*

Assessment Finding AF-UKEPR-PSA-030: *The licensee shall ensure that the PSA uses an appropriate loss of ultimate heat sink frequency for the site.*

Assessment Finding AF-UKEPR-PSA-031: *The licensee shall ensure that hazards such as internal explosion, turbine missiles and animal infestation are considered and if necessary included in the PSA model.*

Assessment Finding AF-UKEPR-PSA-032: *The licensee shall ensure that the screening criteria used in the GDA PSA are confirmed to bound specific site hazard characteristics and include in the PSA any hazards and combination of hazards that have been screened in.*

4.13.1.3 Conclusions

- Although there are findings that will need to be addressed in later phases of the PSA development, the overall approach to hazards and hazards screening is considered adequate for GDA.

4.13.1.4 Internal Fire (A1-2.7.2)

200 The GDA Step 3 assessment noted that the internal fire analysis was a standard Fire PSA carried out at a high level, with only very coarse discrimination of fire zones (entire buildings). The analysis does however cover all of the necessary plant locations.

201 In general the method used has been justified and the screening approach to identify the plant areas that do not create an Initiating Event or provide protection or mitigation capability is adequate. For all of the screened in fire scenarios the fire frequencies are derived from appropriate historical data, which is acceptable, however during GDA Step 3 an RO (RO-UKEPR-18) was raised over the subsequent subsuming of the fire suppression reliability into the initiating frequency. This is not a good practice as it may neglect dependencies in the accident sequence analysis and mask significance of the fire suppression equipment.

202 The assumptions noted for the fire analysis in the PCSR and supporting PSA (Ref. 36) will generally lead to a conservative analysis. However, the consolidated PCSR (Ref. 61) does not explicitly discuss the effects of these assumptions.

203 The fire modelling is also asymmetric, as all the fires associated with safeguards buildings are assumed to occur in just one of the buildings. Providing the design is sufficient to prevent fire propagation between buildings the asymmetry should not prevent reasonable risk estimates being made. But, as in the case of other asymmetric assumptions, the PSA is not yet suitable as an operational support tool.

204 All vulnerable components in a fire area with a fire are assumed failed. No specific justification is provided in Ref. 61 to support these assumptions / limitations although it is expected that this will yield conservative results.

205 Non-power states are excluded from the analysis based on an unsupported qualitative low risk argument. This limitation has already been noted as a Finding in this assessment report.

206 As in many other areas of the PSA, there seemed to be no process in place to capture the key fire analyses assumptions and findings from the PSA that may be important for future fire protection strategies and procedures, in the completion of system designs, in the finalisation of cable routings, and in the final construction. Furthermore, it is not clear whether Ref. 61 presents a consolidated list of all the assumptions and discusses the effects of each assumption on the analysis (see Section 5).

207 For RO-UKEPR-18, EDF and AREVA provided a response (Ref. 60) which carried out specific analyses to address the potential dependencies between the fire suppression system and the systems performing nuclear safety functions later in the accident sequences. The analysis was carried out using two fire scenarios, one was the turbine building fire, recognising that this is a high fire load building and the other was the reactor cooling system loop compartment. These fires contributed 0.7% and 1% to the CDF respectively.

208 In the sensitivity study for the turbine building fire the support system for the fire fighting systems (JAC) was explicitly modelled (fault tree analysis) and included in the event tree model for the fire. The results of this analysis showed no increase in the CDF and no significant dependencies between the JAC and the systems performing the nuclear safety functions.

209 For the RCS loop compartment fire, EDF and AREVA noted that the fire suppression system was manually actuated rather than automatically and this would need to be reflected in the PSA. For the sensitivity study it was pessimistically assumed that the operator action fails. EDF and AREVA did however take credit for oil collection devices limiting the likelihood of a significant fire. The oil collection devices have no dependencies with the systems performing nuclear safety functions. This sensitivity also showed no increase in the CDF.

210 The results of these analyses show that the UK EPR PSA results for GDA have not been underestimated by subsuming fire suppression probabilities into the initiating event frequency. EDF and AREVA offered to include these analyses in the revision to the GDA PSA, however as the Fire PSA will require significant upgrading post GDA there is no real benefit in it being modified in this way at this time. Specific base events representing fire suppression were created in response to RO-UKEPR-18.

4.13.1.5 Strengths (Internal Fire)

- The method selected for the analysis of internal fires is appropriately justified, and the analysis covers all the plant locations necessary to perform the risk calculation.
- The qualitative screening approach for internal fires is adequate to screen areas that do not create an initiating event or provide accident mitigation capability.
- For all screened-in scenarios, fire frequencies are identified and well documented.
- The fire event trees are produced from the internal event PSA event trees, and properly calculate core damage frequency.

4.13.1.6 Findings

Assessment Finding AF-UKEPR-PSA-033: *The licensee shall consolidate the assumptions made in the existing PCSR internal fire analysis in one location, and provide appropriate justification, reference, discussion of the effect of each assumption on the analysis and consider them as potential input to the full scope Fire PSA to be carried out post GDA*

Assessment Finding AF-UKEPR-PSA-002: *The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.*

Assessment Finding AF-UKEPR-PSA-034: *The licensee shall develop a full scope, Internal Fire PSA as the detailed design evolves (e.g. systematic inclusion of fire fighting system fault trees, inclusion of all individual buildings and compartments).*

4.13.1.7 Conclusions

- The Fire PSA is carried out at a very high level (single building) so does not provide any detailed information or insight in terms of optimising safety during operations. However I consider that the analysis and results provided are adequate for GDA.

4.13.1.8 Internal Flood (A1-2.7.3)

211 The GDA Step 3 assessment noted that the flooding risk for the UK EPR was carried out using a simplified Flooding PSA. In common with the Fire PSA, the analysis was carried out at a building level (rather than looking at compartments within a building) and was only carried out for at power operating states.

212 In the analysis itself all of the equipment in the affected building is assumed to be unavailable for plant safety, which is conservative. Flood detection is not analysed.

213 The simplified approach results in only two flooding scenarios. Most areas are screened out based on design considerations that would prevent significant floods or flood damage. The analyses are performed in a simplified, generally conservative manner, which shows them to be a very small contributor to the overall core damage frequency. Therefore, it appears that the analysis is sufficient to bound the risk from flooding, but it is not detailed enough to identify specific strengths and weaknesses.

214 The analysis appears to cover all the necessary plant locations relevant to the risk calculations. Section 6.4.3.2.3 of the PSA (Ref. 36) lists the equipment types that are assumed to be susceptible to flooding failure. However, failure mechanisms are not explicitly stated, although all of the equipment is assumed lost.

215 Evaluation of flooding frequencies has been performed for all the compartments qualitatively screened-in. However, the nature of all possible flood causes within each flood area is not provided and the justification for the selection of the chosen source is not described. The source chosen for the flood scenario is provided and is consistent with the assumption that uses the largest inventory of all the systems present in a flood area.

216 In addition, as for the fire analysis (see Section 4.13.1.4), it is not clear whether Ref. 61 presents a consolidated list of all the assumptions and discusses the effects of each assumption on the analysis (see Section 5).

4.13.1.9 Strengths (Internal Flood)

- The method selected for the analysis of internal floods is sufficient to bound the risk from flooding, and the analysis covers all the plant locations necessary to perform the risk calculation.
- The initiating flood frequencies, including uncertainty distribution and error factors, are documented and the values were confirmed to match those between the initiating faults section and the flooding analysis section of the .PSA report.
- The flooding event trees are produced from the internal event PSA event trees, and appear to properly calculate core melt frequency.

4.13.1.10 Findings

Assessment Finding AF-UKEPR-PSA-035: *The licensee shall consolidate the assumptions made in the existing PCSR internal flooding analysis in one location,* *and provide appropriate justification, reference, discussion of the effect of each assumption on the analysis and consider them as potential input to the full scope Flooding PSA to be carried out post GDA.*

Assessment Finding AF-UKEPR-PSA-002: *The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.*

Assessment Finding AF-UKEPR-PSA-036: *The licensee shall develop a full scope Internal Flooding PSA as the detailed design evolves.*

4.13.1.11 Conclusions

- The Flooding PSA is carried out at a very high level (single building) so, like the Fire PSA, does not provide any detailed information or insight in terms of optimising safety during operations. However I consider that the analysis and results provided are adequate for GDA

4.13.1.12 Seismic

217 The seismic analysis is performed using a PSA based Seismic Margins Assessment (SMA). Bounding generic site conditions are used for the design of Structures, Systems and Components (SSC) and a ground motion spectrum shape is assumed.

218 In a Seismic Margins Assessment the High Confidence of Low Probability of Failure (HCLPF) capacity is used as the measure of seismic margin. The HCLPF is a ground motion capacity value for which there is 95% confidence that the probability of failure is less than 5%. The target Seismic Margins Earthquake (SME) for the UK EPR is 1.6 times the Design Basis Earthquake (DBE), i.e. equal to 0.4g peak ground acceleration (PGA).

219 Section 2.2 of the PCSR Subchapter 15.6 (Ref. 1) indicates that the seismic equipment list for the UK EPR SMA has been developed using expert judgement in combination with the Level 1 PSA model. Structures and other passive components that are typically not included in the internal events PSA are also considered, particularly those that could lead directly to core damage or activity release.

220 The seismic fragility analysis follows state of the art methodology and procedures and for the UK EPR GDA, the fragility data are based on the following sources of information:

- Design and qualification data from Flamanville 3 or OL3 EPR studies when applicable.
- The design criteria and qualification procedures for the UK EPR.
- Generic data in the literature.
- Expert judgment.

221 Seismic event sequences are based on the Level 1 PSA internal events model taking account of the plant response to seismic events and the availability of the mitigation systems in the event of an earthquake. Four event tree types are identified and analysed in the SMA:

- Event trees where the initiator occurrence leads directly to core damage (comprises only the seismic initiator and the failure of the critical SSCs).

- Seismically induced LOOP event tree. It is assumed that Loss Of Off-site Power occurs with a probability = 1 following the SME event.
- Seismic small LOCA event tree, where the SBLOCA is caused by failure of small pipework or the reactor coolant pump seals.
- Event tree for ATWS, modelling the failure of control rods to insert following the seismically induced LOOP, due to rod blockage or C&I failure.

222 For human actions in the PSA-based SMA the HFEs are set to 1.0 in the PSA model so that they come to the top of the cutset list and can be evaluated qualitatively. In a Seismic PSA the HFE probabilities would be revised to take account of the conditions, but they would not necessarily be 1.

223 The Level 1 PSA fault trees for individual mitigation systems have also been modified to include a seismic failure mode (system failure or operator action failure) by introducing a seismic failure basic event in the fault tree, with an associated seismic HCLPF capacity for the system. The system HCLPF capacity is determined based on the lowest capacity determined for components in the system train.

224 Internal hazards that might be caused by a seismic event, such as fire or flooding, are not analysed in detail and are not included in the PSA model supporting the SMA.

225 Section 6.5.2 of Ref. 36 indicates that a detailed PSA-based SMA is performed for power states and a simplified approach is taken for shutdown states. The discussion on the simplified analysis approach and results for the seismic analyses for shutdown POS is very limited (Ref.1 Chapter 15.6 Section 4.4). The consolidated PCSR Chapter 15.6 (Ref. 61) does contain further discussion on shutdown POS.

226 The results of the SMA indicate seismic capacity of >0.6 g, which is significantly more robust than the target value.

227 The Seismic Margins Assessment considers the electrical switch gear fragility to be controlling in determining the plant HCLPF. Consequently a bounding risk calculation for the seismic hazard has been carried out as part of the Risk Gap Analysis by using plant fragility information based on the electrical switchgear (see PCSR Chapter 15.6 Ref. 1) together with a typical seismic hazard curve for the UK.

228 The results indicated a potential contribution to the core damage frequency of the same order as the other major contributors to the risk, although this result is likely to be conservative. The RGA clearly indicates that seismic hazard should be included and more detailed site specific analysis should be undertaken.

4.13.1.13 Strengths (Seismic)

- The seismic analysis is performed using a PSA based Seismic Margins Assessment (SMA). Using the internal events PSA fault tree models also ensures that random non-seismic equipment failure probabilities are considered in the analysis.
- The Seismic Equipment List (SEL) developed for the UK EPR SMA appears to be robust.
- A comprehensive set of SSC fragilities have been developed using state-of-the art methods.

- Structures and other passive components which are typically not included in the internal events PSA are also considered, particularly those that could lead directly to core damage or radioactivity release.

4.13.1.14 Findings

Assessment Finding AF-UKEPR-PSA-037: *The licensee shall provide a Seismic PSA for the site. The seismic analysis should take account of consequential hazards that might be caused by a seismic event, such as fire or flooding, and if appropriate include them in the PSA.*

Assessment Finding AF-UKEPR-PSA-038: *The licensee shall ensure that the impact of seismic faults during shutdown is addressed in a consistent manner with other contributions to the risk during shutdown.*

4.13.1.15 Conclusions

- The SMA shows a significant margin between the design basis event and the expected capability of the plant. Although this is encouraging, the Risk Gap Analysis does point to the need for further confirmatory work. To gain real insights in to the plant risk from earthquakes, a Seismic PSA would be needed.

4.14 Low Power and Shutdown (A1-2.8)

4.14.1 Assessment

229 The GDA Step 3 PSA assessment reported that standard PWR Plant Operating States (POS) have been considered for non-full power operational modes. The POS are described in the PCSR (15.1) and are summarised in Section 4.2 of this assessment report.

230 All operational states are addressed from full power operation through core unloading. Note that the return to power sequence of POS is assumed to be covered by the plant shutdown sequence.

231 The POS considered in the analyses, along with their durations and important characteristics of each POS are identified. This includes the status of the LHSI/RHR, the RCS configuration, secondary system heat removal capability status, the containment status, temperature and pressure in the RCS.

232 The list of internal IEs for shutdown states C, D and E appears to be comprehensive – no omissions were spotted – and the frequency analysis appears to be adequate. The success criteria for various IEs for the shutdown POS are clearly presented and supported by thermal-hydraulic analysis.

233 The contribution to the CDF due to internal hazards during shutdown states is considered to be negligible by EDF and AREVA for the following reasons:

- *“Fire and flooding events would be detected with a higher probability due to the fact that the personnel working on the systems and components used for tests and maintenance would detect the internal hazard case in a timely fashion, and*
- *Longer grace periods during plant shutdown lead to more reliable measures to cope with internal fire or flooding event.”*

This is not an adequate justification. These events should be properly modelled as they may lead to operational requirements or restrictions (see Section 4.2).

234 Shutdown POS specific HRA analyses has been performed for required post fault operator actions, but there was no detailed discussion of human action related initiators during shutdown, although they are included in the analysis. The HRA methods used are based primarily on "grace period" and estimated stress level, so are relatively insensitive to the POS.

235 Section 6.5.2 of Ref. 36 indicates that a detailed PSA-based SMA is performed for power states but only a simplified approach is taken for shutdown states. Only very limited discussion on the simplified analysis approach and results for the seismic analyses for shutdown POS was included (PCSR 15.6 Section 4.4).

236 For states Cb and D the RCS water inventory can range from a low value represented by 3/4 loop operation to a greater value (i.e. reactor pool flooded level in plant state D). In the PSA it is stated that the minimum water inventory condition is assumed to represent the shutdown state. However, a number of instances were found where more optimistic assumptions were used (greater water inventories). These assumptions need to be clarified in the development of the PSA during Phase 2 – the site licensing process.

237 The Risk Gap Analysis in this area has looked at the impact of using more conservative estimates for the water inventories for states Cb and D by assuming much shorter grace period for operator action. However the impact is small.

4.14.2 Strengths

- The shutdown Plant Operating States (POS) are adequately defined with a clear progression of states without gaps or overlaps.
- All operational states are addressed from full power operation through core unloading.
- The POS considered in the analyses, along with their durations and important characteristics of each POS, are identified.
- The list of internal IEs for shutdown states C, D and E is satisfactory and the frequency analysis appears to be adequate.
- The success criteria for various IEs for the shutdown POS are clearly presented and supported by thermal-hydraulic analysis.

4.14.3 Findings

Assessment Finding AF-UKEPR-PSA-002: *The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.*

Assessment Finding AF-UKEPR-PSA-038: *The licensee shall ensure that the impact of seismic faults during shutdown is addressed in a consistent manner with other contributions to the risk during shutdown.*

Assessment Finding AF-UKEPR-PSA-039: *The licensee shall ensure that the actual RCS water inventories for shutdown POS need is established and if necessary the analysis repeated to inform appropriate operating restrictions.*

4.14.4 Conclusions

- Despite some limitations in terms of insights to help future operational plant control, there is adequate representation of low power and shutdown in the PSA submitted for GDA purposes.

4.15 Uncertainty, Quantification and Interpretation (A1-2.9)

4.15.1 Assessment

238 The quantification has been performed using the RiskSpectrum® software. The truncation level adopted has been demonstrated to yield stable results. Extensive analysis of the results has been performed using importance analyses and sensitivity studies, so that the important contributors to the results can be identified and the reasons for their significance understood in terms of how they relate to the structure of the PSA model. The presentation of the results is clear and thorough.

239 The parametric uncertainty analysis is not consistent with the state of the art as it does not address the so called “state-of-knowledge correlation” (SOKC). This is identified as a good practice for example in IAEA-TECDOC-1511. This omission is a deliberate choice by EDF and AREVA as they believe that it is misleading to consider that all components sharing the same parameter would be correlated, hence the sampling is done at the basic event level, rather than the parameter level.

240 It is probably true that universal application the SOKC could be misleading, although from a strictly theoretical point of view it is correct to do so. Neglect of the SOKC only has an effect when there are cutsets that include multiple basic events whose probabilities are based on the same parameter. There are in fact no such cutsets in the top 100 for CDF and the error factors used to characterize the uncertainty on the parameters are typically quite small (of the order of 3), so it is not likely that this omission will have an impact on the PSA results. A sensitivity calculation carried out by EDF and AREVA in which the uncertainty characterisation was performed at the parameter level rather than at the basic event level bears out this judgement for CDF. Neglecting the SOKC for ISLOCA was considered in the Risk Gap Analysis although it was difficult to identify a meaningful quantitative study. A bounding estimate for the potential impact was obtained by increasing the ISLOCA frequency by a factor of 10 (which represents the maximum possible increase due to SOKC). This resulted in a moderate impact on the large release frequency.

241 EDF and AREVA also examine key modelling assumptions using sensitivity analysis. Many of the choices made are claimed to be conservative and this appears to be the case. Others are choices that have to be borne in mind when interpreting importance analysis results (for example, the assumption that a LOCA always occurs in train 4 – see 4.1.2). It is important to identify these assumptions since they have an impact on how to interpret the results of the PSA, and provide a guide as to where future refinement of the model might be fruitful.

242 The identification of these key modelling assumptions and the related sources of uncertainty is crucial to fully understand the insights from the PSA model. While the assumptions are documented, they are dispersed throughout the PSA reports and are not always easy to find and hence could be overlooked when interpreting the results of the PSA.

243 The long term analysis sensitivity study reported in chapter 15.7 of the PCSR (Ref. 1) provides some confidence that the CDF in the baseline PSA results has not been significantly underestimated by exclusion of long term LUHS and LOOP faults. The

analysis presented assumes periods of 192 hr for LOOP and 100 hr for LUHS. However the sensitivity results are certainly not negligible. More importantly the analysis contains potentially significant insights for future plant operation such as ability to repair Diesel Generators (DG), and support the emergency feed water system with fire fighting water (from the JAC). Not only do these features need to be properly developed and included in plant procedures, training, technical specifications, etc. the long term faults need to be properly incorporated into the overall PSA as the detailed design evolves so that the importance of these, and possibly other long term recovery measures, is captured and taken into account in future decision making.

244 During the assessment of success criteria discussed in 4.5 above, it was identified that the function "containment heat removal" was not included in some of the event trees as the pressure increase without cooling was acceptable for more than the 24 hr mission period. If the affected sequences were assumed to lead to core damage in the long term, which is clearly conservative, there would be a moderate impact on the results.

4.15.2 Strengths

- The truncation level adopted in the PSA has been demonstrated to yield stable results.
- Extensive analysis of the results has been performed using importance analyses and sensitivity studies.
- Important contributors to CDF and LERF can be identified and the reasons for their significance understood.

4.15.3 Findings

Assessment Finding AF-UKEPR-PSA-040: *The licensee shall ensure that full consideration of parametric uncertainty is included the PSA.*

Assessment Finding AF-UKEPR-PSA-014: *The licensee shall provide and implement a consistent process to ensure capture of assumptions that are currently dispersed throughout the PSA reports and its supporting documentation and gather them together in a single place within the PSA documents. This should be done in a systematic and traceable way, and the assumptions sentenced as part of a future PSA development (out of scope for GDA – see Section 2.3.6).*

Assessment Finding AF-UKEPR-PSA-041: *The licensee shall ensure that long term faults should be properly incorporated into the overall PSA as the detailed design evolves so that the importance of long term recovery measures (such as repair of Diesel Generators and supporting the emergency feed water system with fire fighting water) is captured and taken into account in future procedures and decision making.*

4.15.4 Conclusions

- Overall the consideration of uncertainty in the PSA is judged to be adequate for GDA, although further confirmatory work is expected in later phases of the PSA development.

4.16 Level 1 PSA Results (A1-2.9.3)

4.16.1 Assessment

245 The UK EPR PSA documentation adequately summarizes the results of the Level 1 PSA and a selection of these is reproduced in Section 3 of this assessment report. In addition to the direct core damage frequencies, the documentation also provides discussion of:

- Contributions to the core damage frequency by types of events, operating states, and initiating events.
- The use of importance measures to identify significant components, systems, operator actions, and CCF events.
- The dominant core damage sequences.
- Key assumptions.
- Calculation of parametric uncertainty (although see Section 4.15).
- Sensitivity analyses for selected key issues.

246 The results documented in PCSR Chapter 15.7 Issue 02 have been verified against the actual model results.

247 Section 5 of PCSR (Ref. 1) Chapter 15.7 Issue 02 (and also Chapter 8.4 of the PSA Ref. 36) discusses the use of PSA insights to identify improvements to the plant design. This does not explicitly identify vulnerabilities, as they have been rectified, but captures the purpose of this expectation. Identified corrective actions include improvements such as:

- reinforcement of containment isolation devices to reduce ISLOCA;
- diversification of reactor trip actuators and sensors to reduce ATWS;
- addition of a main feed water pump;
- addition of two Station Blackout (SBO) diesel generators;
- alignment of chilled water to cool LHSI pumps;
- improvements to SIS auto-start signals during mid-loop operation; and
- addition of two bleed lines for feed-and-bleed operation.

248 The PCSR and PSA report sections discussed above state that an iterative process was used to identify design improvement from PSA input.

249 The contributions to the CDF from the different POS are also discussed and although instantaneous frequencies are not quoted directly, the risk information and POS durations indicate that the intent of SAPs NT2 is met.

4.16.2 Strengths

- The PCSR and supporting documentation adequately summarize the results of the Level 1 PSA.
- It is clear that PSA insights were used as a part of an iterative process to identify improvements to the plant design.
- The Level 1 PSA results reported by EDF and AREVA are lower than the BSOs in SAPs Target 8 (see Table 2).

4.16.3 Findings

- There are no findings associated with the presentation of the Level 1 PSA results.

4.16.4 Conclusions

- The presentation of the Level 1 PSA results is considered to be adequate for GDA.

4.17 Level 2 PSA (A1-3)

4.17.1 Assessment

250 The GDA Step 3 assessment report concluded that the UK EPR Level 2 PSA was sound with only minor points being identified during the review. In GDA Step 4 the Level 2 PSA assessment has focussed on the technical evaluations provided in response to TQs raised during GDA Step 3 and a review of the UK EPR MAAP parameter file and selected input and output files from the UK EPR MAAP analysis.

4.17.1.1 Interface Between Level 1 and Level 2 PSA (A1-3.1)

251 PCSR Sub-Chapter 15.4, Section 3.2 provides a detailed description of the interface between Level 1 and Level 2. Using the RiskSpectrum® software, the UK EPR Level 2 PSA has been directly linked to the Level 1 PSA model. This direct link provides for:

- Quantification of the model from initiating event all the way through to the release categories.
- Linking of the Level 1 and Level 2 models allows for accurate transfer of dependency information.

252 Overall, using the RiskSpectrum® PSA software to link the Level 1 and Level 2 analyses is judged to be a strong element of the UK EPR PSA

253 Core Damage End States (CDES) are defined to link the Level 1 core damage event trees to the appropriate Level 2 containment event trees (CET) by combining similar core damage characteristics. Attributes of the CDES include:

- sequence type (Transients, LOCAs, etc);
- containment status (bypass, SGTR, interfacing system LOCA);
- system information;
- offsite power availability;
- feed water availability; and
- steam generator pressure and isolation status.

254 The main purpose for developing the CDES is that the individual severe accident phenomenological split fractions represented in the CET will be dependent on the specific CDES. In addition to at-power conditions, the CDESs are also developed for shutdown end states.

255 The interface between the Level 1 and Level 2 PSA models represents the state-of-art and no limitations have been identified.

4.17.1.2 Deterministic Accident Progression (A1-3.2)

256 The deterministic accident progression analysis is based on calculations performed using the Modular Accident Analysis Program (MAAP) version 4.0.7. This is an EPRI code and is the most widely used severe accident progression code by the nuclear industry worldwide. It represents many years of severe accident research and has been benchmarked against numerous separate effects tests, actual plant data, other detailed code analysis, and experiments.

257 As part of the GDA Step 3 assessment, several points were identified that required a more thorough review in GDA Step 4 since the supporting documentation was not available at that time. The GDA Step 4 assessment included a more detailed review of the following:

- UK EPR MAAP parameter file; and
- specific modelling options selected for the UK EPR.

258 The UK EPR MAAP 4.0.7 parameter file development (Ref. 38 to Ref. 40) provides a strong technical justification for each input parameter. The documentation provides a clear rationale for any departures from default or standard modelling assumptions. A concise description of the UK EPR MAAP containment node and junction derivation is provided with supporting references. Overall, the parameter file development is well documented with clear descriptions of UK EPR-specific modelling assumptions.

259 Use of the MAAP4 code is appropriate for this type of application and the documentation indicates proper use of the code within known limitations.

260 PCSR Sub-chapter 15.4, Section 3.3 identifies the severe accident phenomena represented in the PSA Level 2. References are cited that verify that all relevant phenomena have been addressed. The quantification of individual split fractions is based on a Monte Carlo evaluation.

4.17.1.3 Containment Performance Analysis (A1-3.3)

261 The GDA Step 3 assessment concluded that the containment fragility evaluation included in PCSR Sub-Chapter 15.4 Sub-Section 3.3.14 seemed to use standard practices for evaluating containment failure, but a more detailed review of the structural analysis was needed in GDA Step 4 to assess the boundary conditions and assumptions used in the analysis.

262 The UK EPR Level 2 PSA Supporting Containment Fragility (Ref. 62) was subsequently provided by EDF and AREVA and this report describes the assumptions behind the UK EPR containment failure analysis. The analysis is based on the Finnish EPR OL3 plant evaluation and currently does not include a consideration of penetrations or leakage failure modes of containment, i.e. all failures are assumed to be gross failure of the containment. This analysis is judged to be conservative and is an acceptable approximation for the UK EPR Level 2 PSA, however it does not represent a UK plant specific evaluation.

4.17.1.4 Probabilistic Modelling – Accident Progression Event Trees (A1-3.4)

263 PCSR Sub-Chapter 15.4, Section 3.4 describes the accident sequence analysis along with the Containment Event Trees (CET). The development of 10 Containment Event Trees is used to evaluate severe accident phenomena and to quantify their impact on the

radionuclide release. RiskSpectrum® is an appropriate software tool for modelling the accident progression. The number of CETs and corresponding branch points are sufficient to capture the important elements of a full Level 2 PSA.

264 The split fractions assigned to individual severe accident phenomena are clearly derived in several technical calculations. The supporting analysis documentation addresses the following key Level 2 phenomena:

- In-Vessel Recovery (Ref. 63): A thorough probabilistic assessment is developed for evaluating the potential to recover a damaged core prior to vessel breach. Reference to a variety of experimental and technical studies is used to formulate a credible approach for the UK EPR.
- Hydrogen Combustion (Ref. 64): This evaluation analyses the challenges due to deflagration, detonation, and flame acceleration leading to deflagration-to-detonation transition (DDT). The evaluations use available reference information and develop containment failure probabilities for several unique accident scenarios. This analysis provides a strong technical position for the UK EPR and is of high quality.
- Induced RCS Ruptures (Ref. 65): As a result of core uncovery and heatup, superheated gas can be circulated to the steam generators via the hot leg. Induced rupture of the RCS can occur primarily at the hot leg nozzle and within the steam generator tubes. The supporting analysis performed as part of the EPR Level 2 PSA investigates both of these failure modes in detail and provides sensitivity analyses to further investigate the impact of uncertainties associated with this phenomenon. The evaluation utilizes current industry references and provides a strong technical position for the UK EPR.
- Vessel Failure (Ref. 66): Relative to the vessel failure analysis, it is stated that over-pressure of the reactor pit would only impact melt stabilization and does not represent a direct containment failure. Should the reactor pit fail there may be a possibility for the reactor vessel to shift, causing damage to reactor vessel piping that could potentially lead to containment bypass. This phenomenon is not considered for the EPR.
- Long-Term Containment Challenges (Ref. 67): These begin when core debris is discharged from the reactor vessel. The report looks at phenomena associated with steam generation due to core debris quenching and possible molten core concrete interactions in the case of inadequate debris cooling. The UK EPR assessment makes use of available experimental results from the MACE and FZK programs to determine the appropriate debris cooling rates. The probabilistic evaluation utilizes a Decomposition Event Tree (DET) to calculate the containment probabilities for: *No containment failure*, *Late overpressure failure*, *Basemat penetration*. The use of the DET provides a strong technical basis for the late challenges to containment.

265 Each technical evaluation provides a clear description of the problem being investigated and a sound technical approach to address it within the context of the Level 2 PSA. The technical evaluations are well documented and judged to be of high quality.

266 The Level 2 Human Reliability Analysis (Ref. 68) provides a detailed description of the Level 2 operator actions included in the UK EPR Level 2 PSA. Comments on the Level 2 HRA are included in Section 4.8.

267 EDF and AREVA have noted that the latest version of the PSA model (Ref. 71) is now considered inconsistent with the current Severe Accidents Management Strategy (Ref. 72) in respect of claims on the Safety Injection system. A sensitivity study has indicated a

low impact on the LRF, so the conclusions of this assessment report remain valid, although the PSA should be amended to reflect the current strategy (Assessment Finding AF-UK EPR-PSA-046 covers this requirement).

4.17.1.5 Source Term Analysis (A1-3.5)

268 There is a considerable amount of documentation relating to the source term analysis performed for the UK EPR using MAAP 4.0.7. Supporting analyses (Refs 38 to 40 and Ref. 69) are provided as part of the GDA Step 4 submission giving a summary of the MAAP model for the UK EPR and also details of the validation performed to justify the use of MAAP for the UK EPR Level 2 PSA.

269 The EPR MAAP 4.0.7 output documentation details each representative release category MAAP case. The input assumptions are clear and there is a technical description of any post-processing of the results that has been undertaken. Post-processing of the releases is used to represent the following issues, which are not typically included in the MAAP analysis:

- Containment leakage rates;
- Iodine chemistry;
- production of CH_3I;
- annulus and fuel / safeguards building ventilation;
- scrubbing in ISLOCA cases; and
- scrubbing in SGTR cases.

All of the post-processing rules are clearly documented.

270 An assumption is made that all releases can be represented as a single plume with a linear release history. Typical MAAP results show an initial puff release followed by a more gradual long term release. EDF and AREVA subsequently provided plots of the detailed time history of the release to support their assumption. In addition, the release histories for several fission product groups were modified by EDF and AREVA to represent the early low magnitude release due to containment leakage followed by a larger plume at the moment of failure. These modifications more accurately represent the release history and provide a better representation for the Level 3 PSA input and have been considered in the Level 3 PSA assessment reported below (see Section 4.18).

4.17.1.6 Presentation and Interpretation of the Level 2 PSA Results (A1-3.6.)

271 PCSR Sub-Chapter 15.4, Section 4 provides the Level 2 PSA results. Included in the tables are:

- Large Release Frequency (LRF) and Large Early Release Frequency (LERF) for each release category (at-power and shutdown).
- CDES frequency as a fraction of the total CDF.

272 The information provided gives a clear picture of the scenarios that are controlling the radionuclide release.

273 Model sensitivities are investigated for the Level 2 PSA. The results indicate sensitivity to hydrogen deflagration and flame acceleration when the base probabilities were set to 1.0. Sensitivity was also found with containment failure induced by in-vessel steam explosion.

This impacts the large release frequency due to its impact on the melt stabilization process.

274 Other sensitivities were identified for human actions to manually isolate containment and to initiate sprays in the long term. Sensitivity studies also revealed that the total contribution to LRF from human actions was 60% but the majority of this is due to Level 1 PSA actions rather than Level 2 PSA HFEs.

275 There are no specific plant vulnerabilities identified in the Level 2 PSA results.

4.17.2 Strengths

- The implementation of an integrated Level 1 and Level 2 PSA allows for a complete transfer of Level 1 information into the Level 2 and provides for a higher quality Level 2 PSA model.
- Modelling of complicated severe accident phenomena is supported by strong technical evaluations.
- The use of sensitivity and uncertainty analysis in modelling of Level 2 accident phenomenology and primary system and containment response represents a very thorough technical position.
- The use of MAAP is adequately supported by a variety of benchmarks with an acknowledgement of any apparent shortcomings.

4.17.3 Findings

Assessment Finding AF-UKEPR-PSA-042: *The licensee shall ensure that a UK-EPR specific containment structural analysis is performed which addresses all potential modes of containment failure, including penetration and leakage failures.*

Assessment Finding AF-UKEPR-PSA-043: *The licensee shall update the Level 2 PSA model to ensure consistency with the current Safety Injection Severe Accident Management Strategy.*

4.17.4 Conclusions

- Integration of the Level 1 and Level 2 PSA is a real strength of the overall PSA submission. Despite some limitations noted on the modelling of the containment structural response, the Level 2 PSA is considered to be state of the art and is adequate for GDA.

4.18 Level 3 PSA (A1-4)

4.18.1 Assessment

276 No assessment of Level 3 PSA was carried out at GDA Step 3. The primary focus of assessment in GDA Step 4 has been on the adequacy of EDF and AREVA's derivation, from the release frequencies and source terms yielded by other parts of the UK EPR safety case, of risks to the public for comparison with Targets 7 to 9 from NT.1 of the SAPs. It is recognised that, as many parameters needed in Level 3 PSA are site specific (for example weather and population distribution), the risks derived for GDA are only indicative.

277 As EDF and AREVA's case claims risks below the BSOs, in accordance with SAPs requirements under that circumstance, my assessment has been principally concerned with confirming the validity of the claimed risk figures. As suggested in T/AST/30 and T/AST/45, independent calculations were carried out. These were performed using the computer code PC COSYMA by the UK Health Protection Agency (HPA) as a Technical Support Contractor to ND. The results confirmed EDF and AREVA's analysis to the degree of accuracy that can be expected for a Level 3 PSA. The broad agreement between the HPA's calculated radiological consequences and those of EDF and AREVA is important in forming a judgement as to the acceptability of EDF and AREVA's case for the purposes of GDA.

4.18.1.1 Assessment of the Level 3 Analysis (A1-4.1)

278 Sufficient off-site radiological consequence assessments have been carried out by EDF and AREVA for comparison with SAPs Targets 7, 8 and 9. Consequences are calculated in terms of long term doses for comparison with Target 8. Results do not include the specific calculation of early or late health effects based on organ doses. Based only on these doses an estimate of risk of death is made in Chapter 17 of the PCSR for comparison with Target 7 and a screening method is adopted to identify releases that are likely to result in significant off-site consequences for comparison with Target 9.

279 For each release category the source terms are clearly defined including quantities released, release frequencies and timings of release. However, the methods used to calculate doses and to allocate each release category to a particular dose band are not clear in every case in the submission, and there is also some inconsistency in the methods chosen in terms of conservatism. Ultimately, this is not a significant problem in terms of demonstrating that the safety objectives are met, but leads to lack of clarity on their relative significance.

280 The calculation of societal risk uses a screening process to identify only those release categories that are likely to result in 100 or more fatalities. The screening process uses the results of a radiological consequence assessment carried out for the Sizewell PWR in 1982.

281 Both deterministic and probabilistic risk analyses have been used by EDF and AREVA in the Level 3 PSA however the risks presented do not include the probability of a particular weather condition occurring. This probability would normally be included when comparing risks with SAPs Targets 7 and 9. EDF and AREVA's analysis is not state of the art but it is considered adequate for GDA.

282 The treatment of a core melt accident identified in the Severe Accident Analysis clearly defines the source term, countermeasure criteria and off-site consequences. EDF and AREVA have used two methodologies, one probabilistic and the other deterministic. There is a lack of clarity in the radiation dose assessment methodologies used.

4.18.1.2 Presentation and Interpretation of the Level 3 PSA Results (A1-4.2)

283 Results are clearly presented and a useful summary with discussion is provided in Chapter 17 of the PCSR. Results are compared with the appropriate SAPs targets although it should be noted that risks do not include early health effects and do not take into account the probability that a particular meteorological sequence will occur.

284 In Table 10 of Section 15.5.3 of the PCSR, the total frequency of all release categories that fall within each dose band are presented for comparison with SAP Target 8. These

results show that the calculated frequency in each dose band is consistently below the corresponding BSO and in most cases by more than an order of magnitude. In Chapter 17 of the PCSR, the results of Table 10 are converted to risks of death by multiplying the upper end of each dose band by a fatal cancer risk of 5% per Sv and scaling by the release frequency. The result is an estimate of total risk of death of 1.7x 10^{-7} per annum which can be compared with the BSO of 1 $x10^{-6}$ from SAP Target 7. The result does not include variability in meteorological conditions.

285 A screening approach, based on previous accident consequence assessments of UK power stations, is used to determine which release categories from the Level 2 PSA are likely to result in significant off-site consequences i.e. in 100 or more deaths. Table 11 of Section 15.5.3 of the PCSR lists these Level 2 PSA release categories and the corresponding release frequencies and sums them for comparison with SAP Target 9. The result is a risk of 8 $x10^{-8}$ per annum which is just below the BSO for Target 9. However, the actual doses that have been estimated are not presented in the PCSR and the results of the HPA study (Section 3.3.3) suggest that some may result in a number of deaths that significantly exceeds 100. Chapter 17 of the PCSR covers various requirements of ALARP in detail. In particular, Chapter 17.4 demonstrates that the doses and risks calculated are below SAPs targets.

4.18.2 Strengths

- A comprehensive set of accident sequences is considered.
- The reasons for choosing the selected accident sequences are clearly defined.
- The results for comparison with Targets 7, 8 and 9 from Numerical Target NT.1 of the SAPs are clearly presented.
- An analysis is carried out to determine the off-site consequences of a core melt sequence.

4.18.3 Findings

Assessment Finding AF-UKEPR-PSA-044: *The licensee should ensure that the Level 3 PSA is developed to modern standards, in particular by placing less reliance on design basis dose assessments and by fully incorporating probabilistic factors such as weather. For each new plant the Site-specific Level 3 PSA will need to incorporate site specific analyses of frequency for relevant fault sequences, together with site specific dispersion and consequence modelling parameters (such as weather data and distribution of population and agriculture) for all releases.*

4.18.4 Conclusions

- The Level 3 PSA is not state of the art. However, in view of the assurance provided by the correspondence between the numerical outcomes and those from independent calculations performed for HSE, it is considered adequate for the purposes of GDA.

4.19 Overall Conclusions from the PSA (A1-5).

286 My assessment of the UK EPR PSA has been conducted using the framework provided by T/AST/030. There have been difficulties with PSA documentation during the assessment process, leading to the issue of RO-UKEPR-68. EDF and AREVA have

responded positively to this RO. Some of the documentation that will be needed to support a Licence Instrument for nuclear safety related construction are “out of scope” and this is identified in Section 2.3.6.

287 In addition to consolidating the documentation to support a Licence Instrument for nuclear safety related construction, it will be important that a process is put in place after that Licence Instrument to keep the PSA living – i.e. that it is updated to reflect design and anticipated operational features as they evolve during the construction phase.

288 Furthermore the developing PSA needs to be used in an iterative manner as the design develops to help ensure the risks are, and remain ALARP, so that future site specific safety submissions are also capable of being judged to meet SAP FA 10 (Ref. 4).

4.19.1 Strengths

- The PSA is credible and defensible at this stage of the process (i.e. support for a PCSR) and provides overall risk estimates that are lower than the BSOs for Targets 7, 8 and 9 from NT.1 of the SAPs.
- The PSA has been used in an appropriate manner to support the ALARP summary presented in chapter 17 of the PCSR.

4.19.2 Findings

Assessment Finding AF-UKEPR-PSA-011: *The licensee shall ensure that the process for maintaining and developing the PSA model configuration and supporting document trail (see RO-UKEPR-68 discussion) is retained post GDA, or an equivalent process put in its place (out of scope for GDA – see Section 2.3.6).*

Assessment Finding AF-UKEPR-PSA-014: *The licensee shall provide and implement a consistent process to ensure capture of the assumptions that are currently dispersed throughout the PSA reports and its supporting documentation and gather them together in a single place within the PSA documents. This should be done in a systematic and traceable way, and the assumptions sentenced as part of a future PSA development (out of scope for GDA – see Section 2.3.6).*

Assessment Finding AF-UKEPR-PSA-045: *The Licensee shall provide and implement a procedure to maintain the PSA and keep it Living (out of scope for GDA – see Section 2.3.6). This should include PSA task procedures and methodologies.*

Assessment Finding AF-UKEPR-PSA-046: *The Licensee shall provide and implement a procedure for the use of the PSA to support all aspects of design and operation of the NPP (out of scope for GDA – see Section 2.3.6).*

4.19.3 Conclusions

- The overall conclusions from the PSA are set out clearly in the PCSR, in Chapter 15.7 for the PSA itself and in Chapter 17 for the use of PSA in the overall ALARP summary.

4.20 Overseas Regulatory Interface

289 HSE's Strategy for working with Overseas Regulators is set out in Ref. 70. In accordance with this strategy, HSE collaborates with Overseas Regulators, both bilaterally and multinationally

4.20.1 Bilateral Collaboration

290 HSE's Nuclear Directorate (ND) has formal information exchange arrangements to facilitate greater international co-operation with the nuclear safety regulators in a number of key countries with civil nuclear power programmes. These include:

- the United States Nuclear Regulatory Commission (US NRC);
- the French Autorité de Sûreté Nucléaire (ASN); and
- the Finnish STUK.

4.20.2 Multilateral Collaboration

291 ND collaborates through the work of the IAEA and the OECD Nuclear Energy Agency (OECD-NEA). ND also represents the UK in the Multinational Design Evaluation Programme (MDEP) - a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. This helps to promote consistent nuclear safety assessment standards among different countries.

292 In the PSA assessment, insights from other Regulators looking at EPR variants have been gained through the MDEP. We have shared assessment views and findings with our MDEP partners (USA, France, Finland, Canada and China) and contributed to joint working. MDEP is expected to continue beyond GDA and ND will continue to take an active role. One of the key PSA assessment activities undertaken within GDA as a result of MDEP concerned the Level 2 PSA modelling, following advice given by the Finnish nuclear safety authority, STUK, who had raised questions on Level 2 PSA modelling suitability and possible quantification errors. Although the UK Level 2 PSA model was thought unlikely to have these problems, being a more recent analysis from a different source, STUK's advice was welcomed and work was commissioned to examine these points. The outcome of this work is discussed in Section 4.3 above.

293 Also through MDEP, US NRC provided a list of questions and responses they received relating to the US EPR and in an effort to make use of this information we have looked at the US EPR PSA (which is published on NRC's website) (Ref. 37) to gauge the extent to which the NRC views are directly relevant to the UK EPR. We have, however, identified significant differences in the UK and US PSA variants ranging from the accident sequence modelling (see Section 4.6) to the component failure data (4.10) which makes direct use of NRC findings impossible. The use of different approaches and data does not, of course, invalidate either PSA and in the UK ND does not prescribe how a PSA should be done or the data that it uses, only that the utility justifies all parts of the submission.

294 At MDEP, AREVA presented some of the main differences in PSA modelling and plant designs between the FA3 EPR, UK EPR, Taishan EPR, OL3 EPR and the US EPR that could explain the variability in the PSA results submitted to MDEP partners (Ref. 73). In

addition, these projects are at different stages of design development and this is reflected in the amount of detailed information available and considered in the PSA. The overview of the associated PSA results hinted that the risk associated with gaps in the PSA, due to the lack of the detailed design, could have a numerical impact. The MDEP partners are planning to carry out further work on PSA comparison and ND expects to play a prominent role in this exercise. This is likely to include the following items:

- Detailed comparison of the list of Initiating Events.
- Detailed comparison of Event Tree models for a selected number of internal Initiating Events.
- C&I modelling.
- CCF modelling.
- Internal Hazards PSA.

295 Insights obtained from AREVA's MDEP presentation, plus the overview of the USA, France and Finland PSA results, helped us to consolidate GDA assessment findings and milestones and highlighted the importance of implementing an iterative procedure to control the interactions between the PSA and Design Change Process (see Section 4.19).

4.21 Interface with Other Regulators

296 The principal interface with other UK Regulators is with the Environment Agency with whom we have a close working relationship and a shared Joint Programme Office (JPO) for GDA. As PSA is primarily concerned with accidents and the Environment Agency are mainly interested in normal operation, there has been no detailed PSA interaction, although we have met regularly to share emerging findings in an effort to ensure there are no gaps.

4.22 Other Health and Safety Legislation

297 There is no other Health and Safety Legislation relevant to PSA considered in this Assessment Report.

5 CONCLUSIONS

298 This report presents the conclusions and findings of the GDA Step 4 Probabilistic Safety Analysis (PSA) assessment of the EDF and AREVA UK EPR reactor.

299 The Step 4 assessment in my topic area commenced with consideration of the relevant chapters of the PCSR and supporting references available at that time, and these are referred to as appropriate in this report. As the GDA submission developed during Step 4, in response to my regulatory questions, amendments were made as appropriate to the PCSR and its supporting references. A review has been made of the updates to the GDA submission in my technical topic area and the conclusion of this review is that the updates to the GDA submission are not fully as expected, and some further amendments to the consolidated PCSR (Ref. 77) and / or supporting references listed within the Submission Master List (Ref. 78) will be required. These will be progressed through GDA Issue GI-UKEPR-CC-02. However, these actions do not have a significant impact on my assessment report and in my technical topic area.

300 Broad conclusions are as follows:

- EDF and AREVA have provided a large, modern standards PSA as part of their overall GDA submission.
- The scope of the PSA includes internal faults, internal and external hazards, all operating states and reasonable allowances for maintenance and test. It also includes all significant sources of radioactivity. This is considered adequate for GDA.
- The PSA is an adequate representation of the design described in the GDA submissions and it is clear that the PSA has been used to inform the development of the design.
- Integration of the Level 1 and Level 2 PSA models is a strength of the analysis.
- The PSA results presented by EDF and AREVA meet the BSOs of Targets 7, 8 and 9 from NT.1 of the SAPs.

301 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for the PSA. I consider that from a PSA view point, the EDF and AREVA UK EPR design is suitable for construction in the UK. This conclusion is subject to satisfactory delivery, incorporation and assessment of the “out of scope” items listed in Section 2.3.6 of this report, together with confirmation that site specific factors, such as weather conditions, are bounded by the assumptions made in the PSA.

5.1 Key Findings from the Step 4 Assessment

5.1.1 Assessment Findings

302 The overall Assessment Findings are:

- There are some limitations identified in this assessment report as findings, and many of them point to the need for the PSA to develop into a suitable operational support tool. Other limitations are associated with lack of design detail available at this stage of the process, and the need for clear documentation of the analysis and the assumptions that need to be carried into the future design and operation of a UK EPR.

- The Assessment Findings from each part of Section 4 are summarised in Annex 1 and should be considered during the forward programme of this reactor as normal regulatory business, post the Generic PCSR.

303 Assessment Findings' milestones are defined in Annex 1 and relate to the date by which the finding should be addressed. The activity to satisfy the milestone will obviously need to start earlier and will also need to fulfil SAP FA10 requirement (Ref. 4) that sufficient PSA is performed as part of the design development (see Assessment Finding **AF-UK EPR-PSA-048**).

5.1.2 GDA Issues

304 There are no PSA related GDA Issues to be addressed before Consent will be granted for the commencement of nuclear island safety related construction. However, should there be design changes, or changes in other technical areas that have the potential to impact the PSA then the impact on PSA should be addressed. Should that impact be significant, the PSA will need to be updated and those new elements assessed.

6 REFERENCES

1 *PCSR UK EPR Pre-construction Safety Report – November 2009 Submission.* Submitted under cover of letter UN REG EPR00226N. 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Master Submission List. November 2009. TRIM Ref. 2011/46364.

2 *UK EPR Master Submission List*. November 2009. TRIM Ref. 2011/46364.

3 *ND BMS. Technical Reports.* AST/001 Issue 4. HSE. April 2010

4 *Safety Assessment Principles for Nuclear Facilities*. 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf.

5 *GDA Step 4 PSA Assessment Plan for the UK EPR*. HSE-ND Assessment Plan AR 09062 Revision 1. TRIM Ref. 2010/164508.

6 *IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design – Requirements.* NS-R-1 International Atomic Energy Agency (IAEA). Vienna 2000.

7 *Reactor Safety Reference Levels.* Issue 0. Western European Nuclear Regulators Association (WENRA). January 2008. http://www.wenra.org/dynamaster/file_archive/080121/1c826cfa42946d3a01f5ee027825eed6/List_of_reference_levels_January_2008.pdf

8 *ND BMS Technical Assessment Guide.* T/AST/030 Issue 3. HSE. February 2009.

9 *Step 3 Probabilistic Safety Analysis Assessment of the EDF and AREVA UK EPR*. HSE-ND Assessment Report AR 09/027. November 2009. TRIM Ref. 2009/335831.

10 *Risk Gap Analysis of UK EPR PSA for GDA.* ONR Assessment Note. Revision 0. July 2011. TRIM Ref. 2011/310239.

11 *Generic Design Assessment Review of UK EPR PSA Internal initiating events during full power operation.* P0636080002-3295. February 2011. TRIM Ref. 2011/197808

12 *Generic Design Assessment Step 4 Review of UK EPR PSA Accident Sequence Analysis.* P0636090001-3577. February 2011. TRIM 2011/197895.

13 *Generic Design Assessment Step 4 Review of UK EPR PSA* Systems Analysis. 0636090001-3810. January 2011. TRIM Ref. 2011/197747.

14 *Generic Design Assessment Step 4 Review of UK EPR PSA Data and Common Cause Failure Analysis.* P0636090001-3610. December 2010. TRIM Ref. 2011/197937.

15 *Generic Design Assessment Step 4 Review of UK EPR PSA Human Reliability Analysis.* P0636090001-3579. January 2011. TRIM Ref. 2011/197611.

16 *Generic Design Assessment Step 4 Review of UK EPR PSA Fire and Flood Analysis.* 0636090001-3809. January 2011. TRIM Ref. 2011/197707.

17 *Generic Design Assessment Step 4 Review of UK EPR PSA Other Hazards Analysis.* 0636090001-3685. January 2011. TRIM Ref. 2011/197654.

18 *Generic Design Assessment Step 4 Review of UK EPR PSA* Seismic Analysis. P0636090001-3684. January 2011. TRIM Ref. 2011/197967.

19 *Generic Design Assessment Step 4 Review of UK EPR PSA* Low Power and Shutdown Analysis. P0636090001-3698. January 2011. TRIM Ref. 2011/198022.

20 *Generic Design Assessment Step 4 Review of UK EPR PSA* Level 1 Results. 0636090001-3744. March 2011. TRIM Ref. 2011/197590.

21 *Generic Design Assessment Step 4 Review of UK EPR PSA* Level 2 Analysis. P0636090001-3699. February. TRIM Ref. 2011/198070.

22 *UK EPR Level 2 PSA Risk Spectrum model review (Lot 4)*. 32.800.076-R-001. November 2009. TRIM Ref. 2011/264440, 2011/264454 and 2011/264472.

23 *Review of Level 3 PSA for Generic Design Assessment Step 4 EDF/Areva EPR Reactor Design,* CRCE-EA-6-2011. Health Protection Agency Centre for Radiation, Chemical and Environmental Hazards. TRIM Ref. 2011/414211.

24 *C&I Back up system. Design Change Management Form.* UKEPR-CMF-014 Stage 2. EDF and AREVA. 30 June 2011. TRIM Ref: 2011/349776.

25 *Modifications to C&I Architecture. Design Change Management Form.* UKEPR-CMF-015 Stage 2. EDF and AREVA. 28 June 2010. TRIM Ref: 2011/94434.

26 *Control and Instrumentation architecture issues - RI-UKEPR-002*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00180R. 30 September 2009. TRIM Ref. 2009/386051.

27 *Step 4 Fault Studies – Containment and Severe Accident Assessment of the EDF and AREVA UK EPR™Reactor.* ONR Assessment Report ONR-GDA-AR-11-020b Revision 0. TRIM Ref. 2010/581403.

28 *Generic Design Assessment Design Basis Limits and Development of Plant Operating Limits and Maintenance Schedules*. July 2010. TRIM Ref. 2010/299034.

29 *Step 4 Cross-cutting Topics Assessment of the EDF and AREVA UK EPR™ Reactor* ONR Assessment Report ONR-GDA-AR-11-032 Revision 0 TRIM Ref 2010/581499

30 *HSE-ND Comments on EDF/AREVA's Proposed List of GDA Out-of Scope Items*. EPR0710N. 30 December 2010. TRIM Ref. 2011/503.

31 *Defining Initiating Events for Purposes of Probabilistic Safety Assessment*. IAEA TECDOC-719. ISSN 1011-4289. IAEA Vienna. September 1993. www-pub.iaea.org/MTCD/publications/PDF/te_719_web.pdf.

32 *Accident Sequence Evaluation Program: Human Reliability Analysis Procedure.* NUREG/CR-4772; SAND-86-1996. USNRC February 1987. http://www.osti.gov/bridge/servlets/purl/6370593-0eXswa/6370593.pdf.

33 *European Utility Requirements for LWR Nuclear Power Plants. Volume 2: Generic Requirements. Chapter 17: PSA Methodology*. Revision B. November 1995. www.europeanutilityrequirements.org/eur.htm.

34 *EDF and AREVA UK EPR - Schedule of Regulatory Observations Raised during Step 4*. HSE-ND. June 2011. TRIM Ref. 2010/600727.

35 *EDF and AREVA UK EPR - Schedule of Regulatory Observations Raised during Step 3.* HSE-ND. November 2009. TRIM Ref. 2009/358253.

36 *UK EPR Probabilistic Safety Analysis Level 1 Detailed Documentation*. NEPS-F DC 355. AREVA NP. 28 August 2008. TRIM Ref. 2011/85677.

37 *AREVA Application Public Revision 1 Chapter 19*. May 2009. adamswebsearch2.nrc.gov/idmws/ViewDocByAccession.asp?AccessionNumber=ML092450713.

38 *UK EPR MAAP4.07 Parameter File Development Model*. NEPS-F DC 517 Revision A. AREVA. 7 April 2010. TRIM Ref. 2011/92496.

39 *UK EPR MAAP4.0.7 Parameter File Development Geometry*. NEPS-F DC 518 Revision A. AREVA. 15 March 2010. TRIM Ref. 2011/92498.

40. *UK EPR MAA4.0.7 Parameter File Development Include Files*. NEPS-F DC 519 Revision A. AREVA. 7 April 2010. TRIM Ref. 2011/92499.

41 *Step 4 Fault Studies – Design Basis Faults Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-020a Revision 0. TRIM Ref. 2010/581404.

42 *Analysis of the Completeness of the Scope of Initiating Events for the GDA step 3 UK Probabilistic Safety Assessment*. NEPS-F DC 377 Revision B. 10 December 2009. TRIM Ref. 2011/86661.

43 *UK EPR OL3 – PSA Support Studies*. NEPR-F DC 241 Revision B. AREVA. 27 June 2008. TRIM Ref. 2011/92794.

44 *RISKSPECTRUM® Model for UK EPR.* Attachment 1 to Letter ND(NII) EPR00179N. Guidance Notes on Applying the Model and PSA Model Changes. Letter from UK EPR Project Front Office to ND. 23 September 2009. TRIM Ref. 2009/394793.

45 *Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment*. NEPS-F DC 191 Revision A. AREVA. TRIM Ref. 2011/92797.

46 *EPR Probabilistic Analysis of Accident Sequences Caused by Anticipated Transient Without Scram*, PSSE DC 901C Revision C. AREVA. October 2004. TRIM 2011/92866

47 *Synthèse des Critères de Succès pour les EPS de Niveau 1 Note*. EPRR/DC/1667 Revision B. FRAMATOME ANP. December 2001.

48 *Summary of the Input Data for the UK EPR Probabilistic Safety Assessment*. Letter from ND to UK EPR Project Front Office. NEPS-F DC 565 Revision A. 4 June 2010. TRIM Ref. 2010/245430.

49 *Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-022 Revision 0. TRIM Ref. 2010/581510.

50 *UKEPR: Description of the Control and Instrumentation Modelling in the PSA*. NEPS-F DC 576 Revision A. AREVA. 2 July 2010. TRIM Ref. 2011/92999.

51 *Probabilistic Justification of Non-Computerised Safety System*. NEPS-F DC 192 Revison A. AREVA. 4 September 2010. TRIM Ref. 2011/92798.

52 *Response to Regulatory Observation RO-UKEPR-047*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00467R. 6 July 2010. TRIM Ref. 2010/298203.

53 *Step 4 Human Factors Assessment of the EDF and AREVA UK EPR^TM Reactor*. HSE-ND Assessment Report ONR-D6-GDA-AR-11-028 Revision 0. TRIM Ref. 2010/581503.

54 *The SPAR-H Human Reliability Analysis Method.* NUREG/CR-6883 INL/EXT-05-00509. Idaho National Laboratory. August 2005. www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/cr6883.pdf.

55 *UK EPR Level 2 Supporting Human Reliability Analysis*. NEPS-F DC 527 Revision A. AREVA. 12 January 2010. TRIM Ref. 2011/92809.

56 *UK EPR Summary of the Input for the UK EPR Probabilistic Safety Assessment. NEPS-F DC 565 Revision A. AREVA. May 2010. TRIM Ref. 2011/92819.*

57 *Step 4 Structural Integrity Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-027 Revision 0. TRIM Ref. 2010/581504.

58 *Use of PSA insights to optimise STI of EPR safety functions*. EDF. 7-11 September 2008. TRIM Ref. 2010/497037.

59 *Common-Cause Failure Database and Analysis System: Event Data Collection, Classification and Coding*. NUREG/CR-6268, INEL/EXT-07-12969, Revision 1. September 2007. www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6268/.

60 *Response to RO-18*. Letter from ND to UK EPR Project Front Office. ND(NII) EPR0246R. 23 December 2009. TRIM 2009/506871.

61 *EPR Pre-Construction Safety Report Issue 03*. Chapters 15, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6 15.7. March 2011. TRIM Ref. 2011/204318, 2011/204319, 2011/204320, 2011/204321, 2011/228240, 2011/204323, 2011/204324, 2011/204325.

62 *UK EPR Level 2 Supporting Containment Fragility*. NEPS-F DC 526 Revision A. AREVA. December 2009. TRIM Ref. 2011/92807.

63 *UK EPR Level 2 Supporting Analysis-In-Vessel Recovery*. NEPS-F DC 548 Revision A. AREVA. June 2010. TRIM Ref. 2011/92815.

64 *UK EPR Level 2 Supporting Analysis – Hydrogen*. NEPS-F DC 540 Revision A. February 2010. TRIM Ref. 2011/92810.

65 *UK EPR Level 2 Supporting Analysis – Induced RCS Ruptures*. NEPS-F DC 541 Revision A. AREVA. February 2010. TRIM Ref. 2011/92811.

66 *UK EPR Level 2 Supporting Analysis – Vessel failure*. NEPS-F DC 567 Revision A. AREVA. June 2010. TRIM Ref. 2011/92820.

67 *UK EPR Level 2 Supporting Analysis – Long Term Containment Challenges*. NEPS-F DC 543 Revision A. AREVA. June 2010. TRIM Ref. 2011/92813.

68 *UK EPR Level 2 Supporting Human Reliability Analysis.* NEPS-F DC 527 Revision A. AREVA. January 2010. TRIM Ref. 2011/92809.

69 *UK EPR Level 2 PSA Supporting Severe Accident Analysis*. NEPS-F DC 458 Revision A. AREVA. August 2009. TRIM Ref. 2011/92802.

70 *New Nuclear Power Stations - Generic Design Assessment - Strategy for working with overseas regulators.* HSE-ND. March 2009. www.hse.gov.uk/newreactors/ngn04.pdf.

71 *RISKSPECTRUM® PSA Model for UK EPR GDA Step 4.* Attachment 1 to Letter ND (NII) EPR00860N. Letter from UK EPR Project Front Office to ND. May 2011. TRIM Ref. 2011/251161.

72 *Severe Accident Management OSSA FA3*. NEPS-F DC 457. June 2009, TRIM 2011/92207.

73 *EPR PRA inputs for MDEP Meeting*. Paris MDEP RPR Working Group. AREVA. May 2011. TRIM Ref. 2011/0316073.

74 *HSE-ND Comments on EDF/AREVA's Proposed List of GDA Out-of-Scope Items*. Letter from UK EPR Project Front Office to ND. ND(NII) EPR00710N. 30 December 2010. TRIM Ref. 2011/503.

75 *Generic Design Assessment Review of UK EPR PSA Quantification, Uncertainty and Sensitivity Analysis.* P0636090001-3700. February 2011. TRIM Ref. 2011/366489.

76 *Success Criteria for PSA UK EPR.* GRS-V-HSE-WP12,15 &15a-01. January 2011. TRIM Ref. 2011/109457.

77 *UK EPR Consolidated Pre-construction Safety Report – March 2011 Submission.* Detailed in EDF and AREVA letter UN REG EPR00997N. November 2011. TRIM Ref. 2011/552663.

78 *UK EPR Master Submission List.* UKEPR-0018-001, Issue 01, EDF and AREVA. November 2011. TRIM Ref. 2011/552512.

Table 1

Main GDA Supporting Documentation for PSA Considered During Step 4

Document Ref.	GDA Supporting Documentation Title
PCSR Chapter 15 Issue 4	PSA part of the PCSR
NEPS-F DC 355 C	PSA Level 1 Detailed Documentation
NEPS-F DC 377 B	Analysis of the Completeness of the Scope of Initiating Events for the GDA step 3 UK Probabilistic Safety Assessment
NEPS-F DC 191 A	Human Reliability Analysis appendix of the UK EPR Probabilistic Safety Assessment
NEPSF DC 458 A	PSA Level 2 – Supporting Severe Accident Analysis
NEPSF DC 462 A	PSA Level 2 – Source Term Analysis
NEPSF DC 459 A	PSA Level 2 – Supporting Severe Accident Calculation
NEPSF DC 460 A	PSA Level 2 – Source Term Calculation
NEPSF DC 493 A	PSA Level 2 – Source Term Methodologies and Identification of Key Uncertainties
UK_HSE2.RSD	Step 3 PSA model, September 2009 version (RiskSpectrum® model)
NEPS-F DC 565	Summary of the input data for the UK EPR Probabilistic Safety Assessment
NPSFP10154, EPR00294R & EPR00544R	Fire modeling in the PSA
NEPS-F DC 576	Report to answer HSE concerns on C&I modeling. Includes R0 47 response
ENFPFC0200484	EPR PSA – Assessment of initiating event frequencies
NEPR-F DC 241 B FIN UK	OLEVEL 3 – PSA support studies (success criteria)
PSRR DC 25 B UK	PSA support studies (ATWS)
EPSE DC 833 F	EPR – Probabilistic Analysis of Accident Sequences Caused by Interfacing Loss of coolant Accidents
PSSE DC 901 C	EPR – Probabilistic Analysis of Accident Sequences Caused by Anticipated Transients Without Scram
NGPS4 2003 en 0120B	TR04/138 Heterogeneous boron dilution – PSA demonstration of dilution accident practical elimination
NFPMR DC 1048	Reactor Consequences Assessment of a RPV Closure Head Accidental Drop during Lifting Operation, TR N° 98
NEPS-F DC 526	PSA Level 2 - Containment Fragility
NEPS-F DC 527	PSA Level 2 - HRA
NEPS-F DC 517, 518,519	MAAP 4.0.7 parameter file Development, (model, geometry, input files)
NEPS-F DC 548	UK EPR Level 2 Supporting Analysis – In-Vessel Recovery,

Table 1

Main GDA Supporting Documentation for PSA Considered During Step 4

Document Ref.	GDA Supporting Documentation Title
NEPS-F DC 540	UK EPR Level 2 Supporting Analysis – Hydrogen
NEPS-F DC 541	UK EPR Level 2 Supporting Analysis – Induced RCS Ruptures
NEPS-F DC 567	UK EPR Level 2 Supporting Analysis – Vessel Failure
NEPS-F DC 543	UK EPR Level 2 Supporting Analysis – Long Term Containment Challenges
NEPS-F DC 458	UK EPR Level 2 Supporting Severe Accident Analysis
NEEL-F DC 87 A UK	UK EPR GDA Seismic Fragilities of Primary Equipment for Use in Seismic Margin Assessment
UK EPR SMA GDA Report Rev 0_CCI	Seismic Fragilities of Structures and Equipment of UK European Pressurized Reactor for Use in Seismic Margin Assessment".
NEPS-F DC 192	PSA Justification of NCSS
PCSR Chapter 15 Issue 03.	Step 4 PSA model (consolidated)
	Consolidated PCSR (Submitted March 2011)

Table 2

Relevant Safety Assessment Principles for Probabilistic Safety Analysis Considered During Step 4

SAP No. and Title	Description	Interpretation	Comment
FA.10 Fault analysis: PSA Need for a PSA	"Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis"	This principle sets the framework and requirements for a PSA study. The overriding aim of the PSA assessment is to assist ND judgements on the safety of the facility and whether the risks of its operation are being made as low as reasonably practicable.	Addressed in Section 4 & 5 of this report. The need for PSA has been recognised from the outset, and this assessment report concludes that the PSA is suitable and sufficient for GDA, hence the SAP is met.
FA.11 Fault analysis: PSA Validity	"PSA should reflect the current design and operation of the facility or site"	This principle establishes the need for each aspect of the PSA to be directly related to existing facility information, facility documentation or the analysts' assumptions in the absence of such information. The PSA should be documented in such a way as to allow this principle to be met.	Addressed in Section 2.3 of this report. The PSA provided is applicable to the current stage of the design, so the SAP is met.
FA.12 Fault analysis: PSA Scope and extent	"PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site"	In order to meet this principle the scope of the PSA should cover all sources of radioactivity at the facility (e.g. fuel ponds, fuel handling facilities, waste storage tanks, radioactive sources, reactor core, etc), all types of initiating faults (e.g. internal faults, internal hazards, external hazards) and all operational modes (e.g. nominal full power, low power, shutdown, start-up, refuelling, maintenance outages).	Addressed in Section 4.2 of this report. The scope of the PSA is adequate and the SAP is met.

Table 2

Relevant Safety Assessment Principles for Probabilistic Safety Analysis Considered During Step 4

SAP No. and Title	Description	Interpretation	Comment
FA.13 Fault analysis: PSA Adequate representation	"The PSA model should provide an adequate representation of the site and its facilities"	The aim of this principle is to ensure the technical adequacy of the PSA. Inspectors should review PSA models, data and results to be satisfied that the PSA has a robust technical basis and thus provides a credible picture of the contributors to the risk from the facility.	Addressed in Section 4.1 and 4.3 to 4.19 of this report Section 4 of this report is almost entirely devoted to this SAP, and Section 5 concludes the PSA is adequate for GDA. Hence the SAP is met. There are however a number of findings that will need to be addressed for compliance with this SAP at later site licensing stages, such as fuel load.
FA.14 Fault analysis: PSA Use of PSA – FA.14	"PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities"	The aim of this principle is to establish the expectations on what uses the duty-holders should make of the PSA to support decision-making and on how the supporting analyses should be undertaken.	Addressed in Section 4.16 this report. There is clear evidence that the PSA has been used in the design process and in this respect the SAP is adequately met at this point. Many of the assessment findings are aimed at ensuring the PSA is developed sufficiently to aid detailed design and operational safety decisions in future.

Table 2

Relevant Safety Assessment Principles for Probabilistic Safety Analysis Considered During Step 4

<table>
<tr><th>SAP No. and Title</th><th>Description</th><th>Interpretation</th><th>Comment</th></tr>
<tr><td rowspan="2">Numerical Targets NT.1</td><td>Target 7: Individual risk to people off the site from accidents
Target 8: Frequency dose targets for accidents on an individual facility – any person off the site</td><td>BSL 10^{-4}/yr BSO 10^{-6}/yr
<table>
<tr><th></th><th>BSL</th><th>BSO</th></tr>
<tr><td>Offsite dose 0.1-1mSv</td><td>1</td><td>10^{-2}</td></tr>
<tr><td>Offsite dose 1-10mSv</td><td>10^{-1}</td><td>10^{-3}</td></tr>
<tr><td>Offsite dose 10-100mSv</td><td>10^{-2}</td><td>10^{-4}</td></tr>
<tr><td>Offsite dose 100-1000mSv</td><td>10^{-3}</td><td>10^{-5}</td></tr>
<tr><td>Offsite dose >1000mSv</td><td>10^{-4}</td><td>10^{-6}</td></tr>
</table></td><td rowspan="2">Addressed in Section 3 of this report.
The results produced by EDF and meet the BSOs for Targets 7, 8 and 9.
Chapter 17 makes use of the results to give a conservative estimate an individual risk, which is below the BSO.
The PSA related elements of NT1 are met</td></tr>
<tr><td>Target 9: Total risk of 100 or more fatalities</td><td>BSL 10^{-5}/yr BSO 10^{-7}/yr</td></tr>
</table>

Table 2

Relevant Safety Assessment Principles for Probabilistic Safety Analysis Considered During Step 4

SAP No. and Title	Description	Interpretation	Comment
Numerical Targets NT.2	Sufficient control of radiological hazards at all times	Sufficient protection based on engineering and operational features. Avoidance of high point in time risks that would exceed BSLs if evaluated as continuous risks.	Addressed in Section 4.11 & 4.16 of this report. The main times where there will be elevated risk (above the average) are during maintenance and test and in shutdown operating modes. The PSA contains explicit modelling of these matters and there is sufficient information to conclude that point in time risk estimates do not approach BSLs, Hence NT2 is met

Table 3

EDF and AREVA PSA Results for the UK EPR

Item	EDF and AREVA Target (per yr)	Result (per yr)
Core Damage Frequency (CDF) internal events	1×10^{-6}	5.31×10^{-7}
CDF ext hazards	5×10^{-6}	7.59×10^{-8}
CDF internal hazards	1×10^{-6}	1.01×10^{-7}
Offsite dose 0.1-1mSv	1×10^{-2}	1.4×10^{-3}
Offsite dose 1-10mSv	1×10^{-3}	1.3×10^{-5}
Offsite dose 10-100mSv	1×10^{-4}	1.2×10^{-6}
Offsite dose 100-1000mSv	1×10^{-5}	1.5×10^{-7}
Offsite dose >1000mSv	1×10^{-6}	8.0×10^{-8}
Individual risk	1×10^{-6}	$1.7\text{x } 10^{-7}$
>100 Fatalities	1×10^{-7}	8.0×10^{-8}

PSA results, extracted from the relevant sections of the consolidated PCSR (Ref. 61), reflect the latest update of the PSA to include all the PSA related matters that have been resolved during the GDA process.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-1. General Expectations		
Table A1-1.1 Approaches and Methodologies		
AF-UK EPR-PSA-001	The licensee shall develop the UK EPR PSA into a fully symmetric model.	Fuel load
Table A1-1.2 PSA Scope		
AF-UK EPR-PSA-002	The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.	Fuel on-Site
Table A1-2. Level 1 PSA		
Table A 1-2.1 Identification and Grouping of Initiating Events		
AF-UK EPR-PSA-003	The licensee shall provide FMEAs to support derivation of initiating events (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
AF-UK EPR-PSA-004	The licensee shall ensure that those IEs related to plant systems that are not yet included due to lack of design detail are incorporated into the PSA as more information becomes available.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
Table A1-2.2 Accident Sequence Development: Determination of Success Criteria		
AF-UK EPR-PSA-005	The licensee shall ensure that all of the success criteria underpinning the UK EPR PSA should be best estimate.	Fuel load
AF-UK EPR-PSA-006	The licensee shall ensure that the design and operational assumptions used in the non UK EPR studies (Ref. 43) are adhered to and confirmed for the UK EPR, or alternatives justified.	Fuel on-Site

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UK EPR-PSA-007	The licensee shall provide and implement a procedure to ensure that, for Phase 2 of the UK EPR project, clear traceability and alignment of the success criteria in the PSA supporting documentation is maintained by adherence to a suitable Living PSA control process (out of scope for GDA - see Section 2.3.6). RO-UKEPR-68 is relevant here.	Nuclear island safety related concrete
AF-UK EPR-PSA-008	The licensee shall ensure that the PSA documentation for the UK EPR PSA contains clear and explicit links between the grace periods for human action and the supporting analysis and the timing of cues for those actions.	Fuel on-Site
AF-UK EPR-PSA-009	The licensee shall ensure that, in the development of best estimate success criteria noted in AF-UK EPR-PSA-005 all of the relevant phenomena are shown to be bounded, and that the success sequence end points are justified as real successes, not simply time bound because there has been no failure in 24 hr.	Fuel on-Site
Table A1-2.3 Accident Sequence Development: Event Sequence Modelling		
AF-UK EPR-PSA-010	The licensee shall ensure that the detailed Level 1 PSA document (Ref. 36) (out of scope for GDA – see Section 2.3.6) is updated so that it is fully consistent with the current PSA model (Ref. 71).	Nuclear island safety related concrete
AF-UK EPR-PSA-011	The licensee shall ensure that the process for maintaining and developing the PSA model configuration and supporting document trail (see RO-UKEPR-68 discussion) is retained post GDA, or an equivalent process put in its place. (Out of scope for GDA – see 2.3.6).	Nuclear island safety related concrete
AF-UK EPR-PSA-012	The licensee shall ensure that all the support systems (e.g. HVAC) are incorporated into the PSA, both as potential initiators (see 4.4) and their role during accident sequences. The role of the operator in HVAC recovery should be examined closely.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UK EPR-PSA-013	The licensee shall ensure that future development of the PSA properly accounts for multiple demands on safety valves and should make use of current best estimate reliability data.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UK EPR-PSA-014	The licensee shall provide and implement a consistent process to ensure capture of the assumptions that are currently dispersed throughout the PSA reports and its supporting documentation and gather them together in a single place within the PSA documents. This should be done in a systematic and traceable way, and the assumptions sentenced as part of a future PSA development (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
Table A1-2.4 System Analysis		
Same as finding in A1-2.3 AF-UK EPR-PSA- 010	The licensee shall ensure that the detailed Level 1 PSA document (Ref. 36) (out of scope for GDA – see Section 2.3.6) is updated so that it is fully consistent with the current PSA model (Ref. 71).	Nuclear island safety related concrete
Same as finding in A1-2.3 AF-UK EPR-PSA-011	The licensee shall ensure that the process for maintaining and developing the PSA model configuration and supporting document trail (principles established in the RO-UKEPR-68 response) is retained post GDA, or an equivalent process put in its place (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
AF-UK EPR-PSA-015	The licensee shall ensure that the modelling of the C&I in the PSA is reviewed and if necessary amended as the details of the C&I systems evolve. This should include explicit consideration of C&I based initiating events (including spurious signals) and the potential for dependencies such initiators and the safety mitigation systems and potential dependencies between the cues for operator action and signals used for the automatic C&I.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UK EPR-PSA-016	The licensee shall ensure that future updates of the model explicitly include the actuators associated with the compact model, and also take account of any CCF related to the actuators.	Fuel load
Table A1-2.5 Human Reliability Analysis		
AF-UK EPR-PSA-017	The licensee shall ensure that substantiation for the HRA in the form of task analysis, procedures and training is provided to underpin the numerical HFE values used in the PSA The substantiation should include further consideration of pre-initiating HFEs and the potential for HFE dependencies (pre & post fault).	Fuel load (but needs to be consistent with HF findings in Ref. 53)
AF-UK EPR-PSA-018	The licensee shall ensure that Level 2 PSA sensitivities to individual and collective HEPs are used to provide insights into the development of the EPR severe accident guidance (OSSA).	Fuel load (but needs to be consistent with HF findings in Ref. 53)
Table A1-2.6 Data Analysis		
Table A1-2.6.1 Initiating Event Frequencies		
AF-UK EPR-PSA-019	The licensee shall ensure that the generic LOOP frequency is confirmed to be bounding in comparison to a site specific value or demonstrate that a site specific frequency is acceptable in risk terms.	Nuclear island safety related concrete
AF-UK EPR-PSA-020	The licensee shall ensure that the PSA uses an appropriate LOOP frequency for the site and justified ratios used for long and short duration LOOP, both in terms of initiating event and conditional LOOP.	Fuel load

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-2.6.2 Component Failure Rates		
AF-UK EPR-PSA-021	The licensee shall ensure that the test intervals underpinning EDF derived component failure probabilities (out of scope for GDA – see Section 2.3.6) are provided consistently with EMIT programmes or alternatives justified.	Nuclear island safety related concrete
AF-UK EPR-PSA-022	The licensee shall ensure that the implicit rather than explicit inclusion of test intervals (Ts) are revisited for the data inputs to the Operational PSA post GDA.	Fuel load
Table A1-2.6.3 Unavailabilities Due to Testing and Maintenance		
AF-UK EPR-PSA-023	The licensee shall ensure that the basis for the time periods assumed for maintenance and test unavailabilities is justified and that those time periods, together with the “allowable” maintenance combinations assumed in the PSA are incorporated into the Technical Specifications and EMIT programmes, or alternative values / strategies justified.	Fuel load
Table A1-2.6.4 Common Cause Failures (CCF)		
AF-UK EPR-PSA-024	The licensee shall use the PSA to explore intersystem CCF effects and to inform the incorporation of appropriate defences (e.g. detailed design, procurement strategy and operational features such as test and maintenance). Where appropriate the intersystem CCFs should be included explicitly in the model.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UK EPR-PSA-025	The licensee shall ensure that the use of global CCF parameters in the PSA model are reviewed and where appropriate that the parameters are replaced with available system or component specific values.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UK EPR-PSA-026	The licensee shall ensure that CCF uncertainty is included in the PSA post GDA.	Fuel load

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UK EPR-PSA-027	The licensee shall provide and implement a procedure to ensure that CCF related assumptions are captured and used for future development of testing, maintenance strategies and completion of system designs post GDA (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
Table A1-2.7 Analysis of Hazards		
Table A1-2.7.1 General		
AF-UK EPR-PSA-028	The licensee shall ensure that the dependency between a LOOP and extreme weather events is taken into account and if necessary the PSA amended.	Fuel load
AF-UK EPR-PSA-029	The licensee shall ensure that the generic loss of ultimate heat sink frequency is confirmed as bounding in comparison to a site specific value or demonstrate that a site specific frequency is acceptable in risk terms.	Nuclear island safety related concrete
AF-UK EPR-PSA-030	The licensee shall ensure that the PSA uses an appropriate loss of ultimate heat sink frequency for the site.	Fuel load
AF-UK EPR-PSA-031	The licensee shall ensure that hazards such as internal explosion, turbine missiles and animal infestation are considered and if necessary included in the PSA model.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
AF-UK EPR-PSA-032	The licensee shall ensure that the screening criteria used in the GDA PSA are confirmed to bound specific site hazard characteristics and include in the PSA any hazards and combination of hazards that have been screened in.	Nuclear island safety related concrete

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-2.7.2 Analysis of Internal Fires		
AF-UK EPR-PSA-033	The licensee shall consolidate the assumptions made in the existing PCSR internal fire analysis in one location, and provide appropriate justification, reference, discussion of the effect of each assumption on the analysis and consider them as potential input to the full scope Fire PSA to be carried out post GDA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
Same as finding in A1-1.2 AF-UK EPR-PSA-002	The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.	Fuel Load
AF-UK EPR-PSA-034	The licensee shall develop a full scope, Internal Fire PSA as the detailed design evolves (e.g. systematic inclusion of fire fighting system fault trees, inclusion of all individual buildings and compartments).	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
Table A1-2.7.3 Analysis of Internal Flooding		
AF-UK EPR-PSA-035	The licensee shall consolidate the assumptions made in the existing PCSR internal flooding analysis in one location, and provide appropriate justification, reference, discussion of the effect of each assumption on the analysis and consider them as potential input to the full scope Flooding PSA to be carried out post GDA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site
Same as finding in A1-1.2 AF-UK EPR-PSA-002	The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.	Fuel Load
AF-UK EPR-PSA-036	The licensee shall develop a full scope Internal Flooding PSA as the detailed design evolves.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-2.7.4 Seismic Analysis		
AF-UK EPR-PSA-037	The licensee shall provide a Seismic PSA for the site. The seismic analysis should take account of consequential hazards that might be caused by a seismic event, such as fire or flooding, and if appropriate include them in the PSA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site (includes polar crane, RPV installation and installation of DGs)
AF-UK EPR-PSA-038	The licensee shall ensure that the impact of seismic faults during shutdown is addressed in a consistent manner with other contributions to the risk during shutdown.	Fuel Load
Table A1-2.8 Low Power and Shutdown Modes		
Same as finding in A1-1.2 AF-UK EPR-PSA-002	The licensee shall ensure that the scope of the PSA is expanded to include hazards, such as fire and flooding during non power operating states.	Fuel Load
Same as finding in A1-1.2.7.4 AF-UK EPR-PSA-038	The licensee shall ensure that the impact of seismic faults during shutdown is addressed in a consistent manner with other contributions to the risk during shutdown.	Fuel Load
AF-UK EPR-PSA-039	The licensee shall ensure that the actual RCS water inventories for shutdown POS need is established and if necessary the analysis repeated to inform appropriate operating restrictions.	Fuel load
Table A1-2.9 Uncertainty Analyses, Quantification and Interpretation of the Level 1 PSA Results		
AF-UK EPR-PSA-040	The licensee shall ensure that full consideration of parametric uncertainty is included the PSA.	Fuel load

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Same as finding in A2-1.4 AF-UK EPR-PSA-014	The licensee shall provide and implement a consistent process to ensure capture of assumptions that are currently dispersed throughout the PSA reports and its supporting documentation and gather them together in a single place within the PSA documents. This should be done in a systematic and traceable way, and the assumptions sentenced as part of a future PSA development (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
AF-UK EPR-PSA-041	The licensee shall ensure that long term faults should be properly incorporated into the overall PSA as the detailed design evolves so that the importance of long term recovery measures (such as repair of Diesel Generators and supporting the emergency feed water system with fire fighting water) is captured and taken into account in future procedures and decision making.	Fuel load
Table A1-3. Level 2 PSA		
AF-UK EPR-PSA-042	The licensee should ensure that a UK-EPR specific containment structural analysis is performed which addresses all potential modes of containment failure, including penetration and leakage failures.	Containment Pressure test
AF-UK EPR-PSA-043	The licensee shall update the Level 2 PSA model to ensure consistency with the current Safety Injection Severe Accident Management Strategy.	Fuel Load

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-4. Level 3 PSA		
AF-UK EPR-PSA-044	The licensee should ensure that the Level 3 PSA is developed to modern standards, in particular by placing less reliance on design basis dose assessments and by fully incorporating probabilistic factors such as weather. For each new plant the Site-specific Level 3 PSA will need to incorporate site specific source term and release frequency analyses together with site specific dispersion and consequence modelling parameters (such as weather data and distribution of population and agriculture) for all releases.	Fuel load
Table A1-5. Overall Conclusions from the PSA		
Same as finding in A1-1.4 AF-UK EPR-PSA-011	The licensee shall ensure that the process for maintaining and developing the PSA model configuration and supporting document trail (principles established in the RO-UKEPR-68 response) is retained post GDA, or an equivalent process put in its place (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
Same as finding in A2-1.4 AF-UK EPR-PSA-014	The licensee shall provide and implement a consistent process to ensure capture of the assumptions that are currently dispersed throughout the PSA reports and its supporting documentation and gather them together in a single place within the PSA documents. This should be done in a systematic and traceable way, and the assumptions sentenced as part of a future PSA development (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete
AF-UK EPR-PSA-045	The Licensee shall provide and implement the procedure to maintain the PSA and keep it Living. This should include PSA task procedures and methodologies. (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business

Probabilistic Safety Analysis – UK EPR

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UK EPR-PSA-046	The Licensee shall provide and implement a procedure for the use of the PSA to support all aspects of design and operation of the NPP (out of scope for GDA – see Section 2.3.6).	Nuclear island safety related concrete

Notes

1 The Assessment Finding milestones relate to completion, the activity to satisfy the milestone will obviously need to start earlier and will also need to fulfil SAP FA.10 requirement that sufficient PSA is performed as part of the design development.

2 It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

3 For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Probabilistic Safety Analysis – UK EPR

There are no GDA Issues for this topic area.