Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 PROBABILISTIC SAFETY ANALYSIS OF THE EDF AND AREVA UK EPR

DIVISION 6 ASSESSMENT REPORT NO. AR 09/027-P

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This report provides an overview of the Nuclear Directorate's (ND) Step 3 Generic Design Assessment (GDA) of the Probabilistic Safety Analysis (PSA) discussed in EDF and AREVA's PCSR (*UK EPR Pre-Construction Safety Report*, UK EPR-0002-132 Issue 02, EDF and AREVA, June 2009); it identifies the standards and criteria adopted in the assessment and then goes on to detail individual findings and draws general conclusions for Step 3 of the GDA process.

For GDA Step 3 the PSA is not being assessed in its entirety, rather it is the arguments that support high level claims (assessed in Step 2 (*ND Division 6 AR 08/011 EDF/AREVA Step 2 PSA Assessment*)) that are being assessed, and in Step 4 the evidence supporting these claims and arguments will be examined. For PSA, 'arguments' has been broadly interpreted as being the methods, techniques and scope of the PSA.

Scope of Assessment

EDF and AREVA have submitted a full scope, modern PSA in support of the UK EPR which covers all modes of operation, includes consideration of internal and external hazards and the effect of preventative maintenance. There are necessarily some areas where the analysis is incomplete or at an early stage, since detailed design information is not yet available, but these are identified within the PSA.

The PSA assessment has been carried out using ND's PSA guide (*ND BMS, Technical Assessment Guide* T/AST/030, Issue 3, HSE, February 2009) to identify potential shortfalls. For the main part my concerns arose because the required depth of information was not contained in the submitted documents and or the reference trail to that information was not clear. These shortfalls have led to the issue of a number of Technical Queries (TQs) and 3 Regulatory Observations (ROs). In all cases there has been a positive response by EDF and AREVA to the TQs and ROs.

In support of ND's Control & Instrumentation (C&I) assessment (*ND Division 6 AR 09/038 Step 3 Control and Instrumentation Assessment of the EDF and AREVA UK EPR*), the impact of different levels of numerical reliability and independence of the computer based reactor protection systems has been explored using the PSA model. Some of these 'sensitivity' runs give results where some of ND's numerical targets are not met, underlining the importance of resolving the C&I Regulatory Issue (RI) (*EDF and AREVA UK EPR - Schedule of Regulatory Issues Raised during Step 3*, HSE-ND, TRIM Ref. 2009/358254) and ensuring that the PSA is quantified using justifiable inputs

During GDA Step 3 a more detailed review (GDA Step 4 level) of the initiating event analysis was undertaken. This review involved not only consideration of documents submitted with the PCSR, but examination of detailed supporting evidence at AREVA's offices. Although there is further confirmatory work required in response to ND's TQs in this area, it was clear that the initiating event identification process for the UK EPR design conforms with current PSA standards and is satisfactory.

Conclusions

The PSA produced by EDF and AREVA covers the areas I would expect to see in the scope of a nuclear power plant PSA. For the most part the methods and techniques used by EDF and AREVA are acceptable. The numerical risk estimates produced by the PSA are generally better than the Basic Safety Objectives in the SAPs Numerical Targets.

EDF and AREVA have committed to make improvements to the UK EPR C&I architecture and we will need to assess the impact of these improvements on the PSA. In the event that revised PSA results exceed those quoted in the PCSR, we may need to revisit the ALARP (As Low As

Reasonably Practicable) arguments. Similarly any other potential engineering or operational shortfalls identified during the assessment may require further ALARP justification.

So far no PSA related Regulatory Issues have been identified, and EDF and AREVA's readiness to address the ROs is encouraging. Overall I see no reason on PSA grounds why the UK EPR should not proceed to Step 4 of the GDA process.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ASEP	Accident Sequence Evaluation Program
BMS	(Nuclear Directorate) Business Management System
CCF	Common Cause Failure
CDES	Core Damage End States
CDF	Core damage Frequency
CET	Containment Event Trees
DBA	Design Basis Accident
EA	The Environment Agency
EAL	Emergency Action Level
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EG&G	Edgerton, Germeshausen, and Grier Inc know as EG&G a division of URS Corporation
FMEA	Failure Modes Effects Analysis
FV	Fussel-Vesely
GDA	Generic Design Assessment
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
IE	Initiating Event
ISLOCA	Interfacing System LOCA
LHSI	Low Head Safety Injection
LOCA	Loss Of Coolant Accident
LOOP	Loos Of Offsite Power
LUHS	Loss Ultimate Heat Sink
MAAP	Modular Accident Analysis Programme
MCs	Minimum Cut Set
MDEP	Multi-national Design Evaluation Panel
MGL	Multiple Greek Letter
MHSI	Medium Head Safety Injection
MOV	Motor Operated Valve
ND	The (HSE) Nuclear Directorate
PCER	Pre-construction Environment Report
PCSR	Pre-construction Safety Report

LIST OF ABBREVIATIONS

POS	Plant Operation State
PSA	Probabilistic Safety Analysis
RCS	Reactor Cooling System
RI	Regulatory Issue
RIA	Regulatory Issue Action
RIF	Risk Increase Factor
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
SAP	Safety Assessment Principle
SEL	Seismic Equipment List
SGTR	Steam Generator Tube Rupture
SMA	Seismic Margin Assessment
SOV	Solenoid Operated Valve
SSC	System, Structure and Component
STUK	The Finnish nuclear safety authority
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
US NRC	The United States Nuclear Regulatory Commission
WENRA	The Western European Nuclear Regulators' Association

TABLE OF CONTENTS

1 INTRODUCTION

1 Nuclear Directorate's (ND) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) safety submission. As with the other technical areas, the Probabilistic Safety Analysis (PSA) assessment is following the claims-argument-evidence hierarchy. In Step 2 the claims made by the RP were examined, in Step 3 the arguments that underpin those claims have been examined and in Step 4 the evidence that supports those claims and arguments will be assessed. The Step 2 assessment (Ref. 13) concluded that EDF and AREVA had provided an adequate overview of the approach, scope, criteria and results of the Level 1+ PSA they had produced at that time. The Step 2 assessment also noted some points, or observations that were intended to be picked up in Step 3 and the way these have been carried forward is summarised in Annex 1.

2 This report deals with the GDA Step 3 assessment of the PSA reported in Chapter 15 of the PCSR (Ref. 1) and supporting submissions provided by EDF and AREVA for the UK EPR. The PCSR was updated to Issue 2 at the end of June 2009, so the bulk of the assessment reported here was carried out against Issue 1 of this document. Some of the key changes between Issue 1 and Issue 2 of the PCSR are noted in this report and the revised numerical results at Issue 2 have been quoted.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

3 This section of the report covers 3 main areas: a short summary of the RP's submission, identification of the standards and criteria used to assess the PSA and thirdly the assessment findings.

2.1 Requesting Party's Case

4 Probabilistic studies were carried out during the UK EPR design process to support and optimise the design of systems and processes. EDF and AREVA claim that this has allowed a well-balanced system and process design to be achieved. They also consider that it has also provided a reasonable assurance that the plant complies with the stated safety objectives. In the PSA, fault trees are used to estimate the failure probability of the system missions. Event trees are used for estimating the Core Damage Frequency (CDF) due to each initiating event in the Level 1 PSA and further event trees are used to analyse potential failure sequences that could give rise to releases in the Level 2 PSA.

5 The scope of the PSA includes consideration of internally initiated faults, internal and external hazards and includes non-power operating states. An allowance for plant unavailability due to maintenance is also included in the PSA and Common Cause Failure (CCF) is modelled in the fault trees using Multiple Greek Letter (MGL) parameters. Human reliability is modelled explicitly in the PSA and makes use of the ASEP methodology (Ref. 14).

6 Initiating faults have been derived using the method proposed by IAEA (Ref. 15) which includes the use of past PSAs, operational feedback data and for new systems Failure modes and effects analysis. The component reliability data used in the PSA has been derived mainly from French and German operational experience feedback.

7 The PSA is physically large, and contains 159 event trees for the Level 1 PSA and a further 92 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.

8 PSA results are reported against a number of targets and a range of these are presented in Table 1 below.

Table 1: UK EPR PSA Targets and Results

Item	EDF and AREVA Target (per yr)	Result (per yr)
Core Damage Frequency (CDF) internal events	1×10^{-6}	2.77×10^{-7}
CDF ext hazards	5×10^{-6}	5.07×10^{-8}
CDF internal hazards	1×10^{-6}	3.98×10^{-8}
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}	8.8×10^{-7}
Offsite dose 100-1000mSv	1×10^{-5}	6.5×10^{-7}
Offsite dose >1000mSv	1×10^{-6}	5.6×10^{-8}
>100 Fatalities	1×10^{-7}	6×10^{-8}

2.2 Standards and Criteria

9 The main standards and criteria used are ND's Safety Assessment Principles (SAPs) (Ref. 4). The PSA strategy (Ref. 8) identified SAPs FA.10 to FA.14 and NT.7 to NT.9 as the relevant parts of that document. Also of importance in the strategy are relevant parts of IAEA standards (Ref. 9) and the WENRA reference levels (Ref. 10).

10 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. 7) and it is this guide that provides the principle means for assessing the PSA in practice. The assessment has been conducted in accordance with ND's Business Management System (Ref. 2 and Ref. 3).

11 For Step 3 it is important to note that the PSA is not being assessed in its entirety; rather it is the arguments that support high level claims (assessed in Step 2 – Ref. 13) on how the PSA SAPs etc. will be met that are being looked at, and in Step 4 the evidence supporting these claims and arguments will be assessed.

12 For PSA 'arguments' has been broadly interpreted as being the methods, techniques and scope of the PSA and although attempts have been made to have restricted assessment to these matters, it is not always a simple matter to disentangle methods from the data, judgements and implementation by EDF and AREVA. The latter constitute the evidence that will be looked at in detail in Step 4 but there are inevitably some overlaps in this report.

2.3 Nuclear Directorate Assessment

13 The Step 3 PSA assessment has followed the PSA strategy that was set out at the end of Step 2 (Ref. 8), and has been carried out by a high level review against the tables contained in Annex 1 of ND's PSA guide (Ref. 7). This review has been undertaken with the assistance of Technical Support Contractors who have carried out their work under

direction and supervision by ND. For each of the relevant 'assessment expectations' in the tables, a view on the adequacy or otherwise of the documentation has been taken. Where the documentation is considered less than adequate, this has led to or will lead to dialogue with EDF and AREVA. For the main part such views arise because the depth of information is simply not visible and/or the reference trail to such information has not been identified in sufficient detail. This leads in many cases to there being an inadequate justification in the submitted documents of the assumptions made during the conduct of the PSA. These shortfalls have generally led to the issue of Technical Queries (TQs). In some limited cases the nature of the shortfall between the PSA and ND's expectations is such that Regulatory Observations have been issued and these are discussed below. In addition to the high level review against the TAG, assistance has been provided to other assessment areas in ND, notably the C&I assessment (Ref. 12).

14 A summary of the Step 3 assessment findings are listed below and are supported by the detailed assessment reported in Annex 3. The format of Annex 3 follows Annex 1 of the PSA guide (Ref. 7). Where a topic has not been addressed in Step 3 this is clearly stated.

15 PSA strengths:

- Overall modelling approach is sound.
- PSA modelling software is state of the art.
- Accident sequence (event trees) analysis is comprehensive.
- Seismic analyses (seismic margins method) is robust, though it is not a full seismic PSA.
- Level 2 PSA analysis is comprehensive.

16 Limitations in the PSA and PSA Documentation:

- Justification for the key assumptions is not explicit.
- Details of supporting Thermal/Hydraulic studies are not presented or referenced.
- Some outdated generic data sources have been used.
- The process to capture PSA assumptions for future changes to operations or design is not described.
- Simplified fire & flooding analyses has been performed.
- Human Reliability Analysis documentation is sparse and does not address initiators with unique conditions (fires, flooding and during shutdown states).
- Common cause failure data is not well supported and unjustified simplifying assumptions are used.
- A clear definition of system and component boundaries is missing.
- The submitted documentation for Initiating Event (IE) analyses and data sources is inadequate.

17 In general the limitations noted above require further documentation, updates to the PSA input parameters and in some cases the analysis itself needs to be refined to make the PSA suitable to support any future operation of the UK EPR. In many cases TQ responses addressing these limitations have been received and these will be taken into account during Step 4. But it is emphasised that these limitations are not fundamental flaws in the PSA model provided by EDF and AREVA. As noted in the 'strengths' of the PSA, the main features and structure of the PSA are considered to be adequate. Annex 3 concentrates on those areas of the PSA where further justification or refinement of the

analysis is needed rather than going in to detail on those elements found to be acceptable.

18 On the last bullet in para. 16 above, point it is worth noting that during Step 3 a more detailed (Step 4 level) review of the Initiating event (IE) analysis to identify a full range of initiators has been carried out. This review involved not only consideration of the documentation provided in support of the PCSR, which as noted above has some limitations, but examination of detailed supporting evidence (not formally referenced in the PCSR) at AREVA's offices. Although there is significant further confirmatory work required in response to TQs, I am able to conclude that identification process for IEs conforms to current PSA standards, and is adequate to identify IEs for the UK EPR design.

19 The PSA results depend, among many other things, on the reliability and degree of independence between the computerised C&I systems involved in delivering reactor protection. During the Step 3 C&I assessment (Ref 12) both of these elements have been challenged and the potential impact of different levels of numerical reliability and independence has been explored using the PSA model. Some of these 'sensitivity' runs produced results that did not meet EDF and AREVA's own Safety Design Objectives (SDOs). In some cases the SAP Target 8 Basic Safety Objective (BSO), was not met and in the most extreme trial the SAP Target 9, BSL, was challenged. In this latter case it is acknowledged that the numerical estimate contains some significant conservative assumptions and that there may be legitimate scope for refining that result. Nevertheless the studies serve to underline the importance of resolving the C&I issue and ensuring that the PSA is quantified using justifiable inputs.

20 **Requirements of GDA guidance**. The guidance to RPs on GDA required them, at Step 3, to include a PSA. The PCSR and supporting documentation fulfil that requirement.

21 **HSE undertakings for Step 3.** For PSA items 3.15, 3.22, and 3.23 of the GDA guidance (Ref. 21) are the main points to consider.

- 3.15 is addressed by this report;
- 3.22 is addressed by TQs and ROs raised to date;
- 3.23 is addressed by comparison with numerical targets (note these may change as a result of ongoing design and assessment);
- 3.26. PSA is not a major overlap area for the Environment Agency (EA);

22 **Use of other regulators information** Insights from other regulators looking at EPR variants have been gained through the Multi-national Design Evaluation Panel (MDEP). The main inputs so far are from the Finnish nuclear safety authority, STUK and US NRC. STUK had raised questions on L2 PSA modelling suitability and possible quantification errors. Although the UK variant is unlikely have these problems, being a more recent analysis, STUK's comments have been taken seriously and work has been commissioned to examine this issue. US NRC has provided a list of their questions and the responses they received related to the US EPR. All of the US NRC information will be reviewed and where relevant included in ND's assessment. I expect to share and discuss the results of the Step 3 PSA assessment with the other members of MDEP.

23 **Plans for Step 4 assessment.** It is intended that the Step 4 assessment will look in detail at all of the areas reviewed at a high level in Step 3 using the additional information received as a result of the TQs and ROs as a basis together with any further planned submissions from EDF and AREVA. The first stage will be a Step 3 assessment 'wrap up meeting' meeting with EDF and AREVA which will summarise the work done so far, and aim to agree and assign priorities to the work needed to address the TQs and ROs. All of the areas in the TAG will be addressed, though this does not mean that each and every

fault tree, event tree, item of reliability data or supporting analysis will be reviewed. Instead the aim is to establish that implementation of the methods and techniques used is adequate by reviewing the procedures used, and then establishing, on a sample basis, that the procedure delivers adequate results.

24 **Related research.** I have not identified any PSA related research requirements at this stage.

25 **Technical Queries (TQs)**. During Step 3 I have issued many TQs covering all aspects of the PSA (Ref. 11). All of the TQs issued up to August 2009 have been responded to and the others have been acknowledged by EDF and AREVA. The responses will form the basis for ongoing assessment (this of course does not preclude further TQs during Step 4 should they be needed, or indeed issue of RO or RIs).

26 **Regulatory Observations (ROs).** In a few areas it has been clear that there is a shortfall that cannot be clarified by a TQ, or the TQ response reveals such a shortfall. In such cases I have issued a Regulatory observation (Ref. 16). The ROs issued have been:

- Maintenance Unavailability (RO-UKEPR-16) – the PSA results were quoted assuming all plant is available and the impact of maintenance was only addressed in a sensitivity study.
- Fire PSA (RO-UKEPR-18) – the reliability of fire suppression systems was subsumed into initiating event frequencies, so potential dependencies between safety systems *might* be overlooked.
- Omission of 2A LOCA (RO-UKEPR-29) - The large double guillotine failure of primary circuit cooling loops (2A-LOCA) had been excluded from the PSA on the grounds it was 'remote' and there was ample plant to deal with it.

27 In each case there has been a positive response from EDF and AREVA. The most recent issue of the PCSR (Ref. 1) now includes 2A-LOCA analysis, and the overall results include consideration of plant being unavailable due to preventative maintenance activity, so the results are now more representative. The detailed implementation of these upgrades will be reviewed in Step 4. For the Fire PSA RO, EDF & AREVA have accepted the point and the next revision of the PSA is intended to disentangle the fire suppression reliability from the initiating event frequency. This should improve the transparency of this element of the analysis, but again I will need to review the implementation of this improvement.

28 **Regulatory issues (RIs)**. In the PSA area I have not identified any failings or shortfalls of sufficient magnitude to warrant the issue of an RI for the PSA itself. I have, however provided support to the ND's assessment effort related to the RI issued on C&I (Ref. 12). In this regard I have reviewed sensitivity studies provided by EDF and AREVA exploring the impact of a range of assumptions on C&I reliability and have initiated dialogue with EDF and AREVA on the modelling of C&I within the PSA. This activity is ongoing and will to continue into Step 4.

29 **Potential exclusions.** There are no PSA based exclusions at this time.

3 CONCLUSIONS AND RECOMMENDATIONS

30 EDF and AREVA have produced a large, modern-standards, PSA to support the PCSR submitted to ND.

31 The reports produced by EDF and AREVA have coverage of all of the areas I would expect to see in the scope of an Nuclear Power Plant (NPP) PSA and the risk estimates they produce are generally better than the BSOs in the SAPs Numerical Targets. With the exception of the C&I reliability issue, I have not yet identified any matters that challenge this conclusion. EDF and AREVA have committed to make improvements to the UK EPR C&I architecture and we will need to assess the impact of these improvements on the PSA. In the event that revised PSA results exceed those quoted in the PCSR, we may need to revisit the ALARP (As Low As Reasonably Practicable) arguments in Chapter 17 of the PCSR.

32 For the most part the methods and techniques used by EDF and AREVA are acceptable in principle, though I have not yet fully explored implementation of these methods; this will be done in Step 4.

33 Although the PSA model is large and comprehensive, the supporting documentation has a number of shortfalls in terms auditable trail to the supporting evidence for the claims and arguments in the reports and it is this evidence trail that I will be seeking to address in Step 4. Indeed many of the TQs raised during the Step 3 review of the PSA have been aimed at identifying the information and answers to questions needed for Step 4.

34 So far no PSA related RIs have been identified, and EDF and AREVA's readiness to address the ROs is encouraging.

35 Hence, there are currently no identified PSA related impediments to licensing of the UK EPR.

Recommendation 1: I recommend that assessment of the UK EPR PSA should progress into Step 4 of the GDA process.

4 REFERENCES

1 *UK EPR Pre-Construction Safety Report.* UK EPR-0002-132 Issue 02 EDF and AREVA June 2009.

2 *ND BMS, Assessment Process.* AST/001 Issue 2 HSE February 2003.

3 *ND BMS, Guide: Assessment Process.* G/AST/001 Issue 2 HSE February 2003.

4 *Safety assessment principles for nuclear facilities.* (2006 Edition Version 1) HSE December 2006.

5 *ND BMS, Assessment - Assessment Reports.* AST/003 Issue 2 HSE October 2003.

6 *ND BMS, Guidance: Assessment Reports.* G/AST/003 Issue 2 HSE October 2003.

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

8 *New Reactor Build Step 3 PSA Strategy.* ND Division 6 Assessment Report No. AR08/029 HSE March 2008. TRIM Ref. 2008/317683.

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

10 *Reactor Safety Reference Levels,* Issue O, Western European Nuclear Regulators Association (WENRA), January 2008.

11 *EDF and AREVA UK EPR - Schedule of Technical Queries Raised during Step 3.* HSE-ND November 2009. TRIM Ref. 2009/358252.

12 *Generic Design Assessment – New Civil Reactor Build. Step 3 Control and Instrumentation Assessment of the EDF and AREVA UK EPR.* ND Division 6 Assessment Report No. AR09/038 HSE November 2009. TRIM Ref. 2009/339202.

13 *New Reactor Build – EDF / AREVA Step 2 PSA Assessment.* ND Division 6 Assessment Report No. AR08/011 HSE March 2008. TRIM Ref. 2008/86480.

14 *Accident Sequence Evaluation Program (ASEP). Human Reliability Analysis (HRA). Procedure* NUREG/CR-4772 US NRC 02-1987.

15 *Defining Initiating Events for Purposes of Probabilistic Safety Assessment.* TECDOC-719 IAEA Vienna 1993.

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

17 *UK EPR Probabilistic Safety Analysis Level 1 Detailed Documentation.* Document Number NEPS-F DC 355 AREVA NP August 2008.

18 *European Utility Requirements for LWR Nuclear Power Plants. Volume 2: Generic Requirements. Chapter 17: PSA Methodology.* Revision B, November 1995.

19 *EDF and AREVA UK EPR - Schedule of Regulatory Issues Raised during Step 3.* HSE-ND November 2009. TRIM Ref. 2009/358254.

20 *The SPAR-H Human Reliability Analysis Method.* NUREG/CR-6883 Idaho National Laboratory August 2005.

21 *Nuclear power station generic design assessment – guidance to requesting parties.* (Version 3) HSE August 2008.

Table 2: HSE – ND Safety Assessment Principle Compliance – Probabilistic Safety Analysis

SAP	EDF and AREVA	Comment
FA.10 – FA.14	PCSR Chapter 17 includes EDF and AREVA commentary on meeting of the SAPs.	At this point the PSA is considered to be broadly compliant with the SAPs, but there is a significant amount of assessment to do before I can give an overall judgement.
NT.1, parts 5-9 But see note below	Targets 5 &6: no explicit analysis, but argument provided that the risk is bounded by offsite figures in Targets 7 and 8 for hypothetical offsite person due to the conservative assumptions made in the latter calculations. Target 7: Individual risk (offsite) – EDF and AREVA calculate a figure of 4.2 x 10^{-7}/yr, which is claimed to be conservative. This meets their SDO-5 of 1 x 10^{-6}/yr. Target 8: Dose Frequency SDO-6 seeks results that are below the BSOs in UK SAPs Target 9 – Societal Risk. SDO-9 is equivalent to the BSO in the UK SAPs. EDF and AREVA quote results that the risk of >100 fatalities is lower than 1 x 10^{-7}/yr.	For GDA purposes I consider this argument sufficient. The individual risk estimate is below the BSO in the SAPs, and therefore acceptable. The results presented by EDF and AREVA (see table 1) are below the BSOs in the SAPs and are therefore acceptable. The results presented by EDF and AREVA (see table 1) are below the BSO in the SAPs and are therefore acceptable.
NT.2		Chapter 17 description doesn't really cover the intent. In reality this SAP is intended to control configuration changes for operational plant so for GDA the results are indicative that the SAP can be met in operation. The PCSR (15.7 part 6) does, however include consideration of instantaneous risk and shows variations of CDF that remain within the EDF and AREVA's original target value, so this is an encouraging result, though I will want to look in more detail at this.

Note on numerical results: This table has been compiled assuming that EDF and AREVA can provide evidence to support the claims and arguments and that evidence will be assessed in Step 4. If unresolved, the C&I reliability issue could have a significant impact on the results quoted in Table 1 and on the SAPs table above.

Annex 1 – Progress with Items Identified During GDA Step 2 Assessment

Between Step 2 and Step 3, EDF and AREVA provided completely new PSA documentation in Issue 1 of the PCSR and the associated supporting PSA information. This new information has in a number of instances meant that the points raised in Step 2 have been overtaken by events. Nevertheless it is worth providing a brief update on those points and a pointer to where the topic is covered in this Step 3 report, as follows.

Step 2 Assessment Item	Resolution, or place where the item is noted in this Step 3 assessment report
Break preclusion approach to 2A LOCA (i.e. not included)	The argument for exclusion of the 2A LOCA provided in Issue 1 of the PCSR was not convincing and an RO was issued. EDF and AREVA have subsequently included such an analysis in Issue 2 of the PCSR, so the point is resolved.
Bounding of event groups	This has been looked at in detail in Step 3 and further work carried by EDF and AREVA in response to TQs (see 1.2.1 of Annex 3 of this report).
Treatment of Uncertainties & sensitivity.	Issue 1 of the PCSR and its supporting documentation provide detailed results and there are sections dealing with both uncertainty and sensitivity. Any further follow up will be noted in 1.2.9 of Annex 3 of this report.
Initiating event frequency judgements	There was little information on initiating event frequency derivation in the Step 2 information. Issue 1 of the PCSR provided much more detail. I have l raised TQs on this matter and will go into greater detail still in Step 4. Follow up will be in 1.2.6.1 of Annex 3 of this report.
Justification of CCF exclusion	As in other areas, Issue 1 of the PCSR and its supporting documentation provide much more detail. Some CCFs have been excluded, though the rationale for this is still not satisfactory and TQs have been issued requesting further information. The responses are expected to form part of the basis for the Step 4 assessment and this will be tracked under part 1.2.6.4 of Annex 3 of this report.
More on non-core sources of radioactivity	The PCSR addressed this point by inclusion of non-core sources. It was raised as a SAPs compliance issue, and I intend to review some of the non-core faults associated with the fuel pool in detail in Step 4.

Annex 2 – Probabilistic Safety Assessment – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
None.				
Regulatory Observations				
RO-UKEPR-16	15 July 2008	Scope of PSA (Results of the PSA should include allowance for maintenance)	Closed (though further points on detailed modelling of maintenance may be raised).	N/A
RO-UKEPR-18	5 Nov 2008	Fire PSA – Numerical Combination of Fire Frequency and failure probability of fire protection/suppression	Ongoing.	Step 4
RO-UKEPR-29	24 Feb 2009	Omission of2A-LOCA from the PSA	Ongoing (but PSA now includes 2A LOCA, waiting for some further details).	Step 4

Annex 3

Detailed Assessment Against T/AST/030 Expectations

The assessment results are presented below under the headings of Annex 1 of ND's PSA Technical Assessment Guide, T/AST/030 (Ref. 7). Points arising from this step of the assessment where I have sought clarification or additional information have been the subject of TQs or ROs and will be tracked to completion through ND's GDA administrative systems (Refs 11 and 16).

Unless otherwise stated references to section or chapter numbers relate to the PSA report (Ref. 17) supporting the PCSR.

Ref. 7, Table A1-1.1 - Approaches and methodologies

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

2 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 calculations. Whilst this will not invalidate high level numerical targets, 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 any potential nuclear power plant (NPP) in the UK. This is not a barrier to GDA confirmation but it is something that a potential utility would need to address during licensing in Phase 2 (site licensing).

Ref. 7, Table A1-1.2 PSA Scope

3 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. All sources of radioactivity are included in the PSA documentation. In principle the scope of the PSA is adequate, though the detailed Step 4 review may identify some omissions.

4 Section 1.1 indicates that the sources of identified radioactive releases are:

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

5 The last two sources are not considered in the PSA Level 1, but are considered in the offsite PSA (Section 3.1), which is satisfactory.

6 PSCR sub-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.

7 Section 1.3 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.

8 PSCR sub-chapter 15.1 (Ref. 1) indicates 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.

9 Section 1 indicates that the risk for internal hazards were not assessed quantitatively (considered negligible) for shutdown states (CA, CB, D and E). It is argued that fire and flooding events would be detected with a higher probability and longer grace periods lead to more reliable measures to cope with internal fire or flooding events. Neglecting to model these initiators may result in failure to discover plant design or operational vulnerabilities that may require plant design modifications or additional operational requirements or restrictions.

Ref. 7, Table A1-1.3 Freeze date

10 The PSA freeze date has been not been stated but EDF and AREVA will re-issue the PSA supporting document at the end of Step 4. The Step 3 assessment has focussed primarily on Issue 1 of the PCSR, though the results quoted are from Issue 2 as they take account of new analysis in response to PSA related ROs.

Ref. 7, Table A1-1.4 Computer codes and inputs

11 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. The software is considered acceptable.

12 The other computer codes and inputs used in the EPR Level 1 and Level 2 PSA are not well described or referenced in the documentation, nor is there any discussion on the experience of the analysts, the uncertainties and limitations associated with the selected computer codes, or details of the thermal-hydraulic plant models (e.g. nodalization) in the reviewed PSA documentation.

Ref. 7, Table A1-2 Leve1 1 PSA

Ref. 7, Table A1-2.1 Identification and grouping of IEs

13 During Step 3 a more detailed (Step 4 level) review of the Initiating event analysis carried out to identify a full range of initiators has been undertaken. This review involved not only consideration of the documentation provided in support of the PCSR, but examination of supporting evidence at AREVA's offices. Although there is some further confirmatory work required in response to TQs, I am able to conclude that identification process for IEs conforms to current PSA standards, and is adequate to identify IEs for the UK EPR design.

14 PCSR subchapter 15.1 indicates that a systematic and exhaustive search for potential initiating events following the guidance in IAEA-TECDOC-719 (Ref. 15) was performed and that the process included the following elements:

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

.

15 Generally, the source documents for identifying the potential IEs to be included in the UK EPR PSA have been identified. However, in almost all cases the information taken from these documents is inadequately described. Furthermore, how this information is utilized to identify and select IEs for inclusion in the UK EPR PSA study is generally not provided. The information taken from the referenced sources should be identified and a discussion on how this information was used to support IE selection should be included in the UK EPR PSA documentation.

16 Individual initiating events are not clearly defined and characterised (i.e. their causes and impact on plant) in the PSA since the specific IEs (and their characteristics) that have been assigned to each identified IE group are not systematically discussed.

17 The process for grouping initiating faults in the documentation reviewed in Step 3 is not clear (i.e. the grouping criteria and the mapping to derive the final initiating fault groups). Only a limited description/discussion of the grouping process is presented. The documentation should provide a list of the individual IEs included in the PSA and to which IE group each individual IE is assigned and the reason(s) for assigning specific individual IEs to a specific group. This discussion should include the IE group characteristics and the characteristics of the individual IE to be assigned to the group.

18 As a consequence of the current lack of transparency in the grouping process it is not possible at this stage to determine if each initiating fault group is represented by the most onerous fault or if the initiating fault groups have been defined in a way that vulnerabilities are masked. EDF and AREVA do actually have this information and they are currently preparing further supporting documentation.

Ref. 7, Table A1-2.2 Accident sequence development & success criteria

19 For each initiating event (fault) group, the safety functions, the systems which can perform each of the functions, and any need for operator intervention, is 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.17).

20 ND's PSA guide, T/AST/030, (Ref. 8) requires that 1) sufficient and representative thermal-hydraulic analyses have been performed to demonstrate that a given system response will prevent the safety limit being exceeded, 2) the thermal-hydraulic, neutronics (and any other) analyses used for derivation of success criteria have been performed on a best-estimate basis and are specific to the facility, 3) timing for operator actions is justified (e.g. by sufficient and representative thermal-hydraulic analyses) and 4) the thermal-hydraulic, neutronics (and any other) analyses used for derivation of success criteria are thoroughly documented and fully traceable. However, there appears to be little or no discussion of the thermal-hydraulic, neutronics (and any other) analyses performed to support the success criteria development. The information provided in the PSA documentation is insufficient to allow identification of the specific analysis supporting each success criteria claim.

21 Section 3.2.3 indicates that in most cases, the required capacity of a system (i.e. the success criteria) is determined by the system design requirements. Realistic success criteria are claimed to have been used. However, most of them are based on calculations made for the worst-case scenarios and may therefore be conservative.

22 The limiting conditions defined (parameter thresholds) for the success/failure (for example, cladding temperature, coolant system pressure, coolant system level, enthalpy in fuel pellets, containment temperature and pressure, etc) are provided in Table 3.2-1. However, no or limited discussion is provided to explain or justify the thresholds given in this Table.

Ref. 7, Table A1-2.3 Accident sequence development & Event sequence modelling

23 The general assumptions for the event tree development for each class of initiating event are adequately defined and justified. Additional more detailed assumptions are provided for individual initiators within these categories.

24 The level at which the event tree headings are defined is discussed. The event tree headings can be a status of a safety function, a status of a system, a basic event occurrence, or an operator action. Generally, the event tree headings functions/success criteria/dependencies, etc. are well presented and discussed.

25 A consequence or end state associated with each Level 1 accident sequence are identified and defined. General end states developed for the UK EPR PSA include Success, Core Damage, Fuel Damage, and Steaming. The latter 2 end state categories are specific to fuel pool sequences.

26 The evolution of the sequence of events following the representative initiator from each initiating fault group is described. The (physical) parameters and actuation signals that initiate reactor trip and initiate the required safety systems are identified and discussed. Required operator actions are discussed. Although the timing of required operator actions is generally provided the source of these timing values is often not identified. The overall timing of sequence progression and the time of required system operation does not appear to be as clearly delineated.

27 No discussion was found showing the relationship between the various headings/nodes of the event tree and the relevant thermal-hydraulic analyses performed to support the event sequence modelling. The link between the various headings/nodes of the event trees and the relevant thermal-hydraulic analyses performed to support the event sequence modelling should be transparent. As discussed previously there is a lack of traceability of the thermal-hydraulic analyses that supporting event sequence definition, success criteria, human reliability analyses, etc.

28 The mission times for the functions represented by each event tree branch are not stated explicitly. However, the success criteria tables (e.g. Table 6.3.1-6 in Ref. 17) associated with each event tree specify the functions and systemic success criteria for each function. In general, the EPR PSA model uses a component failure-to-run mission time of 24 hours, in line with standard international practice. For certain sequences and components shorter or longer mission times may be utilized (e.g. for short term LOOP the mission time is generally two hours). The mission time for any basic event that is than 24 hours is coded into the event name code. However, no listing of basic events with mission times different than 24 hrs was found in the documentation. Hence, there was also no information as to how these mission times were determined.

29 Due to the absence of fully developed procedures, typical PWR actions and operating procedures adapted to the EPR design have been used in the UK EPR PSA. Operator actions and human error estimates have been identified and included in the accident sequence analysis.

30 There seemed to be no discussion on how EDF and AREVA will use the findings from the PSA for procedure development.

Ref. 7, Table A1-2.4 System Analysis

31 The PSA results depend, among many other things, on the reliability and degree of independence between the computerised C&I systems involved in delivering reactor protection. During the Step 3 assessment (Ref.12) ND has challenged both of these elements and the impact of different levels of numerical reliability and independence has been explored using the PSA model. Some of these ‘sensitivity’ runs produced results that did not meet EDF and AREVA’s own safety design objectives (SDOs). In some

cases the SAP Target 8 BSO was not met and in the most extreme trial the SAP Target 9 BSL, was challenged. In this latter case it is acknowledged that the numerical estimate contains some significant conservative assumptions and that there may be legitimate scope for refining that result. Nevertheless the studies serve to underline the importance of resolving the C&I issue and ensuring that the PSA is quantified using justifiable inputs.

32 The major components associated with each system model are described in the various system analyses appendices in Ref. 17. These appendices also describe the connection of a specific system to other systems. Simplified flow diagrams are provided in each appendix showing major system components and (mechanical) system interfaces. However, only a limited discussion is generally provided as to which system model contains specific components (e.g. valves) at system interfaces.

33 No discussion of what constitutes the boundary for each component was found. Component boundaries should be identified for all component types (and failure modes) that are included in the PSA to assure consistent modelling among system analysts and to assure that these boundaries are consistent with the failure rate data sources that are utilized for the PSA.

34 Section 4.2.2.4 indicates that the unavailability of components due to scheduled test and maintenance is not included in the PSA model. It is further stated that the consideration of maintenance is part of the sensitivity analysis. For sensitivity analysis purpose, maintenance of a system train is modelled in the fault tree.

35 Pre-accident errors are considered in the system analyses. Their treatment is discussed in Section 4.4.1. However, failure to perform a critical step in a calibration procedure (calibration of C&I or of an actuator or a pressure setting of a relief valve) is not assessed as pre-accident human error in the PSA. The calibration errors are assessed in the failure rate of the instrumentation component.

36 The general approach to the treatment of post accident human errors is discussed in Section 4.4.2. Post-accident tasks include diagnosis tasks and post-diagnosis tasks.

37 Common cause failures (CCF) are used to represent all dependencies which are not explicitly included in the event tree and system models. Specific CCFs considered for each system are described in the system analyses appendices of Ref. 17. This includes a discussion of the components included in CCF groups and the quantification method. The failure modes for the components considered for CCF are generally not specified in the system analyses sections nor are the size combinations of the CCF events specified, (i.e. for a CCF group of 4, if 2 of 4, 3 of 4, 4 of 4 are modelled). CCFs are not modelled on groups of identical components in different systems (Intersystem CCFs are not modelled).

38 Generally in the Level 1 analyses structural failures are only considered for external hazards and are treated as initiating events. The screened-in external hazards identified in the EPR PSA potentially leading to structural failures are earthquakes and aircraft crashes (Section 6.5). For other causes of potential structural failures including dropped heavy loads and internal missiles, Section 6.4.6. states that *"Due to the low initiating event frequency (<1 x 10^{-6}/ry) and the results of the structural analysis confirming that the residual heat removal function remains available, heavy load drop is screened out from the present PSA analysis"*. No reference is provided. Section 6.4.5 presents a qualitative argument for not including (screening out) internal missile hazards from the PSA.

39 The system analyses discussed in the system analysis appendices of Ref. 17 generally assume that the failure of passive components, (e.g. pipes), is negligible compared to failures of active components, (e.g. pumps). Table 4.6-1 indicates that passive components: pipes, tanks, heat exchangers, vessels are not assumed to be impacted by fire events. Reference to a suitable source such as NUREG/CR-6850 could be added to

support these assumptions. In addition, verification that these general assumptions can be applied to all passive components in the EPR should be provided.

40 Assumptions regarding fault tree system modelling are contained in the system analyses appendices in the Section 'Assumptions and Limitations' of Ref. 17. There does not appear an upfront discussion of general modelling assumptions related to system fault tree modelling. Each system has its own discussion and these sections do not present a detailed discussion of the justification for the assumptions.

41 Table 4.2-3 provides the basic event coding scheme and the codes for component failure modes. The list of failure modes appears reasonably complete. However, this table does not indicate which specific component types are modelled for which specific failure modes. Section 4.2.2.4 states that the fault tree model considers failures of the components themselves in their specific failure modes and to simplify and reduce the size of the fault trees, some failure modes are excluded due to their low probability in comparison with other failure modes. However, the specific failure modes included or excluded for each component type are not specified in this section. In addition, for certain components failure modes that might be expected are not listed in Table 5.1-1 (e.g. - there is no failure to close (re-close) for safety valves). Plugging type failure modes appear to be included only for filter type components (Table 5.1-1).

42 No discussion of circular logic or logic loops (whether they exist, which parts of the model they impact, or how they were addressed) was located in Ref. 17.

43 The systems analyses appendices provide: a description of each modelled system including its principal components, the system functions and operational modes, system operation and configurations under normal power operating conditions (state A), normal shutdown (states B &C), maintenance shutdown (state D), refuelling shutdown (state E), core unloaded (state F) and for a variety of transient conditions including conditions leading to reactor trip. Simplified flow diagrams are also provided for each system. These diagrams identify the interfaces to other systems. A spot check of the CCW Systems Analysis description (Appendix SA7) was performed. The CCW flow diagram (Figure SA7-1) contains all of the principal components listed as included in the model in Section SA7.1.1. The CCW simplified flow diagram appears to provide an adequate high level description of the system boundary and interfaces to other systems. During Step 4 confirmation will be required that the simplified diagrams adequately represent the system model. The document text (i.e. text in systems analyses appendices) does not explicitly address the locations (e.g. last component included within a system boundary). However, the simplified flow diagrams do appear to provide this information. Potential gaps or overlaps in system model boundaries will be investigated during the detailed review.

44 The success criteria tables (e.g. Table 6.3.1-6 in Ref. 17.) associated with each event tree specify the functions and systemic success criteria for each function conditioned on the IE and the prior event tree success and failures. System specific success criteria are specified in the detailed system analysis Appendices for the front line systems. These tables give the success criteria for each IE/event tree where system operation is questioned. A spot check of the Section 6.3.1-6 success criteria with the success criteria specified for the SIS system for a medium break LOCA (PBM1) in Appendix SA3 appear to be consistent.

45 For support systems such as the Ultimate Cooling Water System (UCWS) (Appendix SA14) there are no top events that appear in the event trees. Top events, which are transfer gates to other fault trees without a direct link to any event tree, do not have assigned success criteria. The detailed PSA report (Ref. 17.) does not describe the analyses of the necessary support systems (see for example Appendix SA14).

46 Support system information is provided in the systems analyses appendices section for the major components in a system in a general way. It would be to include a table listing

47 For component unavailabilities the systems analyses appendices contain only very limited information on the assumed test schedules for only a limited number of components in each system. These assumptions appear to be included to support the PSA quantification task and may or may not reflect the actual future test schedules. However, no information was located on the process to be used to assure that future changes to the test schedules reflect assumptions made in the PSA.

48 Section 5.4.2 states: *"The maintenance scenario takes into account the following preventive maintenance on certain groups of systems. These groups are determined by a functional analysis (see Table 5.4-1) and based on a preliminary EPR maintenance schedules".* Section 5.4.2.1 provides the assumed maintenance schedule for each system group and systems associated with each group for power operation (state A). Maintenance is performed on a single train for each system in a system group simultaneously. However, no information was located on the process to be used to ensure that the PSA assumptions are captured in the future development of the maintenance schedule.

49 Each system analysis Appendix presents the fault tree modelling assumptions associated with the system model. Assumptions that simplify the model are presented. Justification for each assumption is generally not discussed. This will be followed up in Step 4.

50 In general, it appears that failure of C&I components are not considered as a contribution to HF-errors. Section 4.3.1.3.1 states: *"The contribution of C&I to the failure of the operator control functions is negligible with regards to the contribution of the operator errors"*. This will need to be justified and will be followed up in Step 4.

51 Generally, in the Level 1 PSA EPR, repairs are not considered. Recovery of failed hardware components appears to be considered in only a limited manner.

52 A table of fault tree top events is provided in the system analyses Appendices. These tables provide a description of the top event, the associated event tree(s) and transfers to other fault tree system models. However, a comprehensive list of basic events and intermediate events (i.e. gates) does not appear to have been included in the PSA documentation, either for the overall model or associated with individual fault tree system models.

Ref. 7, Table A1-2.5 HRA

53 The Human Reliability Analysis has been carried using the Accident Sequence Evaluation Programme (ASEP) (Ref. 14) method. The method includes pre-accident tasks and post-accident tasks and is acceptable in principle. There do not appear to be any clearly excessive numerical claims being made on the operator. It also appears that the major types of HFEs have been included in the model. Detailed review of individual human error calculations, assumptions etc. will be carried out during Step 4 when EDF and AREVA have provided additional information and justification.

54 Pre-initiating fault HFEs include errors in positioning actuators (valves, circuit breaker racked-out). Failure to perform a critical step in a calibration procedure (calibration of C&I or of an actuator, pressure setting of a relief valve) is not assessed as pre-accident human error in the PSA. The calibration errors are assessed in the failure rate of the instrumentation part.

55 Section 4.4.1.2 indicates that there are four categories of recovery factors with non-recovery probabilities ranging from 1×10^{-3} to 1 depending on the extent of indication,

alarms, testing, associated with the physical parameters related to the required human action. However the basis for these non-recovery probabilities is not given.

56 There is no evidence of a process to ensure that the assumptions regarding tests, maintenance tasks or operational realignments that could lead to pre-initiating fault HFEs are captured in all future developments.

57 Similarly, HFE specific information, for each post-initiating fault HFE (involving failure to respond to procedural steps, equipment failures, alarms or other cues) has not been provided in the supplied documentation. Hence, assumptions regarding the cues available to the operator are not identified. Consequently, a process has not been identified to ensure that these assumptions are captured in the future development of procedures and completion of design.

58 Systematic analyses of each human action to determine the appropriate HEP for the action is not reported and there is no evidence that task analyses were performed.

59 Detailed descriptions of the HRA calculations were not included, or referenced in the documentation. No specific discussion of HRA related to Low Power and Shutdown Events was found nor was any specific discussion of HRA related to External Hazards IEs found.

Ref. 7, Table A1-2.6 Data Analysis

Ref. 7, Table A1-2.6.1 Initiating event frequencies

60 Section 3.4.1.1.3 indicates the following process for evaluation the frequencies of IEs:

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

61 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 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 generally assessed using expert judgement.
- For the initiating events resulting from component failure: the frequency is calculated from reliability data on the relevant component.

62 The majority of the data for similar plant designs appears to come from the French 1300 MW PWR (or the 900 MW PWR). However, details of this data are not provided in the PSA documentation.

63 LOCA frequencies were generally taken from NUREG/CR-6928, Industry - Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, 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 get a slightly higher frequency. There are similar issues with the medium LOCA frequencies.

64 It is indicated in Table 3.4-6 that the IE frequencies for small break LOCAs for shutdown states CA, CB, D and E were taken from NUREG/CR-6928. However, NUREG/CR-6928 explicitly states that *"Low power and shutdown IEs are not addressed"*.

65 A number of IE frequencies (e.g. loss of condenser vacuum and LOOP) are derived from the 1995 European Utility Requirements for 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 justification for using IE frequencies from a superseded version of the EUR document is not discussed.

66 For many situations where fault trees are identified as being the source for the IE frequency (see Table 3.4-6). The validity of these fault trees will be assessed in Step 4.

Consequential Initiating Events

67 Section 3.4.1.5.3 addresses the potential loss of main grid due to a sudden loss of the connection to the grid (consequential LOOP). The conditional probability of a LOOP of $1x10^{-3}$ is claimed to be derived from British operating experience feedback. However, no reference to the data source was provided. Similarly there is no basis given for the ratio of short to long duration LOOP.

68 Section 3.4.1.3.2 indicates that the conditional probabilities of a SGTR have been agreed between EDF and French Safety Authorities (IRSN). A TQ was raised and further information provided to support the numerical values and this information will be assessed during Step 4.

Ref. 7, Table A1-2.6.2 Component failure rates

69 The data section in the PSA simply quotes sources and there is no discussion of component populations and no apparent recognition of the importance of establishing component boundaries. Other important omissions are the rationale for source selection and precedence, and on occasions where expert judgement is cited there is no reference trail, it is just a statement. Error factors are assigned but no rationale is offered for why they are appropriate.

70 Component categories assigned reliability data are shown in Table 5.1-1. Neither the characteristics of each category nor why specific subsets of component types are modelled using different data sources than the overall generic component categories are discussed.

71 No discussion of the subcomponents included within the component boundary of each component type group was found. In addition, there is no assurance that the generic data source component boundary is consistent with the PSA modelling assumptions.

72 The system analyses appendices generally assume that the failure of passive components, (e.g. pipes), is negligible compared to failures of active components, (e.g. pumps).

73 Generally only limited information is provided on structural analyses performed to support the PSA. The methodology used for the calculation of structural failure probabilities is generally not discussed.

74 Section 4.3 indicates that the role played by the Instrumentation and Control system is modelled in the PSA by using a specific C&I reliability model called ‘Compact Failure Model’. The compact failure model provides a decoupling of C&I reliability studies and plant PSA modelling by the introduction of fixed numerical values for I&C unavailability in plant PSA. It should be noted that the C&I is the subject of a Regulatory issue by ND’s C&I specialists. The outcome of this work could significantly impact on the C&I PSA models.

75 Although it is stated that the C&I reliability studies have been performed there are no references to these studies.

76 Mission times are discussed and generally a 24 hour time is used in line with international practice. ND normally like to see some arguments that a safe stable situation has been reached at the 24hr point, not that the accident sequence has not yet reached core damage. EDF and AREVA do in fact look at longer mission times so they are aware of this issue.

Ref. 7, Table A1-2.6.3 Unavailability Due to Test & Maintenance

77 There is no description of the events that represent unavailability due to test and maintenance and they were not included in the baseline results at Issue 1 of the PCSR though a sensitivity analysis does look at this topic. This is not satisfactory since the PSA results for comparison with targets should account for all contributions and without appropriate allowance for unavailability due to maintenance will be optimistic. An RO (Ref. 16) was raised to deal with this matter and as a result Issue 2 of the PCSR includes maintenance in the baseline PSA results. This is clearly acceptable in principle, though the way in which maintenance is included has not been reviewed, this will be done in Step 4 and may, as with all Step 4 assessment activities, lead to further TQs and ROs.

Ref. 7, Table A1-2.6.4 Common Cause Failure

78 Common Cause Failure (CCF) methodology is based on an extended Beta factor method and data taken from a superseded EUR document (Ref. 18) though it is converted to a Multiple Greek Letter (MGL) method for use in RiskSpectrum. EDF and AREVA need to modernise or justify the adequacy of the CCF inputs. The MGL formulation is an accepted PSA method, but the parameter inputs and the justification for them needs to be addressed and TQs have been raised on this matter.

79 The parameter estimates are applied to all CCF groups independent 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. This is not acceptable at face value and no justification is given. Generic component-type specific and failure mode specific CCF parameter estimates have been published and are likely to enable a better analysis of the CFF contribution to the risk.

80 Section 5.3.2.4 indicates that several specific common cause failure probabilities have been based on expert judgment. However, the expert judgement process is not described nor are the uncertainties associated with expert judgement estimation process provided.

81 The documentation does not discuss uncertainties associated with the CCF parameters and again this information is readily available.

82 The PSA contains no discussion of assumptions made in regard to the defences against CCFs. There was no information located on the process to be used to ensure that PSA CCF assumptions are captured in the future development of testing, maintenance and operational strategies and procedures and strategies and completion of system designs.

Ref. 7, Table A1-2.7 Analysis of Hazards

83 The rationale for screening of hazards is not clear.

84 Table 3.4.8 provides a list of external hazards considered for inclusion in the UKEPR PSA. Sections 2.4.3, 2.4.4 and 2.4.5 discuss, in more depth, man-made external hazards, natural external hazards and animal infestation hazards that were considered.

Section 3.4.2 presents the internal hazards which were considered including fires, flooding, high energy component breaks, internal missiles, internal explosions, and dropped loads.

85 Section 6.5.1 provides the process and criteria for screening in or screening out external hazards. An external hazard is screened in if:

- The consequences of the external hazard could be important (to the plant structures, plant cooling systems etc) and the hazard frequency is not bounded by an internal event analysis already performed in the level 1 PSA.
- A detailed analysis is necessary to evaluate the frequency of core damage due to the external hazard.

86 An external hazard is screened out if:

- There is no impact expected on the plant safety.
- The levels of defence are judged sufficiently efficient to give a low frequency of core damage.
- The frequency of the external hazard is low (1×10^{-5}/y).

87 Table 6.5-4 presents the rationale for screening in or screening out of external hazards. However, it is not clear that a consistent process or set of criteria was applied to screening of internal hazards.

88 Section 6.4.5 indicates missile hazards are treated by a qualitative study on the basis of the corresponding deterministic analysis (and was screened out of the quantitative analyses).

89 Section 6.4.6 states that *"Due to the low initiating event frequency (<1 x 10^{-6}/ry) and the results of the structural analysis confirming that the residual heat removal function remains available, heavy load drop is screened out from the present PSA analysis"*. No reference is provided.

90 Section 6.4.7 indicates that the analysis of risk associated with internal explosions will be undertaken later in the licensing process after completion of detailed design studies.

91 Table 3.4-7 and table 3.4-8 present the frequencies for internal and external hazards, respectively. Section 6.5.3 presents the calculated frequency for aircraft crashes of various types. Table 3.4-8 and Section 6.5.3 presents frequencies but do not indicate whether these are mean frequencies. In addition, Table 3.4-8 does not present any other distribution parameters so it cannot be determined if the uncertainties in the external hazards are considered.

92 The frequency of combined strong winds and extreme snow as an initiator (plus a long LOOP) seems to be underestimated. Similarly it is stated (6.5.3.3) that the aircraft crash and LOOP events are independent. This is obviously incorrect.

93 Information on hazard sources is generally provided (Sections 2.4.3, 2.4.4, 2.4.5, 3.4.2, 3.4.3, 6.4, and 6.5). However, there is no discussion on hazard control programmes and only limited discussion related to hazard protection features.

94 There is no indication any unique characteristics of external hazards were considered in evaluating the impact on human performance. Furthermore there was no discussion of any process in place to ensure that relevant assumptions or findings from the PSA are captured in the future development of hazard protection strategies and procedures, in the completion of system designs, etc.

Ref. 7, Table A1-2.7.2 Internal fires

95 The internal fire analysis is a standard fire PSA but it has been carried out at a very high level, with only very coarse discrimination of fire zones (entire buildings). The modelling is also asymmetric as all the fires are assumed to occur in one of the buildings.

96 There is no discussion of fire propagation between buildings and if this is an issue, then the asymmetric assumption is questionable since the buildings/fire zones are not next to the same things, so consequences will be dissimilar.

97 All vulnerable components in a fire area with a fire are assumed failed. No specific justification is provided to support these assumptions/limitations.

98 Subsuming the fire suppression reliability (which is merely assumed at this stage, rather than calculated) into the initiating frequency (6.4.2) is not good practice and an RO (reference) has been issued covering this matter.

99 Non-power states are excluded from the analysis based on an unsupported qualitative low risk argument. This argument is not convincing and further information has been requested. EDF and AREVA do plan to look at this area in future PSA revisions and I will endeavour to agree a reasonable way forward on this point otherwise a further RO is likely.

100 Given the simplifying assumption noted above (and others not noted) it is unlikely that the analyses as they currently exist are suitable to help identify strengths and weaknesses of the UK EPR design associated with internal fires. Furthermore, it is difficult to judge whether the overall fire CDF estimates are realistic.

101 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 development fire protection strategies and procedures, in the completion of system designs, in the finalisation of cable routings, and in the final construction.

Ref. 7, Table A1-2.7.3 Internal flood

102 As stated in Section 6.4.3.2 the approach to assessing internal flooding risk in the UK EPR PSA is a simplified flooding PSA. Section 6.4.3.1 lists the major assumptions associated with the flooding analyses. These include:

- the study is performed at building level;
- the study is for at-power operation;
- conservatively all the equipment located in the affected building is assumed to be unavailable for ensuring the plant safety;
- for the evaluation of initiation frequencies, only generic values are applied;
- the flooding event is defined as a leakage and failure to isolate the break; flooding detection and isolation is taken into account in the evaluation of the initiating event frequency using a simplified approach;
- flooding detection instrumentation equipment is not analysed; and
- automatic reactor trip is assumed not to be prevented by flooding event.

103 No justification for these assumptions is provided. The Step 4 review will assess whether the simplified PSA allows a realistic estimation of the risk from flooding and the identification of specific strengths and vulnerabilities.

104 Table 6.4-3 present the flooding areas considered in the analyses and whether they are screened in or screened out and a brief discussion of the rationale for the screening

decision. A number of flood areas are screened out (or covered by another initiator) for the following reasons:

- important safety equipment is above maximum flooding level;
- redundancy - flooding in an area would impact only 1 of 4 trains (and for these areas it is generally argued that these vents are covered by similar internal event initiators);
- no water source expected for flooding area;
- no immediate plant trip; and
- covered by higher frequency internal initiator or fire initiator.

105 No quantitative screening of flooding appears to have been performed with the exception of subsuming certain scenarios into existing internal events or fire scenarios. The only screened in flooding areas are the safeguards building(s) and the turbine building. No estimates of the core damage frequency and significant release frequency arising from the set of flooding compartments/scenarios screened-out from the analysis are provided.

106 No discussion is provided on the assumptions of the impacts of flooding on human performance.

107 The system that is the source of the flooding is identified. However, source location, flow rate, maximum flood volume are not identified (see Sections 6.4.3.3.1 and 6.4.3.3.2). The characteristics of the flooding cause are generally not identified. The flooding source is generally just identified as leakage in the system (see Sections 6.4.3.3.1 and 6.4.3.3.2). Generally only one flooding source is identified for a flood area so grouping of similar scenarios is not performed.

108 The table shown in Section 6.4.3.2.3 lists the equipment types that are assumed susceptible to flooding failure. The failure mechanisms are not explicitly stated; however, the comment before the table *"The event is assumed to result in the failure of all components listed below that are present in the area, below the level of the maximum flood"* suggests that only submergence is considered as a failure mechanism and jet impingement, pipe whip, humidity, condensation, temperature, etc. are not considered.

109 A comprehensive list of assumptions related to flooding sources, allocation of equipment, segregation, flood detection and protection measures, etc. is not provided.

110 Indications, events and any other cues which can provide flood symptoms and allow for flood detection are not identified. Although isolation of the leak is considered for certain flooding initiators and a probability of isolation assigned the details are not explicitly discussed, the reliability of the flooding protection measures (both in terms of equipment as well as human performance) are not substantiated.

111 Flooding frequencies have been evaluated for the screened in safeguards and turbine buildings based on generic data from NUREG/CR-2300 (Sections 6.4.3.3.1 and 6.4.3.3.2). Use of the generic information from NUREG/CR-2300 which was issued in 1983 has not been justified and more recent generic source for flooding frequencies are available.

112 The flood frequencies used also contain the probability that the operator isolates the leak in sufficient time to prevent damage to critical equipment. This is not good practice; the operator action ought to be explicitly modelled so that potential dependencies can be addressed.

113 Again there was no indication of any attempt to capture the key flooding analyses assumptions and findings from the PSA.

<u>Ref. 7, Table A1-2.7.4 Seismic</u>

114 Section 6.5.2 indicates that the seismic hazard is analysed via a Seismic Margins Assessment (SMA) since a full seismic PSA cannot be performed at the stage of Generic Design Assessment (GDA), as no specific site has been selected. However, bounding site conditions are used for the design of Structures, Systems and Components (SSCs) and a ground motion spectrum shape is assumed. A bounding ground motion spectrum is used as input data for the estimation of equipment and structures fragilities.

115 Section 2.2 of the PCSR Subchapter 15.6 (UKEPR-0002-156 Issue 03) indicates the seismic equipment list (SEL) for the UK EPR SMA is developed using expert judgement in combination with the Level 1 PSA model. Two tables in Section 4.2 of PCSR Subchapter 15.6 present the SEL for structures and for systems /components.

116 Section 2.3 of PCSR Subchapter 15.6 indicates that the seismic initiating events are determined from the experience of past seismic PSAs and a review of the internal events of the level 1 PSA. Structures and other passive components that are typically not included in the internal events PSA should also be considered, particularly those that could lead directly to core damage or activity release.

117 Four event trees types are identified and analysed in the SMA.

- Event trees where the initiator occurrence leads directly to core damage.
- Seismically induced LOOP event tree. It is assumed that loss of off-site power occurs with unit probability following the SME event.
- Seismic small LOCA event tree, caused by failure of small pipework or the Reactor Coolant Pump seals.
- Event tree for ATWS caused by the failure of Control Rods to insert following the seismically induced LOOP, due to rod blockage or I&C failure.

118 Section 6.5.2 indicates that 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.

Ref. 7, Table 1.2.8 Low Power and Shutdown

119 Section 3.3 indicates that standard PWR Plant Operation States (POS) have been considered for non-full power operational modes.

120 The contribution to the CDF due to internal hazards during shutdown states is considered to be negligible due to 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 acceptable justification.

121 For external hazards Section 6.5.2 indicates that a detailed PSA-based SMA is performed for power states and a simplified approach is taken for shutdown states. No discussion on the simplified analysis approach and results for the seismic analyses for shutdown POS was located. The only other external hazards considered during shutdown POS appear to be the biological clogging of the water intake and frazil ice leading to loss of the ultimate heat sink (LUHS).

122 Section 1.6 indicates that definition of operator actions that may create an initiating event is part of the Shutdown PSA. Shutdown POS specific HRA analyses has been performed

for required post fault operator actions, but there was not any detailed discussion of human action related Initiators during shutdown, though they are included in the analysis.

123 Section 3.4.1.6.3 and 3.4.5 presents the IE frequencies in shutdown POS for loss of residual heat removal and loss of cooling chain shutdown states although the source of these frequencies is not clear. Section 3.4.1.6.4 presents the IE frequencies for uncontrolled level drop for shutdown POS. These are determined using fault tree analyses but the reference for these fault tree analyses is not stated.

124 Success criteria for various IEs for shutdown POS are given in various tables in Section 6.3. These tables describe the safety function, the systemic success criteria to meet the safety function, and operator response times for any required action. However, they do not describe or reference thermal-hydraulic, neutronics (or any other) analyses performed to support the determination of the success criteria.

125 There is no information on the process to ensure that relevant assumptions or findings of the PSA for low power and shutdown are captured.

Ref. 7, Table A1-2.9 Uncertainty, Quantification and Interpretation

126 Section 6.7 presents the uncertainty analyses on the Core Damage Frequency (CDF) due to reliability data uncertainties and to truncation of the Minimal Cut Sets (MCS). Uncertainty on the Level 1 Internal Events PSA results is quantified using the built-in uncertainty analysis capabilities of Risk Spectrum. This PSA uncertainty quantification evaluates parametric uncertainty. The uncertainty sampling has been performed at the basic events level rather than parameter level. This sampling method results in similar basic events being treated as independent rather than correlated.

127 An uncertainty distribution for each input parameter of the PSA model (except for parameters linked to C&I modelling) has been specified. Only point estimate value has been used for C&I failure probability modelling according to the 'compact model' approach. Section 6.7.1.2 discusses the source of the distribution parameters for various categories of events (IEs, component failures, HRAs, etc). Uncertainty analyses are performed with 30000 Monte Carlo simulations.

128 When quantitative results are presented they generally are point-estimates rather than the mean values calculated from the uncertainty analysis.

Ref. 7, Table A1-2.9.2 Quantification of the L1 PSA

129 Section 6.1.2.2.2 indicates that the small event tree / linked large fault tree method is used for quantification. Assumptions associated with the quantification of specific scenarios are given in the system analyses sections. For example, see Section 6.3.1.2.1 for assumptions related to the LOCA category.

130 Section 6.7.2 indicates that a minimal cut-set truncation level of 1×10^{-15} was used in the UK EPR PSA quantification. Figure 6.8-2 presents the calculated CDF as a function of truncation level. The CDF has reached an asymptotic plateau for truncation levels of 1×10^{-15} and lower. This is a good feature of the report.

131 Appendix DR2.1 presents the top 100 minimal cuts-sets for the overall PSA and for various subdivisions of the PSA (e.g. power operations, shutdown, etc) with a description of the basic events associated with each cut-set.

132 Fussel-Vesely (FV)1 and Risk Increase Factor (RIF)2 importance measures are presented in Section 6.8.2.

133 Appendix DR3.1 contains a more extensive listing of FV and RIF importance measures for basic events in the model. No discussion was found indicating importance measures were developed for groups of components or basic events, though pie charts giving system importance for each accident are included.

134 In the latest version of the PCSR (Issue 2) the distribution between the different plant operating states is shown in Subchapter 15.6, Section 15.6.1 Figure 2. Power states A and B contribute 78% to the internal event CDF. The time spent in the shutdown states (C to E) represents around 7% of the year and these states account for less than 22% of the internal event CDF. It is claimed that the distribution of risk is therefore proportionate to the time ratio between power and shutdown and due to the improvement of the protection during shutdown states the level of risk is uniform.

135 However, this presentation of the results is potentially misleading because it lumps all shutdown POS together. Consideration of the individual shutdown POS individually may lead to different conclusions.

Ref. 7, Table A1-2.9.3 Presentation of the Level 1 PSA Results and Interpretation

136 Section 2.2 in PCSR Subchapter 15.7 (Issue 2) presents the risk distribution between internal events, internal hazards and external hazards; between power operation and shutdown states; and the among the initiating event groups. However, as noted above more discussion is required regarding the relative importance and individual CDF results for each shutdown state.

137 Section 8.4 indicates that an iterative process to identify design improvements using the PSA was implemented throughout the development of the UK EPR design. Section 8.4 presents the main examples of design changes implemented due to prior PSA studies.

Ref. 7, Table A1-3 Level 2 PSA

138 In general the Level 2 PSA is considered to be a good piece of work and only minor points have been identified during the Step 3 review.

Ref. 7, Table A1-3.1 Interface between L1 & L2 PSA

139 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 has been directly linked to the Level 1 core damage 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.

[1] The Fussel Vesely Importance gives an idea of the fractional contribution of an equipment or human failure to the top event frequency. It is calculated by dividing the sum of all of the minimal cutsets containing the failure by the sum of all of the minimal cutsets.

[2] The Risk Increase factor for a component or human failure is the factor by which the top event frequency would increase if that component or human failure probability was set to 1. This is a very powerful means of establishing the significance of particular components or human actions.

140 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;
- steam generator pressure and isolation status.

141 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.

142 Section 3.3.16 describes the Level 2 human error probability (HEP) evaluation using the SPAR-H (Ref. 20) model and represent the following actions:

- isolate containment;
- transition to OSSA;
- depressurise the primary system;
- cool core debris in-vessel;
- depressurise containment;
- switch to active cooling in containment; and
- initiate containment sprays.

143 SPAR-H (Ref. 20) is also used to assess the dependencies between the Level 2 and Level 1 Human Failure Events.

144 The interface between the Level 1 and Level 2 PSA models represents the state-of-art and no findings are identified.

Ref. 7, Table A1-3.2 Deterministic Accident progression

145 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. 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. In support of the Level 2 PSA, MAAP calculations were performed to represent the CDES sequence, sensitivity to the calculation, evaluate specific phenomena, and to confirm if a particular scenario results in core damage.

146 The list of severe accident phenomena and challenges appears to represent a complete set when compared against the ASME Standard, IDCOR, NUREG-1150, and NUREG/CR-6595.

147 Split fraction assignments are made based on Monte Carlo evaluations; however, there is not sufficient detail provided to judge if the assumptions and input are appropriate.

148 As stated above, use of the MAAP4 code is appropriate for this type of application and the documentation indicates proper use of the code within known limitations. A review of

the MAAP EPR parameter file and selected input and output files from the EPR MAAP analysis is planned for Step 4.

149 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 said to be based on a Monte Carlo evaluation, however, details of that process were not reviewed in Step 3.

Ref. 7, Table A1-3.3 Containment performance analysis

150 The PCSR Sub-Chapter 15.4, Section 3.3.14 briefly summarizes the containment fragility evaluation. The containment failure analysis evaluates six dominant potential failure modes which are used to assess failure pressure, location and size. The analysis performed appears to utilize standard practices, however it is not clear if dynamic loading of the containment was considered along with the normal quasi-static pressurization.

Ref. 7, Table A1-3.4 Probabilistic Modelling – Accident progression trees

151 PCSR Sub-Chapter 15.4, Section 3.4 describes the accident sequence analysis along with the containment event trees (CETs). 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.

Ref. 7, Table A1-3.5 Source Term Analysis

152 PCSR Sub-Chapter 15.4, Section 3.5 describes the release category definitions and the source term analysis. There are 29 unique release categories established with attributes defined based on the status of the following.

- containment bypass;
- timing of containment failure;
- containment failure mode;
- core melt arrested in-vessel;
- core concrete attack;
- core debris flooding ex-vessel; and
- mitigation by containment sprays.

These attributes define the most important aspects of the source term analysis and provide an adequate grouping for the consequence (Level 3) evaluation. The radionuclide releases are based on the standard set of 12 fission product groups.

153 The objectives of the source term analysis are properly stated as:

- characterize the source term for each release category; and
- perform analysis to determine the sensitivity of the source term to a range of input parameters.

154 MAAP analysis is then described to calculate the source terms for the release categories with clearly stated post-processing rules to adjust for; 1) Iodine chemistry, 2) scrubbing in ventilation systems, 3) submergence of ISLOCA piping, and 4) SGTR scrubbing.

155 There is currently no justification provided for the associated decontamination factors and this matter will be reviewed in Step 4.

Ref. 7, Table A1-3.5 Source term analysis

156 Presentation Source term analyses have typically tracked Cs release in the form of CsI and CsOH. Recent experiments at the Phebus facility at the Cadarache research centre have discovered that instead of CsOH, Cs2MoO4 is the released compound for the remaining Cs not used in the formation of CsI. This compound has significantly lower vapour pressure and will result in a lower overall Cs release fraction.

157 Scrubbing in the case of a SGTR is only credited for submergence of the tube rupture. Deposition of aerosols due to impaction on adjacent tubes has been observed at the Paul Scherrer Institute ARTIST facility. Total decontamination factors on the order of 7 have been observed indicating that the current source term may be conservative.

Ref. 7, Table A1-3.6. Presentation and Interpretation of the Level 2 PSA Results

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

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

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

160 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

161 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%.

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

Ref. 7, Table A1-4 Level 3 PSA

163 This area will be assessed in Step 4.