Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 PROBABILISTIC SAFETY ANALYSIS OF THE WESTINGHOUSE AP1000

DIVISION 6 ASSESSMENT REPORT NO. AR 09/017-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) Generic Design Assessment (GDA) Step 3 assessment of the AP1000 Probabilistic Safety Analysis (PSA) presented in report *UK AP1000 Probabilistic Risk Assessment* (UKP-GW-GL-022, Rev 0) provided by Westinghouse in support of the *AP1000 European Design Control Document* (EPS-GW-GL-700, Rev 0).

For GDA Step 3 it is important to note that the PSA has not been assessed in its entirety; rather, the arguments that support high level claims (which were assessed in Step 2) on how the PSA related Safety Assessment Principles are met, have been looked at. The evidence supporting these claims and arguments will be examined in Step 4.

For PSA, 'arguments' are interpreted as being the methods, techniques and scope of the PSA. The assessment conducted during GDA Step 3 has mainly been restricted to those areas but some in-depth spot checks of models and data have also been conducted to gather information on how those methods and techniques have been applied by Westinghouse.

The AP1000 PSA is a Level 1 and Level 2 PSA. A Level 3 PSA has been performed but it has not been reviewed during GDA Step 3. The scope of the PSA includes consideration of internal initiated events and internal hazards and includes low power and shutdown operating states. The methods and data used in the PSA are well known, although not always up-to-date or aligned with the latest international good practices.

During GDA Step 3 a high level review of all the PSA technical areas against the tables contained in Annex 1 of Nuclear Directorate's PSA guide (T/AST/030 Issue 3, February 2009) has been conducted. In addition, a detailed review of the PSA Task on "identification and grouping of internal initiating events during operation at power" has been also done to confirm whether the basis of the PSA are robust and to gain confidence on its completeness.

The GDA Step 3 review has been undertaken with the assistance of Technical Support Contractors who have carried out their work under direction and supervision of ND.

From the GDA Step 3 review carried out, 85 Technical Queries (TQ) and 2 Regulatory Observations (RO) have been issued. An 'AP1000 PSA Step 3 Assessment Wrap-up Meeting' was held in August 2009 with representatives from ND's GDA team (including TSCs), Westinghouse and some Utilities to agree the priority of each TQ and RO.

The current PSA with its current scope provides part of the basis to interpret the risk associated with this reactor and where the main design strengths and relative vulnerabilities may lie. However, shortcomings in scope, methods and data identified during GDA Step 3 indicate that work will be required to complete and modernise the PSA so that it can provide a more adequate input into the demonstration that the risk associated with the AP1000 is ALARP.

Despite the above, the current Core Damage and Large Release Frequencies presented by Westinghouse provide a degree of confidence that the relevant Numerical Targets of the SAPs will be met. At the moment, I do not have any reason to believe that this position will change dramatically once the PSA has been completed and updated.

Westinghouse's PSA team are making a significant effort to establish a programme of work to update the AP1000 PSA and bring it to modern standards. They have shown readiness to address the TQs and ROs properly and they appear to listen and take on board feedback given by ND.

Overall, I see no reason, on PSA grounds, why the AP1000 should not proceed to Step 4 of the GDA process.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ALWR URD	Advanced Light Water Reactor Utility Requirements Document
APET	Accident Progression Event Tree
BMS	(Nuclear Directorate) Business Management System
BSL	Basic Safety Level
CAFTA	Computer Aided Fault Tree Analysis System
CCF	Common Cause Failure
CDF	Core Damage Frequency
Ceff	Containment Effectiveness
CET	Containment Event Tree
CHR	Containment Heat Removal
C&I	Control and Instrumentation
DCD	Design Control Document
DF	Decontamination Factor
EA	The Environment Agency
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
FA	Fault Analysis
FIVE	Fire-Induced Vulnerability Evaluation
FMEA	Failure Modes and Effects Analysis
GDA	Generic Design Assessment
HCLPF	High Confidence of Low Probability of Failure
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Analysis
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
IE	Initiating Event
INPO	Institute of Nuclear Power Operations
IRWST	In-containment Refuelling Water Storage Tank
IVR	In-Vessel Retention
LCF	Late Containment Failure
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power

LIST OF ABBREVIATIONS

LRF	Large Release Frequency
MAAP	Modular Accident Analysis Program
MCCI	Molten Corium-Concrete Interaction
MCR	Main Control Room
MDEP	Multi National Design Evaluation Programme
MGL	Multiple Greek Letter
MOV	Motor Operated Valve
ND	(HSE) Nuclear Directorate
NPP	Nuclear Power Plant
PCER	Pre-construction Environment Report
PCSR	Pre-construction Safety Report
PDS	Plant Damage State
PGA	Peak Ground Acceleration
P&ID	Piping and Instrumentation Diagram
PID	Project Initiation Document
PLS	(AP1000) Plant Control System
PMS	(AP1000) Protection and Safety Monitoring System
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PWR	Pressurised Water Reactor
PSA	Probabilistic Safety Analysis
RHR	Residual Heat Removal
RC	Release Category
RI	Regulatory Issue
RIA	Regulatory Issue Action
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RPV	Reactor Pressure Vessel
SAMDA	Severe Accident Management Design Alternatives
SAP	Safety Assessment Principle
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SMA	Seismic Margins Analysis
SSC	Structures, Systems and Components
ST	Source Term

LIST OF ABBREVIATIONS

TAG	(Nuclear Directorate) Technical Assessment Guide
TCS	(AP1000) Turbine Building Closed Cooling Water System
THERP	Technique for Human Error Rate Prediction
T&M	Testing and Maintenance
TQ	Technical Query
TSC	Technical Support Contractor
US NRC	United States Nuclear Regulatory Commission
WEC	Westinghouse Electric Company LLC
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) is following the claims-argument-evidence hierarchy. In Step 2 the claims made by the RP were examined, in Step 3 the assessment focussed on the arguments that underpin those claims and in Step 4 the evidence that supports the claims and arguments will be looked at. The Step 2 assessment (Ref. 1) concluded that Westinghouse had provided an adequate overview of the approach, scope, criteria and output of the PSA but also noted some points, or observations to be followed up in Steps 3 and 4.

2 This report deals with the GDA Step 3 assessment of the UK AP1000 Probabilistic Risk Assessment (PRA) report (Ref. 2) provided by Westinghouse in support of Chapter 19 (Probabilistic Risk Assessment) of the *AP1000 European Design Control Document* (Ref. 3). At the time when this assessment process commenced, Ref. 2 was fully available on the internet.

3 During a visit to Westinghouse Offices in Pittsburgh in March 2009 to undertake a detailed assessment of the PSA task on *Identification and Grouping of Initiating Events* it became apparent that some parts of the UK AP1000 PRA report (Ref. 2) had been superseded or supplemented by more up-to-date documents. For example, Chapters 26 (Protection and Safety Monitoring System) and 28 (Plant Control System) of Ref. 2 are now superseded by Calculation Notes APP-PRA-GSC-222 Rev. 1 and APP-PRA-GSC-228 Rev. 0 respectively. The PSA electronic model built up in CAFTA submitted to ND for assessment and contained within / attached to Calculation Note APP/PRA/GSC-236 Rev. 0 is an updated version of the one documented in Ref. 2. The existence of these newer documents has been taken into consideration during the Step 3 assessment and, in this report, an attempt has been made to reflect and / or acknowledge key changes, but the new material has not been reviewed in detail. However, these will be part of the suite of PSA documents and computer files that will be assessed in detail during GDA Step 4.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

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

2.1 Requesting Party's Safety Case

5 Probabilistic Safety Analysis was performed by Westinghouse to support the design of the AP600 in the 1990s. This practice was carried over to the design of the AP1000.

6 The construction of the PSA is based on the standard small event tree / large fault tree approach, and is a Level 1 and Level 2 PSA. A simplified Level 3 PSA has been performed but it has not been reviewed during GDA Step 3.

7 The scope of the PSA includes consideration of internal initiated events and internal hazards and includes low power and shutdown operating states.

8 The methods and data used in the PSA are well known, although not always up-to-date or aligned with the latest international good practices, as will be discussed later in this report.

9 The PSA quantification for both Level 1 and Level 2 is carried out using the CAFTA software developed by the Electric Power Research Institute (EPRI).

10 The AP1000 PSA results are presented in Table 1 below.

Table 1: AP1000 PSA Results (from Ref. 2)

Item	AP1000
Core Damage Frequency (CDF) internal events at power	2.41×10^{-7} /yr
CDF internal hazards (fires and floods) at power	5.69×10^{-8} /yr
CDF internal events during low power and shutdown	1.23×10^{-7} /yr
CDF internal hazards (fires and floods) during low power and shutdown	8.8×10^{-8} /yr
Large Release Frequency (LRF) (reactor internal events at power)	1.95×10^{-8} /yr
LRF (reactor internal events during low power and shutdown)	2.05×10^{-8} /yr

2.2 Standards and Criteria

11 The main standards and criteria used are ND's Safety Assessment Principles (SAPs) (Ref. 4). The PSA Step 3 assessment strategy (Ref. 5) identified SAPs FA.10 to FA.14 and Numerical Targets 7 to 9 as the relevant parts of that document. Attention has also been paid to relevant parts of the International Atomic Energy Agency (IAEA) standards (Ref. 6) and the Western European Nuclear Regulators' Association (WENRA) reference levels (Ref. 7).

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

13 For Step 3 it is important to note that the PSA has not been assessed in its entirety; rather, the arguments that support high level claims (which were assessed in Step 2, Ref. 1) on how the PSA SAPs are met, have been looked at. The evidence supporting these claims and arguments will be examined in Step 4.

14 For PSA 'arguments' are interpreted as being the methods, techniques and scope of the PSA. The assessment conducted during GDA Step 3 has mainly been restricted to those areas but some in-depth spot checks of models and data have also been conducted to gather information on how those methods and techniques have been applied by Westinghouse.

2.3 Nuclear Directorate Assessment

2.3.1 Strategy

15 The Step 3 PSA assessment has followed the PSA strategy set out at the end of Step 2 (Ref. 5), and has been carried out by conducting a high level review of all the PSA technical areas against the tables contained in Annex 1 of ND's PSA guide (Ref. 8). A detailed review of the PSA Task on 'identification and grouping of internal initiating events during operation at power' has also been conducted during GDA Step 3 to confirm whether the bases of the PSA are robust and to gain confidence on its completeness.

16 The Step 3 review has been undertaken with the assistance of Technical Support Contractors (TSC) who have carried out their work under direction and supervision of ND. This is documented in detail in Refs 9 to 11.

17 For each of the relevant 'assessment expectations' in the tables of Ref. 8, a view has been formed on the adequacy or otherwise of the documentation. Commentaries explaining the reason for that view have also been provided. Cases where the RP's documentation has been found to be less than adequate have led to or will lead to dialogue with Westinghouse and / or the issuing of Technical Queries (TQ) or Regulatory Observations (RO), as appropriate.

18 In order to provide a conclusion to the GDA Step 3 assessment an 'AP1000 PSA Step 3 Assessment Wrap-up Meeting' was held at HSE's Headquarters on 19th and 20th August, 2009. Representatives from ND's GDA team (including TSCs), Westinghouse and some Utilities attended the meeting. The objective of the meeting was to discuss the outcome of ND's Step 3 GDA in the area of PSA for the AP1000. This included for each technical area:

- Summary of the assessment work done (as documented in this report and its References 9 to 11).
- Overview of key queries raised.
- Westinghouse's responses or proposed responses.
- Summary of findings.

19 During the meeting ND gave an indication of the priority of each TQ or RO. This provided clarity on ND's expectation and was appreciated by all involved. The prioritisation scheme was as follows:

- P1: Adequate response needed immediately (because it is necessary to proceed with GDA Step 4 detailed PSA assessment).
- P2: Information needed within GDA framework. If work is necessary to address the TQ / RO satisfactorily, this should be started in GDA Step 4 timeframe (for ND to gain confidence that it is addressing the TQ / RO satisfactorily) but not necessarily finished. If work is not completed within GDA it could constitute a 'Condition' attached to the GDA certificate. If work is not started within GDA it could constitute an 'Exclusion' attached to the GDA certificate.
- P3: Information is necessary for Licensing. However, since this will be normally pointing to a deficiency or gap in the PSA, if not done within GDA it could constitute a 'Condition' attached to the GDA certificate.

20 The highlights of the 'AP1000 PSA Step 3 Assessment Wrap-up Meeting' and decisions made are documented in the meeting Contact Report (Ref. 12).

21 A summary of our Step 3 assessment findings is presented below. Further details are provided in Annex 2.

2.3.2 Strengths of the PSA

22 The AP1000 PSA includes reactor faults: Level 1 PSA (Core Damage Frequency, CDF); Level 2 PSA (Large Release Frequency, LRF); some internal hazards (internal fires and internal floods) and low power and shutdown. In this regard, the AP1000 PSA provides part of the basis to interpret the risk associated with this reactor and where the main design strengths and relative vulnerabilities may lie.

23 The AP1000 PSA appears to be supported by a considerable amount of analysis. This is particularly the case for the Level 2 PSA.

24 The PSA documentation is well structured and consistent throughout. Because of this, the current PSA documentation forms a good basis for future developments of the PSA (although there is some lack of traceability in the references).

25 Westinghouse's PSA team are dealing with a PSA that was originally developed years ago to standards that are no longer modern in some areas. The PSA team however, are making a significant effort to establish a programme of work to update this PSA and bring it to modern standards. They appear to be listening and taking on board feedback given so far by the ND team. Discussions between ND and Westinghouse's PSA team have been open and positive.

2.3.3 PSA Limitations, Initial Concerns and Points for Further Consideration

26 The initial findings of the assessment of the AP1000 PSA are described in the following paragraphs. It should be noted that this is a snapshot in the assessment process and represents an interim position. Detailed review of Westinghouse's responses to the TQs / ROs, and detailed assessment of the various PSA tasks during GDA Step 4 will confirm or otherwise these initial concerns; it also may raise additional findings.

2.3.3.1 PSA Scope

27 The scope of the PSA is not complete. Initial concerns have been raised in the following areas:

- The PSA documentation does not present an integrated picture of the risk associated with all the sources of radioactivity in an AP1000 Nuclear Power Plant (NPP). Only reactor accident sequences initiated by internal events have been carried forward to the Level 2 PSA. A separate study of the risk associated with the spent fuel pond has been provided to ND but has not yet been assessed.
- The risk associated with non-core damage sequences has not been evaluated and integrated with the overall PSA results. It appears that the releases from the Design Basis Accident sequences have been evaluated but we are not yet in a position to judge whether this, together with the results from the various parts of the risk assessment, will allow a meaningful comparison against the Numerical Targets of the SAPs (in particular Target 8, popularly known as the 'dose-band staircase')
- Sequences where core damage / containment failure may happen in the long term are currently excluded from the evaluation of the risk.
- Formal screening of internal hazards is not obvious (only internal fires and floods have been included in the Level 1 PSA but have not been taken forward to the Level 2 PSA).
- The screening of external hazards for analysis appears incomplete. The PSA does not include any external hazard.
- The Level 1 Shutdown PSA contains little AP1000-specific analysis being extensively based on AP600, and the presented documentation provides little technical detail.
- AP1000-specific shutdown Level 2 PSA has not been performed (the current analysis is a scaling of the AP600 analysis to the AP1000 CDF).

28 At this point it is difficult to evaluate the overall impact of the above omissions in the PSA and it would not be feasible for Westinghouse to complete (and update as required) the PSA and for ND to assess the updated PSA within GDA timeframe. Therefore ND's PSA review team will make an assessment of the potential risk gap to report in GDA Step 4.

29 In any case Westinghouse ultimately needs to provide an overall ALARP (As Low As Reasonably Practicable) evaluation taking into consideration all sources of risk. A key element of this should be a full scope high quality PSA.

2.3.3.2 PSA Documentation

30 The AP1000 PSA documentation is not consolidated. Some chapters of the UK AP1000 PRA report (Ref. 2) reviewed in GDA Step 3 are superseded by Calculation Notes (including the PSA model itself). Also there is heavy reliance on, and reference to, the AP600 PSA documentation and supporting analyses. The AP600 PSA documentation will need to be referred to during the detailed review in GDA Step 4 and justification/s of applicability may be needed in order to progress the assessment.

2.3.3.3 PSA CAFTA Model

31 The original PSA was built in Westinghouse's in-house software and later transferred to the well established internationally used CAFTA software developed by EPRI. Nevertheless, the current model has certain limitations, e.g. event and fault trees are not linked (event trees are only drawings while the model consists of a series of top-logic fault trees constructed semi-manually). Many gates are not described. The model does not include the Fire and Flooding PSA models or models for the initiating events (which have been analysed via fault trees). Because of this, additional assessment effort may be required during the detailed review in GDA Step 4.

2.3.3.4 System to Capture Assumptions

32 The PSA is built on numerous assumptions that can be affected by siting, design and construction, or operational matters (procedures, testing and maintenance strategies, staffing, training). It is therefore important that a well designed system is in place to: 1) enable the assumptions made in the PSA to be captured during design, construction, procedure development, etc; and 2) enable the latest available design and operational information to be transferred to the PSA so that assumptions (and models) can be reviewed accordingly and timely. This system has not been visible during GDA Step 3.

2.3.3.5 Identification and Grouping of Initiating Events (IE)

33 As well as a high level review of the AP1000 PSA task on 'Identification and Grouping of IEs' against the expectations in T/AST/030 (Table A1-2.1), a detailed review of the identification and grouping of internal initiating events during operation at power has been conducted during GDA Step 3 to confirm whether the bases of the PSA are robust and to gain confidence on its completeness (Ref.10). 34 TQs were raised from this review (21 on 'scope' and 13 on 'grouping'). An initial look at Westinghouse's responses suggests generally high quality responses and good explanations. From these Westinghouse has already identified and acknowledged the need for some PSA update work.

34 Westinghouse's responses to the 34 TQs will be reviewed in detail early in GDA Step 4 to confirm their technical adequacy. Further changes to the PSA may be required after this. In any case, Westinghouse should enhance the documentation of the Identification and Grouping of IEs so that the traceability and completeness are evident.

2.3.3.6 Success Criteria

35 A high level review of the AP1000 PSA task on 'Success Criteria' against the expectations in T/AST/030 (Table A1-2.2) has been conducted during GDA Step 3. This has raised concerns regarding the general traceability of the success criteria to the supporting analyses (e.g. thermal-hydraulic). To respond to this concern, Westinghouse has developed a roadmap which should provide the required transparency and

traceability. This roadmap will be tested early in Step 4 by assessing in detail the success criteria for two initially selected accident sequences.

36 Westinghouse has used conservative analyses to define the success criteria in some areas of the PSA. This could in principle distort the results of the PSA and limit its usability. Therefore, Westinghouse needs to provide details of the extent of conservatisms in the success criteria and their impact, and justify the approach adopted.

2.3.3.7 Accident Sequence Analysis (Event Trees)

37 A high level review of the AP1000 PSA task on 'Accident Sequence Analysis (Event Trees)' against the expectations in T/AST/030 (Table A1-2.3) has been conducted during GDA Step 3. Key findings are summarised below.

38 It is important that Westinghouse establishes the link between the accident sequences delineated in the PSA and the procedures used by the operators during the course of an accident. This link is currently missing.

39 Westinghouse needs to explain if and how they have evaluated potential dependencies between initiating events and mitigating systems due to software failures.

40 Most event trees contain a header CHR (Containment Heat Removal) following success of the reactor cooling systems. This is because (in the longer term) containment heat removal is necessary to evacuate the residual heat from the reactor. However, sequences with failure of CHR are not added to the CDF or carried over to the Level 2 PSA. Westinghouse needs to demonstrate a safe stable state of the plant at the end of the (selected) PSA mission time in sequences where success of reactor cooling systems is claimed. Further development in the event trees may be needed.

2.3.3.8 Systems Analysis (Fault Trees)

41 A high level review of the AP1000 PSA task on 'Systems Analysis' against the expectations in T/AST/030 (Table A1-2.4) has been conducted during GDA Step 3.

42 A number of concerns raised during this review have been compiled in an RO that mainly addresses incompleteness of the system fault tree models and concerns on how the models have been built. For example, the models do not include pre-accident Human Failure Events (HFE) (e.g. mis-alignments and mis-calibrations) and the criteria for their exclusion are not considered adequate; the criteria for excluding structural failures and passive component failures may be optimistic for a design that bases its safety on the availability of 'passive' systems; the modelling of unavailabilities due to Testing and Maintenance (T&M) is asymmetric, some T&M events are embedded inside modules, and, overall this part of the models is not easily traceable; the AP1000 Fault Tree Guidelines promote simplification of the model structure. This has been achieved by, for example, modelling basic events out of step to the logical sequence described by the gate descriptions, or by using modular events throughout without proper documentation. The simplified approach also affects the way in which Common Cause Failures (CCF) have been included in the fault trees. Also, the modelling of instrumentation failures that contribute to the human errors (e.g. failure of the alarms or indications) is very simplistic and unrelated to the actual instrumentation available. All these simplifications defeat the transparency of the model and bring questions regarding whether all dependencies have been properly captured.

43 Other findings in the systems analysis have been brought to Westinghouse's attention via TQs. In particular, the approach adopted for the definition of system boundaries in the AP1000 PSA is not explicit in the documentation provided. Adequate simplified system diagrams are not included. Also, the PSA report does not include information on the

boundaries adopted for all component types modelled. In addition, the matrices that show the dependencies between components and their support systems do not explicitly indicate which specific component in the support system delineates the interface between both systems. Because of all of this, it is felt that the current system fault tree models are prone to having gaps or overlaps. This also brings questions on whether the data and the models are consistent. Although the correctness and completeness of the system models needs to be reviewed in more detail during GDA Step 4, it is already clear that the systems analysis documentation (including the fault tree guidelines) requires enhancements.

44 One of the issues encountered during GDA Step 3 is that it is not clear what the current status of development of each system design, testing and maintenance schedules and strategies is and what exactly the PSA models. Clarity on this is particularly urgent for the systems that will be reviewed in detail during GDA Step 4.

2.3.3.9 Human Reliability Analysis (HRA)

45 A review of the AP1000 PSA task on 'Human Reliability Analysis' against the expectations in T/AST/030 (Table A1-2.5) has commenced during GDA Step 3. So far, this review has raised initial concerns in the following areas:

- Lack of modelling / consideration of pre-initiator HFEs (discussed above in the systems assessment).
- Assessment of time windows for operator actuation appears optimistic.
- Consideration of post-fault diagnosis appears unrealistic.
- Recovery model used in the Human Error Probability (HEP) calculations (recoveries by other members of the operating team) seems optimistic.
- The Technique for Human Error Rate Prediction (THERP) data requires substantiation for AP1000 digital interfaces and facilities.

46 Westinghouse has been briefed about the above but has not had the opportunity yet to see and comment on the review report. Therefore, formal TQs / ROs have not been raised yet. This review work will continue in GDA Step 4 and will be done in coordination with the Human Factors assessment team.

2.3.3.10 Data Analysis

47 A high level review of the AP1000 PSA task on 'Data Analysis' against the expectations in T/AST/030 (Table A1-2.6) has been conducted during GDA Step 3.

48 For the evaluation of some initiating event frequencies (e.g. transients) Westinghouse has used operational experience data from Westinghouse reactors. However, this data is old and limited to a 5 year period, which brings a concern on its adequacy. Figures used for the frequencies of Steam Generator Tube Rupture (SGTR) and Loss of Coolant Accident (LOCA) need justification. In all cases the criteria for selection of data sources and the order of precedence of data sources used in the evaluation of initiating event frequencies is not explicit in the PSA documentation.

49 Data used for component reliability is old and requires updating. Details of the component types (families) defined and their characteristics and identification of the components grouped within each type / family needs to be explicit, but it is not. Also, ND expects to receive information (description and definition) on boundaries for each component population and evidence that the component boundaries in the generic

sources of data used are consistent with the boundaries used in the PSA Systems Analysis. Concerns with some component mission times have also been raised.

50 Data used for the CCF parameters is also old and requires updating.

51 It is understood that Westinghouse has programmed work to update the PSA database. ND wishes to see and discuss with Westinghouse, during GDA Step 4, the programme to do this work and the methods and data sources selected to gain confidence that the next version of the PSA database is likely to meet ND's expectations. It is however not clear whether this effort will also address CCF data but this data should also be updated.

2.3.3.11 Analysis of Hazards

52 A high level review of the AP1000 PSA task on 'Analysis of Hazards' against the expectations in T/AST/030 (Table A1-2.7) has been conducted during GDA Step 3.

53 The analysis of hazards for the AP1000 PSA does not start with a complete list of internal hazards. Apart from internal fire and internal flood no analysis or screening of additional potential internal hazards (e.g. turbine missile, dropped loads) has been documented in Ref. 2. Westinghouse has been requested to provide justification for this.

54 In the same way, the analysis of external hazards for the AP1000 PSA does not start with a complete list. From the set of hazards listed up front, high winds, tornadoes, external floods and transportation and nearby facility accidents have been screened out based on a frequency $<1.0 \times 10^{-6}$ /yr (according to the PSA documentation, although follow-up discussions with Westinghouse suggest that the screening criteria used was $<1.0 \times 10^{-7}$ /yr). Considering that the AP1000 internal events CDF is 2.41×10^{-7} /yr and the LRF is 1.95×10^{-8} /yr, there is a question on the adequacy of (either) screening criteria. Finally, the seismic hazard is addressed via a Seismic Margins Analysis (SMA) but it is not included in the PSA.

2.3.3.11.1 Fire PSA

55 Currently the estimated CDF from internal fires amounts to approximately 25% of the CDF from internal initiating events, and, therefore, the relative risk significance of internal fires is non negligible.

56 Westinghouse has used the method FIVE with some enhancements to conduct the AP1000 Fire PSA. Since FIVE is a focused screening tool with inherent conservatisms and optimisms, and has now been superseded by NUREG/CR-6850, the adequacy of the approach needs to be justified. In particular, concerns have been raised in the following areas of the analysis: fire frequencies, selection of cables and fire impact on circuits, spurious actuations, fire induced explosions and missiles impacting outside the compartment boundary, multi-compartment fires and human reliability analysis for fire scenarios.

57 During the ND / Westinghouse 'AP1000 PSA Step 3 Assessment Wrap-up Meeting' (Ref. 12), it became apparent that although Westinghouse may be able to provide answers to some of the questions raised, the current Fire PSA is not a good representation of the AP1000 risk due to internal fires since it needs significant update to incorporate design changes.

58 In order to compile all the concerns around the AP1000 Fire PSA an RO has been raised. In response to this Westinghouse is planning to establish and provide, within GDA timeframes, a detailed programme to update the Fire PSA, however the work will not be completed until later. ND will assess Westinghouse's Fire PSA programme in GDA Step 4. Our expectation is that the review and update of the AP1000 Fire PSA should

align it with up-to-date information and modern standards and, therefore, the Fire PSA programme should be accompanied by enough information on standards, approaches and data sources to be used to allow us to establish an initial judgement on whether the final Fire PSA for the AP1000 will be acceptable to ND.

2.3.3.11.2 Flooding PSA

59 Currently the estimated CDF from internal flooding events is much smaller than the CDF from internal initiating events, and, therefore, the relative risk significance of internal floods is small. However, from the review conducted so far, it appears that some aspects of the flooding analysis may be optimistic. For example, old data has been used for flood frequencies while more modern data reflects more accurately the frequency of spraying events. Maintenance induced floods have not been considered. The PSA assumes that doors will remain intact and in their normal position in all flooding scenarios. It is not clear if / how structural failures due to the flood load, or compartment pressurisation, have been considered. 'Immersion' and 'spray hazards' are the only failure mechanisms addressed; 'jet impingement' and 'high temperature and / or humidity effects' or 'over pressurisation' due to high energy line breaks are not discussed. No discussion is included of the post flood human reliability analysis so it is not clear whether the potential degradation of human reliability in some flood scenarios has been addressed. Therefore, additional information, relevant justification or extension of the analysis will be required to address all these points.

2.3.3.11.3 Seismic Hazard

60 Westinghouse has submitted an SMA to address seismic risk. This is not a Seismic PSA and cannot be integrated with the rest of the PSA for overall evaluation of the risk. Using the information in the SMA and the seismic hazard analysis for one of the NPP sites in the UK, ND's assessment team has estimated that the mean LRF for the seismic event would be of the same order as the currently calculated LRF from internal events (1.95×10^{-8} /yr). Therefore, more analysis will be required to determine the seismic contribution to the risk when site-specific information is available.

2.3.3.12 Low Power and Shutdown PSA

61 A review of the AP1000 PSA task on 'Low Power and Shutdown' against the expectations in T/AST/030 (Table A1-2.8) has started during GDA Step 3 however the review team quickly encountered problems in this particular area due to the scattered nature of the documentation of the AP1000 Shutdown PSA. For example, the UK AP1000 PRA does not present the Plant Operational States (POS) during low power and shutdown or the derivation of the IEs during low power and shutdown POSs. This appears to be included in the documentation of the AP600 PSA, but the applicability of AP600 information is not clear. In order to undertake a detailed assessment during GDA Step 4 Westinghouse has been requested to provide a reconstruction of the study from the various sources of information.

2.3.3.13 Uncertainty Analyses, Quantification, and Interpretation of Level 1 PSA Results

62 A systematic description of all sources of uncertainty is currently missing from the AP1000 PSA report. This is necessary to confirm whether the sensitivity and uncertainty analyses are sufficient to address important uncertainties. In addition Westinghouse needs to explain what actions are being taken to reduce uncertainties that have a significant (relative) impact on the overall risk. ND requires this to gain confidence that

the results of the PSA are robust and the PSA can be used in future applications to support decision making.

63 Regarding the parametric uncertainties Westinghouse needs to provide adequate justification of the error factors assigned and they also need to explain how parametric uncertainties of components using the same parameter (e.g. components of the same type the failures of which are combined in the same cutsets) have been propagated in the quantification.

64 The truncation limits used in PSA quantification need to be identified and justified.

65 Finally, Westinghouse needs to revise the PSA documentation to reflect the quantification of the CAFTA model and its results.

2.3.3.14 Interface between Level 1 and Level 2 PSA

66 The review of the AP1000 Level 2 PSA started by conducting a high level review of the 'Interface between the Level 1 and the Level 2 PSA' against the expectations in T/AST/030 (Table A1-3.1).

67 The AP1000 Plant Damage States (PDS) are identified using a 2 / 3 letter code. Each Level 1 sequence is mapped to the relevant PDS by using a set of attributes. However, no evidence is provided in the reviewed documentation that a systematic process to identify and select PDS attributes had been followed and no step-by-step explanation of the criteria used to determine each grouping attribute based on the status of the Level 1 sequences is included.

68 The frequency of each PDS is calculated by adding the frequencies of all the Level 1 sequences. Each PDS is connected to a Containment Event Tree (CET). Careful application of Westinghouse's methodology to address the interface between the Level 1 and Level 2 PSA should be capable of correctly transferring information from the Level 1 sequences to the Level 2 CETs, but lack of transparency in the process was noted.

2.3.3.15 Deterministic (Severe) Accident Progression Analysis

69 A high level review of the 'AP1000 Deterministic Accident Progression Analysis' that supports the Level 2 PSA against the expectations in T/AST/030 (Table A1-3.2) has been conducted during GDA Step 3.

70 The deterministic accident progression analyses for the AP1000 have been done using the MAAP4 code. A summary of these analyses is presented in the PSA documentation. Detailed documentation (and input decks) of individual MAAP4 calculations need to be provided by Westinghouse so that they can be assessed during GDA Step 4.

71 The accident progression analyses are usually specific to the AP1000, although a considerable amount of information is drawn from earlier analysis for the AP600, with scaling arguments and adjustments. The parametric sensitivity to selected assumptions is examined in areas such as depressurisation of the Reactor Pressure Vessel (RPV), In-Vessel Retention (IVR) and hydrogen combustion. However, it was felt that the effects of alternate credible assumptions had not always been thoroughly demonstrated to be negligible.

2.3.3.16 Containment Performance Analysis

72 A high level review of the 'AP1000 Containment Performance Analysis' against the expectations in T/AST/030 (Table A1-3.3) has been conducted during GDA Step 3.

73 The analysis of the AP1000 containment performance is based on typical containment failure mechanisms and locations and no evidence was found of a systematic search for, and evaluation of, all plausible mechanisms and locations of containment failure. Qualitative arguments are used to dismiss the contributions of smaller mechanical and electrical penetrations; these are not considered sufficient. Furthermore, it is not clear from the documentation provided to what extent stress concentration around small penetrations is addressed in the structural response calculations.

74 The contributors to the uncertainty in the ultimate capacity of the containment have been quantified by expert judgment, but no evidence was found of a systematic process of eliciting expert judgment for this purpose.

75 According to Westinghouse, the current AP1000 LRF is not very sensitive to the ultimate capacity of the containment – this is probably due to the fact that the currently estimated low CDF allowed Westinghouse to make conservative assumptions regarding containment performance in the Level 2 PSA while still presenting a LRF that is small. This approach may be no longer adequate if future revisions of the PSA show a higher CDF. This is the reason why assessment of this aspect of the Level 2 PSA will be pursued in GDA Step 4 despite its currently perceived low importance from the risk point of view.

2.3.3.17 Level 2 PSA Probabilistic Modelling Framework: Containment Event Trees (CET)

76 A high level review of the AP1000 Level 2 PSA CETs against the expectations in T/AST/030 (Table A1-3.4) has been conducted during GDA Step 3.

77 The Level 2 PSA documented in Ref. 2 indicates that CETs are not linked fault tree type. This is different to the CAFTA model which appears to present a fully linked fault tree Level 2 model, which however is not documented in detail in any of the references seen during GDA Step 3. So, in order to continue with the detailed assessment of the Level 2 PSA during GDA Step 4, clarification is being sought from Westinghouse on the correspondence between the documentation and the model to be reviewed.

78 Not sufficient evidence was found of a systematic process for the selection of phenomena included in the CET and therefore, it is not clear up front why some events have been included or excluded from the CET. Questions have also been raised on some details of the approach used to evaluate the CET nodal probabilities. An initial review of the CETs suggests that human dependencies for events in the CET may have been ignored when generating probabilities for the CET nodes. This could be important and needs to be explored in further detail during GDA Step 4.

2.3.3.18 Source Term Analysis

79 A high level review of the AP1000 Level 2 PSA 'Source Term Analysis' against the expectations in T/AST/030 (Table A1-3.4) has been conducted during GDA Step 3.

80 Each CET sequence is mapped to a Release Category (RC). RCs are defined in terms of containment failure at different nodes in the CET. RCs are classified as 'large release' (and their frequency added to the LRF) for any CET sequence in which the containment fails or is bypassed. A common Source Term is then developed for each RC based solely on the mode (time) of containment failure without further discrimination of accident sequence characteristics or severe accident phenomena. As a result, there is a wide range of radiological release scenarios enveloped within each RC. This lack of detail may distort any evaluation or understanding of the relative contribution of systems, sequences or phenomenological issues to overall (risk and release frequency) results and may hinder a meaningful comparison against the Numerical Targets of the SAPs.

81 The Source Term for each RC is evaluated by selecting a single representative sequence. A justification of how the sequence is selected or of the adequacy of this simplified approach is not included in Ref. 2. No information has been found to identify and characterise the efficiency of important retention mechanisms, locations of deposited material, of the dominant factors contributing to differences in the releases among the RCs. Also, for the Source Term characterisation some assumptions have been made (e.g. releases are assumed to be continuous, have a constant release rate, are from the ground level and have no internal energy) for which the technical basis are not clear. Each Source Term is then presented in terms of cumulative and time-dependent release fractions of radionuclide groups to the environment however the assumed isotopic inventory of radionuclides used to translate the fractional releases to offsite dose is not described.

2.3.3.19 Presentation and Interpretation of the Level 2 PSA Results

82 The numerical results of the Level 2 PSA are presented in terms of:

- Large Release Frequency (LRF): frequency of all Release Categories except intact containment.
- Containment Effectiveness (Ceff): ratio of intact containment frequency to core damage frequency.

83 The documentation presented by Westinghouse for Step 3 compares the above results with targets derived from the United States Nuclear Regulatory Commission (US NRC) Safety Goals, rather than UK targets.

84 Sensitivity analyses have been performed but propagation of uncertainties (Level 1 parametric uncertainties, Level 2 uncertainties or combination of these) to the LRF has not been performed.

85 A limited scope Level 3 PSA analysis has been presented in Chapter 49 of Ref. 2 which uses as input the Level 2 PSA results in terms of frequency and Source Term for each RC and certain assumptions on demography and weather. The estimated site boundary whole-body dose and the acute red bone marrow dose are compared to the Westinghouse goal of <25 rems (0.25 sieverts), at a frequency not to exceed 1×10^{-6} /yr.

86 Some consideration of UK targets is provided in the 'Safety Assessment Principles Roadmap for AP1000 Design' (Ref. 13). In this document, Numerical Targets 5 to 9 of the SAPs are addressed based on the PSA presented in Chapter 19 of Ref. 3. Compliance is claimed on this basis without additional analysis. It was noted that the success sequences of the Level 1 PSA do not appear to have been considered for their potential low dose band contribution. Furthermore, it is not clear at this stage that the Level 2 PSA has been performed in a way that facilitates easy comparison with the Numerical Targets in the SAPs related to offsite consequences, i.e. it is not clear that a mapping of RCs to Dose Bands (HSE Target 8) and a mapping of RCs corresponding to a 'large accident' (societal risk in HSE Target 9) can be established.

87 A Severe Accident Management Design Alternatives (SAMDA) analysis is presented which is intended to support the ALARP demonstration. Potential modifications (design alternative) have been assessed in this analysis.

2.3.4 Requirements of GDA Guidance

88 The guidance to RPs on GDA required them, at Step 3, to include a PSA. Ref. 2 and supporting documentation fulfil that requirement.

89 HSE undertakings for Step 3 for PSA items 3.15, 3.22, and 3.23 of the GDA guidance (Ref. 16) 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).

90 In relation to 3.26, PSA is not a major overlap for the Environment Agency.

2.3.5 Use of Other Regulators Information

91 Westinghouse has provided a list of questions raised by US NRC during its assessment of the AP1000 PSA and the responses sent by Westinghouse. All of this will be reviewed and where relevant included in ND's assessment. The progress and findings of the assessment of the AP1000 PSA will be also discussed with the other members of the AP1000 Multi-national Design Evaluation Programme (MDEP) as / if required.

2.3.6 Plans for GDA Step 4 Assessment

92 It is intended that the Step 4 assessment will look in detail at all the areas reviewed at a high level in Step 3, using, as the basis, the original PSA documentation and all the additional information received in response to the TQs and ROs raised. All the technical areas of PSA will be addressed following the structure established in Appendix 1 of ND's PSA guide (Ref. 8). However, not each and every fault tree, event tree, supporting analysis or item of reliability data, will be examined in detail. Rather, the aim is to establish, by reviewing in detail a representative sample, whether the implementation of the methods and techniques used is adequate. In addition to this, specific items identified in Step 3 that require follow-up during the Step 4 assessment will be listed in the GDA Step 4 Project Plan for the AP1000 PSA.

2.3.7 Related Research

93 We have identified a potential need to research in the area of Human Reliability Analysis (HRA). The AP1000 HRA uses the well known THERP (NUREG/CR-1278, 1983) data but the AP1000 design, particularly for all control room post-fault actions uses interfaces that are very different to those assumed in the THERP data sets. ND needs to form a view on the work that would be necessary to evaluate THERP data against digital interfaces and whether some research work needs to be commissioned.

2.3.8 Technical Queries (TQ)

94 During Step 3 we have issued 85 TQs covering all aspects of the PSA (Ref. 14). All TQs have been acknowledged by Westinghouse and full or partial responses have already been provided for many of them. The responses to the TQs will form the basis for ongoing assessment (this of course does not preclude further TQs for greater detail, should they be needed or indeed issue of ROs or RIs).

2.3.9 Regulatory Observations (RO)

95 In two areas it has been clear that there are shortfalls that cannot be clarified via TQs. To address these the following ROs have been issued (Ref. 15):

- 'PSA Systems Analysis Guidelines and Systems Models'. This RO addresses the observed incompleteness in the AP1000 systems fault tree models.
- 'Fire PSA'. This RO addresses the fact that the AP1000 Fire PSA, both approach and data used, are out of date.

2.3.10 Regulatory Issues (RI)

96 In the PSA area we have not identified any failings or shortfalls of sufficient magnitude to warrant the issue of an RI for the PSA itself.

2.3.11 Potential Exclusions

97 No firm exclusions have been identified during the assessment in GDA Step 3. However, the potential for exclusions or conditions related to PSA is discussed in Section 2.3.1 above.

3 CONCLUSIONS AND RECOMMENDATIONS

98 Westinghouse has provided a PSA as part of the AP1000 submission to HSE-ND for GDA. During Step 3 a high level review of all the PSA technical areas against the tables contained in Appendix 1 of ND's PSA guide (Ref. 8) and a detailed review of the PSA Task on 'identification and grouping of internal initiating events during operation at power' have been conducted. From the AP1000 assessment work done so far I conclude the following:

99 The current PSA with its current scope provides part of the basis to interpret the risk associated with this reactor and where the main design strengths and relative vulnerabilities may lie. However, shortcomings in scope, methods and data identified during Step 3 indicate that work will be required to complete and modernise the PSA so that it can provide a more adequate input into the demonstration that the risk associated with the AP1000 is ALARP.

100 In addition, I believe that further development will be required in the future to provide the PSA with the level of detail which can support modern decision making tools such as a Risk Monitor

101 Having said that, the current Core Damage and Large Release Frequencies presented by Westinghouse provide a degree of confidence that the Societal Risk associated with the AP1000 (as represented by Target 9 of the SAPs) lies below the Basic Safety Level (BSL). At the moment, I do not have any reason to believe that this position will change dramatically once the PSA has been completed and updated.

102 Finally, I believe that Westinghouse's PSA team are making a significant effort to establish a programme of work to update the AP1000 PSA and bring it to modern standards. They appear to be listening and taking on board feedback given by the ND team and they seek and value the opinion of other peers in the US. Discussions between ND and Westinghouse's PSA team during GDA Step 3 have continually been open and positive.

103 Overall, I see no reason, on PSA grounds, why the AP1000 should not proceed to Step 4 of the GDA process.

104 From the AP1000 PSA assessment work done so far I recommend the following:

Recommendation 1: All the items identified in Step 3 as important to be followed up should be included in ND's GDA Step 4 Project Plan for the AP1000 PSA.

Recommendation 2: Considering the (extensive) current, planned and expected developments of the AP1000 PSA, two technical exchange workshops should be scheduled during GDA Step 4 to discuss in depth the PSA work being done by Westinghouse in the different areas including methods, sources of data and progress. The information compiled from, and outcome of, these workshops should be used to inform ND's Step 4 assessment and its final (GDA Phase 1) position regarding the AP1000 PSA.

4 REFERENCES

1 *New Reactor Build – Westinghouse AP1000 Step 2 PSA Assessment.* ND Division 6 Assessment Report No. AR08/009, HSE, March 2008. TRIM Ref. 2008/86523.

2 *UK AP1000 Probabilistic Risk Assessment.* UKP-GW-GL-022, Revision 0, Westinghouse Electric Company LLC, May 2007.

3 *AP1000 European Design Control Document.* EPS-GW-GL-700, Revision 0, Westinghouse Electric Company LLC, February 2009.

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

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

6 *Safety Assessment and Verification for Nuclear Power Plants.* IAEA Safety Standards Series, Safety Guide NS-G-1.2, International Atomic Energy Agency (IAEA), Vienna, 2001.

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

8 *Probabilistic Safety Analysis, Technical Assessment Guide.* T/AST/030, Issue 3, Health and HSE Nuclear Directorate, February 2009.

9 *Review of the AP1000 PSA for Step 3 of GDA.* JEL1-HSE-0803, Rev 0, Jacobsen Engineering Ltd, October 2009. TRIM Ref. 2009/434983.

10 *Review of the UK AP1000 PRA – Internal Initiating Events during Full Power Operation.* JEL2-HSE-0309, Rev 1, Jacobsen Engineering Ltd, Stetkar J, July 2009. TRIM Ref. 2009/434989.

11 *Generic Design Assessment Step 3 – Review of Human Reliability Assessment for the AP1000 PSA.* PR-2152-1, Greenstreet Berman / Synergy (Consortium), August 2009. TRIM Ref. 2009/415396.

12 *AP1000 Probabilistic Safety Analysis - GDA Step 3 Assessment Wrap-up Meeting.* Nuclear Directorate Division 6 Contact Report No CR09148, HSE-ND, August 2009. TRIM Ref. 2009/347567.

13 *Safety Assessment Principles Roadmap for AP1000 Design.* UKP-GW-GL-741, Rev 0, Westinghouse Electric Company LLC, November 2008.

14 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 3.* HSE-ND, November 2009. TRIM Ref. 2009/358248.

15 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 3.* HSE-ND, November 2009. TRIM Ref. 2009/358257.

16 *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	Interpretation	Comment
Fault analysis: PSA – Need for a PSA – FA.10 "Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis"	This principle sets the framework and requirements for a PSA study. The overriding aim of the PSA assessment is to assist ND judgements on the safety of the facility and whether the risks of its operation are being made as low as reasonably practicable.	Addressed in paras 5 to 10, 22 to 25 and 99 of this report.
Fault analysis: PSA – Validity – FA.11 "PSA should reflect the current design and operation of the facility or site"	This principle establishes the need for each aspect of the PSA to be directly related to existing facility information, facility documentation or the analysts' assumptions in the absence of such information. The PSA should be documented in such a way as to allow this principle to be met.	Addressed throughout this report but in particular in paras 30, 32 and 61.
Fault analysis: PSA – Scope and extent – FA.12 "PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site"	In order to meet this principle the scope of the PSA should cover all sources of radioactivity at the facility (e.g. fuel ponds, fuel handling facilities, waste storage tanks, radioactive sources, reactor core, etc), all types of initiating faults (e.g. internal faults, internal hazards, external hazards) and all operational modes (e.g. nominal full power, low power, shutdown, start-up, refuelling, maintenance outages).	Addressed in paras 7, 22, 27, 33, 34, 53, 54 and 61 of this report.
Fault analysis: PSA – Adequate representation – FA.13 "The PSA model should provide an adequate representation of the site and its facilities"	The aim of this principle is to ensure the technical adequacy of the PSA. Inspectors should review PSA models, data and results to be satisfied that the PSA has a robust technical basis and thus provides a credible picture of the contributors to the risk from the facility.	Addressed in paras 35 to 81 of this report.
Fault analysis: PSA – Use of PSA – FA.14 "PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities"	The aim of this principle is to establish the expectations on what uses the duty-holders should make of the PSA to support decision-making and on how the supporting analyses should be undertaken.	Addressed in paras 5, 32, 87, 99 and 100 of this report.

SAP	Interpretation	Comment
Numerical Targets **Target 7:** Individual risk to people off the site from accidents **Target 8:** Frequency dose targets for accidents on an individual facility – any person off the site **Target 9:** Total risk of 100 or more fatalities		Addressed in paras 83 to 86 of this report.
NT.2		Not addressed in GDA Step 3.

Annex 1 – Probabilistic Safety Analysis – 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-AP1000-045	28 Sept 2009	'PSA Systems Analysis Guidelines and Systems Models'	Issued.	Step 4
RO-AP1000-044	28 Sept 2009	'Fire PSA'	Issued.	Programme: Step 4 Detailed analysis: Phase 2

Annex 2

Detailed assessment against T/AST/030 expectations

Additional information on the assessment of the AP1000 PSA conducted during Step 3 of the Generic Design Assessment (GDA) is presented below under the headings of the 'Table of Assessment Expectations' in Appendix 1 of the HSE Nuclear Directorate's (ND) Probabilistic Safety Analysis (PSA) Technical Assessment Guide (TAG) (Ref. 8). Points arising from this step of the assessment where clarification or additional information have been sought have been the subject of Technical Queries (TQ) or Regulatory Observations (RO) and will be tracked to completion through a purpose designed GDA administrative system.

Unless otherwise stated references to section or chapter numbers relate to the AP1000 PSA report (Ref. 2) supporting the AP1000 GDA submission (Ref. 3).

Further details of the review work done can be found in Refs 9 to 11.

It should be noted that for most of the assessment expectations in ND's PSA guide (Ref.8) a detailed review (of a representative set of examples) still needs to be performed in Step 4 of the GDA, to verify that the stated intent / methods that the PSA has employed (as reviewed in Step 3 of the GDA) have been implemented as correctly, consistently and completely as possible.

Ref. 8, Table A1-1 General Expectations

1 Two points are worth highlighting up front. These are related to the PSA documentation and to the system to capture PSA assumptions.

2 The AP1000 PSA documentation is not consolidated. Some chapters of Ref. 2 have been superseded by Calculation Notes (including the PSA model itself). Also there is heavy reliance on, and reference to, the AP600 PSA documentation and supporting analyses. This is not a desirable position or in line with modern PSA standards. For each instance in which the AP1000 PSA relies on the AP600 PSA, justification of applicability may be needed to progress the assessment during Step 4. In any case, Westinghouse should develop, as soon as possible, a self-standing and comprehensive documentation for the AP1000 PSA.

3 For all technical areas of the PSA, ND's guide (Ref. 8) sets up an expectation that, in the absence of facility-specific information, all the assumptions made should be described and justified and a system should be in place to ensure that relevant assumptions are captured in future developments (e.g. of the design or procedures).

4 PSA assumptions could be affected by siting, design and construction, or operational matters (e.g. procedures, maintenance and testing strategies, training programmes, Main Control Room staffing and organisation, etc), and, thus, they need to be reviewed when detailed information becomes available. Therefore, a system to capture assumptions should really serve two purposes: 1) enable the assumptions made in the PSA to be captured during design, construction, procedure development, etc, and 2) to enable the latest available design and operational information to be transferred to the PSA so that assumptions (and models) can be reviewed accordingly. Such a system has not been visible during GDA Step 3.

Ref. 8, Table A1-1.2 PSA Scope

5 The purpose of the PSA that has been stated in Chapter 1 of Ref. 2 is to satisfy the United States Nuclear Regulatory Commission (US NRC) regulatory requirements that a design-specific Probabilistic Risk Assessment (PRA) be conducted as part of the application for

design certification (10 CFR 52.47(a)(i)(v)). No mention is made of the PSA to support the application to the UK HSE for the purposes of the GDA.

6 The scope of the AP1000 PSA has therefore been based on the regulatory requirements to obtain design approval for the US NRC in the mid 1990s. Thus, there are gaps between the PSA submitted and the requirements to support a safety case submission in the UK as set out in the TAG T/AST/030 (Ref 8).

7 The scope of the PSA included in Ref. 2 considers only potential core damage scenarios. Low consequence, high frequency sequences, potential risks from fuel ponds, fuel handling facilities and waste storage facilities are not included. Report 'AP1000 PRA Spent Fuel Pool Evaluation' (UKP-GW-GL-743 Rev 0), submitted separately to ND, addresses the risk associated with the spent fuel pond. This was not reviewed during GDA Step 3 and, thus, it is not clear how the results of this analysis integrate with the overall PSA results.

8 The treatment of external hazards has been based on screening out, without adequate justification, all external hazards other than earthquakes, which have been analysed via a qualitative Seismic Margins Analysis (SMA). As the Seismic Margins Assessment is a qualitative assessment, it cannot be directly integrated into the PSA. The internal fire and flooding analyses are quantitative but are also not integrated into the overall PSA results.

Ref. 8, Table A1-1.3 Freeze Date

9 A Freeze Date or Design Freeze Reference is not clearly stated or referenced in the PSA, and there are systems that have had design changes implemented and have not been reflected in Ref. 2 (e.g. 11kV power supplies for UK design, but PSA models 6.9kV power supplies).

Ref. 8, Table A1-1.4 Computer Codes and Inputs

10 Level 1 and Level 2 PSA computer codes and inputs are not well documented in the main PSA report (Ref. 2). For example, it is not clear in this report what code was used to quantify the Level 1 PSA and the documentation does not provide the drawings for all the inputs to the models (e.g. fault trees for the Initiating Events, Modules and Control and Instrumentation, C&I, are not provided). However, this is of little significance bearing in mind that although the original PSA was built in Westinghouse's in-house software, it was later transferred to the well established internationally used CAFTA software developed by the Electric Power Research Institute (EPRI). Nevertheless, the CAFTA model has certain limitations, e.g. event and fault trees are not linked (event trees are only drawings while the model consists of a series of top-logic fault trees constructed semi-manually). Many gates are not described. The model does not include the Fire and Flooding PSA models or models for the Initiating Events (IE) which have been analysed via fault trees. Because of this, additional assessment effort may be required during the detailed review in GDA Step 4.

11 In addition heavy reliance is made on the PSA and the supporting analyses performed for the AP600 design. The AP600 documentation and supporting analyses were not consulted during Step 3 but they will be key references to be used for the detailed assessment of the PSA during GDA Step 4 together with appropriate justification of the applicability of AP600 evaluations to the AP1000.

12 The expectations of the PSA TAG (Ref. 8) in relation to computer codes and inputs should be addressed on a case by case basis during the detailed assessment of the individual technical areas, as appropriate, in GDA Step 4.

Ref. 8, Table A1-2 Level 1 PSA

Ref. 8, Table A1-2.1 Identification and Grouping of Initiating Events

13 As well as a high level review of the AP1000 PSA task on 'Identification and Grouping of Initiating Events' against the expectations in T/AST/030 (Table A1-2.1), a detailed review has been conducted during GDA Step 3 to confirm whether the bases of the PSA are robust and to gain confidence on its completeness. The detailed review of the 'Identification and Grouping of Initiating Events' has focused exclusively on internal initiating events for the full power operating mode.

14 The review benefited substantially from meetings with Westinghouse's PSA team held at the Westinghouse offices in Monroeville from 23 to 27 March 2009 during which a number of items were raised with Westinghouse's team (PSA and engineering personnel). All these items are documented in Ref. 10. In some cases, the discussions effectively resolved the questions and concerns. Items that remained unresolved formed the basis for 34 TQs (21 on scope and 13 on grouping of initiating events). The background to each TQ is documented in Ref. 10.

15 The outcome of the review indicated that there may be a number of IEs missing from the PSA's Fault Schedule. Also, some IEs appear to have been grouped incorrectly.

16 An initial look at Westinghouse's responses suggests generally high quality responses and good explanations. From these Westinghouse has already identified and acknowledged the need for some PSA update work.

17 Westinghouse's responses to the 34 TQs will be reviewed in detail early in GDA Step 4 to confirm their technical adequacy. Further changes to the PSA may be required after this. In any case, Westinghouse should enhance the documentation of the Identification and Grouping of Initiating Events so that the traceability and completeness are evident.

Ref. 8, Table A1-2.2 Accident Sequence Development: Determination of Success Criteria

18 The main references for the derivation of success criteria for the AP1000 PSA were: Appendix A of the PSA report (Ref. 2), Chapter 15 of the AP1000 European Design Control Document (Ref. 3), and the AP600 PSA. It was noted that the references to Chapter 15 of the Design Control Document (DCD) in Table 6-2 of the PSA report were too vague to lead the reviewer back to specific analysis cases and that while references to Appendix A of the PSA report are more specific (the Appendix provides definitions of cases) the linkage between the defined cases and actual code runs and the configuration controls applied are not transparent. Reviewers should be able to trace backwards from a specific success criteria claim that they wish to review, through to the specific calculation which justifies the claimed success criteria. The availability of this information will be essential to undertake the detailed PSA review in GDA Step 4.

19 Also, the timing for operator actions should be justified by sufficient and representative thermal-hydraulic analyses, however, the traceability of the time windows used for the analysis and quantification of the Human Failure Events (HFE) modelled in the PSA to specific cases and analyses was not clear.

20 In response to the concerns above, Westinghouse has developed a roadmap which should provide the required transparency and traceability. This roadmap will be tested early in Step 4 by assessing in detail the success criteria for two initially selected accident sequences.

21 ND's PSA guide (Ref. 8) requires that the thermal-hydraulic, neutronics (and any other) analyses used for derivation of success criteria should be performed on a best-estimate basis. Section 6.3.4 (Sequence Success Criteria Summary) of the PSA document (Ref. 2) however states that *"It is important to note that, in general, these are not best-estimate*

success criteria. Criteria have been selected to bound the spectra of conditions identified in Appendix A as being important for the various event categories, in order to avoid quantifying uncertainty bounds for the success criteria". It is therefore not clear the impact of the stated conservatisms in the success criteria on the overall PSA results.

22 Finally, some clarification will be required to be able to understand and trace the information contained in the tables in Chapter 6 of Ref. 2.

Ref. 8, Table A1-2.3 Accident Sequence Development: Event Sequence Modeling

23 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 already discussed above there is an issue with the traceability of the thermal-hydraulic analyses supporting event sequence definitions.

24 The link between the various headings / nodes of the event tree and the potential operational and emergency procedures needs to be clear. In the absence of fully developed procedures, the assumptions regarding any procedures to be developed have to be explicit and justified. Each event class section of Chapter 4 of Ref. 2 has a sub-section clearly identifying operator actions which have been credited. However, it is not very clear what the basis for the choice of the operator actions credited is. Section 30.1 Human Reliability Analysis (HRA) of Ref. 2 states *"The AP1000 human reliability analysis (HRA) is the same as was provided in Chapter 30 of the AP600 PRA. There are no new operator actions modelled in the AP1000 PRA. The operator actions, available action times and other associated assumptions made in the AP600 HRA can be applied to the AP1000"*. Therefore, the AP600 study (together with the justification of its applicability to AP1000) will be a key reference to be used for the detailed assessment of the PSA during GDA Step 4 (although an initial look at Chapter 30 of the AP600 PRA suggests that no significant additional information is provided there). For the detailed PSA review during GDA Step 4 ND will also need the AP1000 Emergency Operating Procedures (EOP) and any other relevant procedures that the operators might use during the course of an accident. In any case Westinghouse should establish, as soon as possible, the link between the accident sequences delineated in the PSA and the procedures designed to be used by the operators during the course of an accident.

25 In principle it appears that the identification and treatment of dependencies in the AP1000 sequence analysis is reasonable. Further confirmatory review will be required during GDA Step 4. However, there is an area that has not come across in a transparent fashion; this is related to dependencies that may arise because of the specific characteristics of the design. An example is dependencies between IEs and mitigating systems due to software failures (including common cause software failures between the control system and the protection system). Whether there is evidence that this type of dependencies (called 'subtle dependencies' in T/AST/030) have been searched for systematically by Westinghouse may be checked on a case-by-case basis during GDA Step 4. In the mean time, and in order to address some general concerns regarding the extensive use of digital systems in modern designs, Westinghouse should explain whether and how the potential dependencies between initiating events and mitigating systems due to software failures have been evaluated and reflected, if appropriate, in the PSA.

26 Most event trees contain a header Containment Heat Removal (CHR) following success of the reactor cooling systems (passive reactor heat removal, RHR, normal RHR or recirculation). This is because (in the longer term) containment heat removal is necessary to evacuate the residual heat from the reactor. Sequences with failure of this final CHR header are stored under the Late Containment Failure (LCF) end state which has a frequency of 6.92×10^{-8} /yr. However, these sequences are not added to the Core Damage Frequency (CDF) or carried over to the Level 2 PSA. This appears to imply that

air cooling of the containment is being claimed but it is not clear whether or not this is justified by supporting transient analysis. Westinghouse needs to demonstrate a safe stable state of the plant at the end of the (selected) PSA mission time in sequences where success of reactor cooling systems is claimed. Further development in the event trees may be needed.

Ref. 8, Table A1-2.4 Systems Analysis

Ref. 8, Table A1-2.4.1 General Methodological Aspects

27 In PSA system analysis it is very important that the approach used for the definition of system boundaries is stated and is adequate. This is because there is a need to ensure modelling consistency among the different system analysts so that there are neither gaps, nor overlaps between the different system models. This would normally be dealt with in the System Analysis Task Procedure. However, the AP1000 PSA Fault Tree Guidelines (Chapter 7 of Ref. 2) do not explicitly provide an approach for the identification and definition of system boundaries. This may lead to additional effort during GDA Step 4, as the review will have to be conducted using detailed system drawings in all cases (e.g. Piping and Instrumentation Diagrams, P&ID) instead of the PSA descriptions and simplified diagrams and cross-reviews between the different systems will need to be undertaken.

28 In PSA system analysis it is also very important that the approach used for the definition of component boundaries is stated and is adequate. Again this is because there is a need to ensure modelling consistency among the different system analysts and also with the data analysts. In Chapter 7.3.5 of Ref. 2 standardised power and control boundaries and failure modes for 4 types of components have been defined but not for all component types included in the PSA models. Component boundaries should be defined for all component types modelled so that the failure modes associated with each component type can be checked. Component boundaries in data sources can then also be checked against the boundaries of the components modelled in the PSA to confirm the applicability of the data used.

29 In relation to the approach used for the inclusion of pre-accident Human Failure Events (HFE) (e.g. misalignments and mis-calibrations) in the AP1000 fault trees, Chapter 7.3.4.1, of Ref. 2 describes the criteria for identifying this type of HFE. The review team believes however that the method for identifying these types of failures is not appropriate. First of all, the method seems to deal exclusively with mispositions of valves but does not appear to consider at all that pre-accident human errors can lead to valves, pumps, bus-bars, etc, being left de-energised (and unable to actuate on receipt of a safety signal). Equally, mis-calibrations are mentioned but not addressed in any detail. It is also believed that the criteria for screening out these types of failures are weak. For example, the screening criteria indicate that misposition of valves should only be included in the fault tree if the HFEs could seriously degrade or fail the system. This screening criterion is not adequate since the impact of a valve misalignment on the failure of the system will be different for different success criteria in different initiating events or sequences. Equally, the impact of a misalignment on the overall risk depends on each sequence and the amount of plant available to cope with the event. Also, the criteria for screening out pre-accident HFEs rely on testing intervals and strategies and alarm design and operational philosophy that have not yet been decided for the AP1000. Therefore, it is possible that the current criteria have the potential to screen out of the models latent HFEs with significant risk contributions (in particular Risk Achievement Worth). Indeed, a more detailed look at some system fault trees has identified that no pre-accident HFEs have been included in the AP1000 PSA models, thus hindering the ability of the PSA to provide support for the development of the surveillance, maintenance and testing strategies, design of the control room displays, development of procedures, etc.

30 The AP1000 Fault Tree Guidelines (Chapter 7 of Ref. 2) require including at least one Common Cause Failure (CCF) in each system model without further guidance. More detailed CCF analysis is reported in Chapter 29 of Ref. 2. The guidance provided to the fault tree analysts is not sufficient to ensure complete and correct CCF modelling and it is not in accordance with modern PSA standards. Guidelines on what components are subject to CCF (and thus which CCF events should be explicitly modelled) or what other CCF aspects the system analyst should consider when developing the system models should be provided. At the moment, it is not clear that the modelling of CCF is consistent throughout. This will need to be checked in detail in GDA Step 4. CCFs could be important risk contributors and, therefore, this issue has potentially high importance.

31 No discussion on the potential inclusion of structural failures could be found except for a related statement on Chapter 7.3.1.1 of Ref. 2 that indicates *"Piping faults considered to be credible include: pipe plugging, orifice plugging, and plugging from chemical crystallization due to the loss of the pipe heat tracing system"*. A discussion of potential structural failures and consequential structural failures (e.g. pipe whip) should be provided together with a justification of why these have not been modelled in the PSA. It should be noted that structural failure probabilities are provided in Table 32-1, Generic Data Base, of Ref. 2, thus, the concern noted here relates exclusively to the modelling of these failures in the fault trees.

32 ND's PSA guide (Ref. 8) expects that the approach for the inclusion of passive component failures into the systems should be stated and adequate. The term passive component failures refers both to the failures of passive components discussed in the previous paragraph and also to the failures of components to remain in the required position. Chapter 7.3.1.1 of Ref. 2 describes Westinghouse's rules for including passive failures. For example, the guidance in Chapter 7 prescribes that passive failures that affect a single loop or train do not need to be included except where potential failure of an entire system is possible. The review team considers that these rules are not adequate for the AP1000 whose high level of safety claimed mainly relies on the availability of passive systems. Therefore, any failure that blocks the paths of these systems has a potentially high relative risk significance and should be modelled. It should be noted that probabilities for these failures are included in Table 32-1 (Generic Data Base) of Ref. 2, thus, the concern noted here relates exclusively to the modelling of these failures in the fault trees.

33 The AP1000 Fault Tree Guidelines (Chapter 7 of Ref. 2) do not present a list of the failure modes applicable to each component type. Therefore, it is not clear whether this has been addressed consistently throughout the fault trees and will be checked during the detailed assessment in Step 4. It should be noted that the list of failure modes applicable to each component type is presented in Table 32-1 (Generic Data Base) of Ref. 2.

34 Normally, it would be expected that the PSA documentation includes a general description of the way in which circular logic (also known as logic loops) has been dealt with in the fault tree models. Although Ref. 2 does not include a general description of the way in which circular logic has been addressed in the AP1000 PSA, Chapter 6 (Success Criteria) identifies independent fault trees for which boundary conditions are provided and it should be noted that for some systems discussion of circular logic is provided in the 'Assumptions and Boundary Conditions'.

35 The expected level of detail of the system fault tree models in modern PSA is such that, first, it is consistent throughout the systems analysis, second, it is sufficient to ensure that the models are realistic, that the logic of the models is correct, that all the dependencies are captured, that the resulting cut sets for failures of the system reflect combinations of failures that can be easily understood, and that the data used is applicable to the boundary selected for each component (basic event) in the PSA. A significant concern raised during the review is that the AP1000 Fault Tree Guidelines (Chapter 7 of Ref. 2)

promote simplification of the model structure such that understanding of the fault tree logic may be compromised, i.e. basic events are modelled out of step to the logical sequence described by the gate descriptions. It also appears that modular events have been used throughout and it is not clear if the contributors to the modules are readily accessible – some information can be extracted from the Table(s) entitled 'Fault Tree Basic Event for…' in Chapters 8 to 28 of Ref. 2 but this is not sufficient to ascertain that the model internal to the module is correct and complete. This may compromise understanding the fault tree logic. For example:

- Cases have been found where unavailabilities due to testing and maintenance (T&M) are embedded in module events[1], which is generally not recommended, as the contributions from these T&M basic events are difficult to identify in cut sets, importance / sensitivity analyses, and are easily overlooked when changes are made.
- There are no detailed descriptions of components and basic events or graphical representations of the individual constituents included in each module. The current documentation therefore does not provide details of the basic events within the modules and evidence that the dependencies are properly captured.

36 Fault Tree models should remain logical and simplification / modularisation should be avoided as they result in models that are difficult to understand and review for completeness, and can lead to application problems when changes to elements in a module get overlooked.

37 Finally, it was noted that the CAFTA model contains a significant number of gates without description.

Ref. 8, Table A1-2.4.2 Specific for Each System Model

38 Whether the AP1000 PSA meets the expectations set up in Table A1-2.4.2 of ND's PSA guide (Ref. 8) will be confirmed during GDA Step 4, since this will require detailed review of the system fault trees. However, some initial findings have been raised from the high level review of Step 3. These are summarised in the following paragraphs.

39 ND's PSA guide (Ref. 8) indicates that a simplified system diagram should be presented for each system modelled in the PSA including all the components modelled (adequately labelled and without omission) and clearly indicating the system boundaries and interfaces with other systems. For some AP1000 systems, reference is made to detailed system descriptions and P&IDs that can be found in the AP1000 Design Control Document (Ref. 3). For other systems some incomplete simplified diagrams (e.g. they do not show all trains, do not include component labels, etc.) have been included. As, already indicated above, this may lead to additional effort during GDA Step 4 since, instead of being able to rely on simplified diagrams (with some spot checks of some detailed system drawings), all the system fault trees will need to be assessed starting from the detailed system drawings.

40 It is to be expected that the design of some AP1000 systems may not be finalised yet; in these cases all the assumptions on system design should be stated. From the system descriptions in Ref. 2, it cannot be inferred whether part of the information is assumed, i.e.

[1] Examples of these are module events AD1MOD05 and 06, AD2MOD01 and 02, AD3MOD03 and 04, which represent the hardware failures of Stage 1, 2 and 3 ADS valves. Each of these events lumps together the following: failure of two Motor Operated Valves (MOV) to open, failure of two circuit breakers to close, failure of two solid state relays to operate and two (generic) unavailability events. Another example is module event TCBMOD01B (described as mechanical failures of the Turbine Building Closed Cooling Water System, TCS, pump 01B) which includes: failure to run of a motor driven pump, failure to open of a check valve, failure to start a motor driven pump, test and maintenance unavailability of 2 loops, failure to close of a circuit breaker, spurious opening of a circuit breaker and failure to operate of a solid state relay.

no specific assumptions on system design have been found. In addition, no process could be found where assumptions are captured to enable verification following completion of the design. This is a general finding throughout all areas of the PSA and has been discussed in para. 4 of this Annex.

41 ND's PSA guide (Ref. 8) sets up the expectation that the information on dependencies for each component should be transparent (including the support systems / actuation signal interface points). Although AP1000 system dependency matrices have been provided, these do not explicitly state which components mark the interface between the systems (e.g. front line and support systems). This finding is closely related to general methodological concerns raised above i.e. the fact that the approaches for the definition of systems boundaries and component boundaries are not explicitly stated and also the fact that simplified diagrams with sufficient level of information to identify where a system stops and the next systems start (e.g. its support systems) have not been provided.

42 Tables i-5 (table number may be different for some systems) in Chapters 8 to 28 of Ref. 2 include information on testing assumptions. This is, in general, limited to a statement of expected testing frequencies but it is not detailed enough to understand system testing strategies, the types of tests to be carried out and what failure modes they test, the necessary realignments (including impact on other systems, if relevant), etc. Westinghouse will need to provide urgently additional available information on system test for those systems that will be reviewed in detail in GDA Step 4.

43 Tables i-6 (table number may be different for some systems) in Chapters 8 to 28 of Ref. 2 include information on maintenance assumptions. This is, in general, limited to a statement of expected maintenance frequencies and expected outage times but it is not detailed enough to understand system maintenance strategies, the types of maintenance to be carried out, the necessary realignments (including impact on other systems, if relevant), any post-maintenance testing required etc. Westinghouse will need to provide urgently additional available information on system maintenance for those systems that will be reviewed in detail in GDA Step 4.

44 It is not clear whether all relevant component failures have been correctly included in the fault trees since no systematic analysis of failures (such as Failure Modes and Effects Analysis, FMEA) or clear description of failure modes that have been modelled (and those that have been excluded) have yet been provided. Detailed assessment of the system models in GDA Step 4 will be required to confirm this.

45 The way in which unavailabilities due to Testing and Maintenance (T&M) have been included in the fault trees has raised concerns. The modelling solution chosen by Westinghouse consists of aggregating all the T&M unavailability for multiple trains into a single (standby) train. No mutually exclusive rules, 'not logic' or post-processing appears to have been included in the quantification to remove (assumed) forbidden combinations of maintenance activities among systems. While correctness of the current models should be checked during the detailed assessment in GDA Step 4, modern practices would suggest symmetric modelling by including specific T&M unavailabilities for each train. In addition, T&M unavailability during shutdown Plant Operational States (POS) does not appear to have been considered. If this is confirmed during GDA Step 4, the implication would be that the current AP1000 shutdown PSA is inadequate and unable to provide an estimation of the risk associated with those POSs.

46 The fault tree models should include those hardware failures that contribute to the Human Failure Events (e.g. failure of the alarms or indications). For the AP1000 PSA these are modelled in a very simplistic manner. A failure probability of 1×10^{-6} /d for the overall failure of relevant alarms and indications has been used throughout the models without consideration of the available instrumentation in each case.

47 Some intersystem common cause failures have been included. While these appear to have been derived in accordance with the general approach, the assessment during GDA Step 3 has not checked the completeness of the CCF modelling. This is an important aspect to be followed up during the detailed review in GDA Step 4.

48 Finally, it is worth mentioning that some areas of the documentation of the fault trees should be improved. For example, Chapter 5 of Ref. 2 provides a table of fault trees with transfers to support systems. However only fault tree denominations are listed without descriptions, which hinders the usefulness of this table; the fault tree descriptions should be added. In addition, it is not yet known whether these fault tree denominations are consistent with those used in the CAFTA model. Tables entitled 'Fault Tree Basic Events' in Chapters 8 to 28 of Ref. 2 should also be improved by including the complete name and description of each basic event in the fault tree.

Ref. 8, Table A1-2.5 Human Reliability Analysis (HRA)

49 A review of the AP1000 PSA task on 'Human Reliability Analysis' against the expectations in T/AST/030 (Table A1-2.5) has commenced during GDA Step 3 with the support of PSA specialists looking at the HRA modelling, and Human Factors specialists looking at human factors background and substantiation aspects of the HRA. So far, the review of the HRA (documented in Refs 9 and 11) has raised the concerns discussed in the following paragraphs.

50 It should be noted that Westinghouse has been briefed about the contents of Ref.11 but have not yet had the opportunity to see and comment on this report. Therefore, formal TQs / ROs have not been raised yet. This review work will continue in GDA Step 4 and will be done in coordination with the Human Factors assessment team. For the purpose of this assessment report, the items discussed below which are not strictly related to the PSA model should be considered preliminary.

51 One of the key findings in the HRA area is related to the identification and modelling of Type A HFEs (pre-accident human errors that cause equipment to be unavailable when required post fault, e.g. misalignments and miscalibrations). This has been discussed at length above.

52 Type B HFEs are those human actions that either by themselves or in combination with other equipment failures lead to IEs. Some Type B HFEs are quantified in Chapter 30 of Ref. 2. These, as well as modelling consistency of Type B HFEs in the initiating event frequency assessment, should be checked in detail during GDA Step 4. Explicit analysis of Type B HFEs is generally performed for Low Power and Shutdown modes, however, Chapter 54 of Ref. 2 does not document the derivation of the low power and shutdown initiating events and, therefore, this needs to be followed up during GDA Step 4.

53 Initial concerns have been raised on how the diagnosis and decision aspects of the human actions have been dealt with in HRA. Westinghouse's analysis assumes that the diagnosis and response aspects of the post-fault actions will be straightforward responses to alarms and entries into defined procedures. This appears likely to be optimistic or / and places considerable requirements on the detailed control room interface designs and information presentation and on the associated procedures.

54 Type C2 HFEs are those human actions during the accident that due to the inadequate recognition of the situation or the selection of the wrong strategy, make it worse (these are one type of errors of commission). ND's PSA guide (Ref. 8) sets up an expectation that those occasions for mis-diagnosis of the situation by the operators should be analysed systematically and HFEs resulting from identified credible mis-diagnosis should be modelled. In Chapter 30.5 of Ref. 2 the claim is made that errors of commission had been subject to a systematic, qualitative assessment. It appears that this analysis is

documented in report APP-GW-GLR-003 Rev. 1 on 'AP1000 Adverse System Interactions Evaluation Report', submitted separately to ND, which should be reviewed in GDA Step 4.

55 Standardised recovery probabilities are applied directly in the quantification of the Human Error Probabilities (HEP) and, depending on the stated time available, multiple recoveries are claimed from the Senior Reactor Operator and the Shift Technical Advisor. Best practice methods would suggest considering recovery factors taking into account the individual characteristics of the accident sequences / scenarios including all the human errors involved and the dependencies. Also, this recovery model assumes a structure of the operating crew which may not be correct for future operating AP1000 reactors. Therefore, considering the high impact of the recovery modelled used on the calculated HEPs, it is suggested that this be looked at in detail during GDA Step 4 in coordination with the ND's Human Factors team.

56 Time windows have been used, in HEP calculation, to allow more or less recoveries depending on the time available. Time windows have not been used to calculate the probability of the human response happening when it is no longer useful. In any case, an initial look at the way in which the time windows have been obtained has shown that there is little justification for them and it appears that these evaluations may be optimistic (against the claimed HEPs).

57 The HRA uses Technique for Human Error Rate Predication (THERP) data but the AP1000 design, particularly for all control room post-fault actions, uses interfaces that are very different to those assumed in the THERP data sets. The justification for use of this data, or provision of alternative data relevant to the AP1000 design, needs to be made. It may be that research is needed to address this.

Ref. 8, Table A1-2.6 Data Analysis

Ref. 8, Table A1-2.6.1 Initiating Fault Frequencies

58 ND's PSA guide (Ref. 8) sets up the expectation that the PSA documentation should state the criteria for the selection / precedence of data sources used for the analysis of Initiating Event (IE) frequencies. This information has not been found in Ref. 2. Without this information a thorough review of the adequacy of data sources, on a case-by-case basis, will be required during GDA Step 4.

59 Clearly, since there are no AP1000 Nuclear Power Plants (NPP) operating yet, it is essential that in cases where operational experience from 'similar' NPPs has been used in the evaluation of IE frequencies, its applicability is justified and the data used is auditable. For some Transient Initiators, Institute of Nuclear Power Operations (INPO) data for 2, 3 and 4 loops Westinghouse Pressurised Water Reactors (PWR) from 1984 to 1989 is recorded in Table 2A-7 of Ref. 2, including event dates. Westinghouse data from the same plant set has been used for the evaluation of Steam Generator Tube Rupture (SGTR) frequency. SGTR failure events are listed in Table 2A-3 of Ref. 2, however the calculation is not auditable. In addition, the calculation of the SGTR frequency for Steam Generators with tubes manufactured from Alloy 690 is not clear.

60 Furthermore, the operational experience used for the evaluation of IE frequencies covers a 5 year period starting 25 years ago. Concerns have been raised on the relevance of 20 to 25 year old data to a new plant design yet to be constructed. Concerns have also been raised regarding the limited amount of operational history used.

61 In relation to the frequencies of the various Loss of Coolant Accidents (LOCA) modelled in the PSA, it appears that generic industry data has been used for the analysis. Little or no justification is provided for the frequencies used and the determination of the frequencies is not auditable.

62 Overall, concerns have been raised about the general lack of auditability of the IE frequency analyses.

63 It is understood that Westinghouse has programmed work to update the IE frequencies. ND wishes to see and discuss with Westinghouse, during GDA Step 4, the programme to do this work, and the methods and data sources selected, to gain confidence that the next version of the IE frequency database is likely to meet ND's expectations.

Ref. 8, Table A1-2.6.2 Random Component Failures

64 Chapter 32 of Ref. 2 is a summary of the data used in the AP1000 PSA. This chapter refers to Chapter 32 Data Analysis for the AP600 PSA and to data derived from EPRI's 1993 Advanced Light Water Reactor Utility Requirements Document (ALWR URD). Thus, Chapter 32 of Ref. 2 does not, in itself, provide extensive detail of how the AP1000 PSA data has been derived. For example, there is no information on the identified component populations together with their characteristics.

65 Concerns with the identification of component boundaries have been discussed in the Systems Analysis section above. In line with that, no discussion of component boundaries has been included in Chapter 32 of Ref. 2 except for a limited description of the boundary for selected components that is provided in Table 32-1 under 'Remarks'.

66 For the evaluation of random component failure probabilities, Ref. 2 states the criteria for selection / precedence of data sources. Priority was given to the ALWR URD 1993 report. In that document it is stated that: *"For each component type and failure mode, the failure rates were extracted from the available sources, and a suitable value was selected based on judgment regarding applicability to the anticipated ALWR designs".* When ALWR URD failure data is not available, or deemed not applicable for AP1000, the data is obtained from 4 sources in the order listed. These are 1) NUREG/CR-2728 (1983), 2) IEEE Std 500 (1984), 3) NSAC-154 (1991) and 4) 'other sources' (such as an ENEA\ENEL paper from 1985). It is not clear what the criteria were for the choice of data sources and the order of precedence. No justification of applicability is documented in Ref. 2.

67 The calculation of the failure probabilities for the basic events in the PSA is documented individually for each system in Table(s) entitled 'Fault Tree Basic Events for…' in Chapters 8 to 28 of Ref. 2 rather than in the Data Analysis Documentation. Mission times and test intervals used for the reliability calculations are also shown in these tables. The review identified that a mission time of 2.5 hours has been applied to Diesel Generators which may be optimistic as it is based on an average Loss of Off-Site Power (LOOP) of 2.5 hours. (Note that the Diesel Generator day tanks only have sufficient fuel to run for a maximum of 4 hours). Initiating Events with LOOP or consequential LOOP greater than 2.5 hours may therefore not be adequately modelled. The adequacy of the missions times assigned to the components need to be reviewed in detail during GDA Step 4.

68 Table 32-5 of Ref. 2 provides the Master Data Bank which lists the parameters according to Component and System type codes / parameter codes with failure mode description and failure rate. A list of the basic events with the respective parameters assigned is provided individually for each system in Table(s) entitled 'Fault Tree Basic Events for…' in Chapters 8 to 28 of Ref. 2. All these tables generally provide a non-specific reference to a document or a PSA chapter. Finally no uncertainty bounds or error factors are presented in any of these tables. Instead these are dealt with in Chapter 51 of Ref. 2. All this may point to some issues in the traceability in the data.

69 It is understood that Westinghouse has programmed work to update the PSA reliability database. ND wishes to see and discuss with Westinghouse, during GDA Step 4, the programme to do this work and the methods and data sources selected to gain confidence that the next version of the PSA reliability database is likely to meet ND's expectations.

Ref. 8, Table A1-2.6.3 Unavailabilities Due to Testing and Maintenance (T&M)

70 Generic unavailbility data used for the AP1000 PSA has been derived from EPRI's 1993 ALWR URD. Table 32-5 of Ref. 2, Master Data Bank, lists some T&M unavailabilities (but not all) according to Component and System type codes. Specific system T&M unavailabilities can be seen in Table(s) entitled 'Fault Tree Basic Events for…' in Chapters 8 to 28 of Ref. 2. Some of these have been embedded into module events. As for the random component failure data (above) this may point to some issues in the traceability in the data and will need detailed review during GDA Step 4.

Ref. 8, Table A1-2.6.4 Common Cause Failures

71 Chapter 29 of Ref. 2 presents the analysis of Common Cause Failures. Both intra-system and inter-system CCFs are considered. The Multiple Greek Letter (MGL) method has been used for the evaluation of CCF probabilities in the AP1000 PSA. This is a well established approach although no detailed assessment of the method and the way it has been applied has been undertaken yet.

72 The CCF parameters used to quantify the CCF probabilities for each component type and different system configurations are presented in Table 32-4 of Ref. 2. This data has been extracted, in general, from EPRI's 1993 ALWR URD. For some components such as check valves and catastrophic failure of motor operated valves, the source of the MGL parameters is a 1985 document. Therefore, it is felt that the CCF data used may be outdated as more recent generic data for MGL parameters is available.

73 The current CCF analysis has assumed, and taken into account, some features that could serve as defences against CCF in order to screen out certain types of CCFs. This is discussed in Section 29.3 of Ref. 2. The review during GDA Step 4 should look in detail at the assumptions made for screening out some CCF types and any other assumptions made in the CCF analysis.

74 The list of CCF events appears in Chapter 29 of Ref. 2. No uncertainty bounds or error factors are presented except for the components listed in Table 29-1 (electrical components with low CCF rate).

75 It is understood that Westinghouse has programmed work to update the PSA reliability database but it is not clear whether this effort will also address CCF. Nevertheless it is felt that this data should also be updated.

Ref. 8, Table A1-2.7 Internal and External Hazards PSA

Ref. 8, Table A1-2.7.1 Screening of Hazards and General Methodological Aspects

76 The analysis of hazards for the AP1000 PSA presented in Ref. 2 does not start with a complete list of internal and external hazards. In each case, a number of specific hazards are listed as a starting point without appropriate justification for the UK expectations as discussed below.

77 No discussion on general screening criteria for internal hazards is provided in Ref. 2. There is no discussion of the reason for limiting the hazards considered to those discussed in the analysis or why the hazards not considered are not applicable. Apart from internal fire and internal flood no analysis or screening of additional potential internal hazards (e.g. turbine missile, dropped loads) has been documented in Ref. 2.

78 For external hazards a Seismic Margins Analysis (SMA) is performed. According to Chapter 58 of Ref. 2 it seems that siting criteria is used as an argument to screen out the remaining external hazards from the initial list (i.e. if their frequency is $<1.0 \times 10^{-6}$/yr)

based on US NRC documents dated 1991. Discussions with Westinghouse suggest that the actual screening criteria used was frequency $<1.0 \times 10^{-7}$ /yr. In any case, the external hazards screened out on those basis were high winds, tornadoes, external floods and transportation and nearby facility accidents. As the AP1000 internal events CDF is 2.41×10^{-7} /yr and the Large Release Frequency (LRF) is 1.95×10^{-8} /yr, the adequacy of either screening criteria is questionable.

Ref. 8, Table A1-2.7.2 Analysis of Internal Fires

79 The methodology used for the AP1000 Fire PSA is EPRI's FIVE method and data with some enhancements. This method was developed in 1992 and has been superseded by NUREG/CR-6850, available in draft in 2001 and published in 2005. While many of the concepts are similar, the level of depth required by the newer approach, i.e. to search out new fire initiators, fire induced mitigating system damage, multiple spurious equipment operations, and degradation of operator reliability and inappropriate operator actions based on spurious indications, may not have been achieved by using FIVE; indeed, no evidence of this depth of analysis has been found in the documentation reviewed.

80 Furthermore, generic fire frequencies tend to be higher in NUREG/CR-6850. In addition, FIVE is essentially a focused screening tool not a Fire PSA methodology. As a result of applying FIVE, no detailed fire modelling has been performed (apart from the analysis of the Main Control Room, MCR).

81 While the reported fire CDF is only 5.6×10^{-8} /yr this represents approximately 25% of the CDF. Therefore, the potential to reasonably assess strengths and weaknesses in the design may have been compromised by the use of FIVE instead of a more modern method.

82 ND's PSA guide (Ref. 8) sets up the expectation that, if complete plant specific information is not available, all the assumptions made in support of the analysis should be identified (e.g. assumptions on ignition sources, amount of combustible material, control programmes for combustible and ignition sources, allocation of equipment / cables, fire barriers, separation, segregation, fire detection and suppression equipment, performance of the fire brigade, etc.). Much of the information used in the AP1000 Fire PSA is derived from the AP600 PSA. This was not reviewed during GDA Step 3. In any case, for any detailed assessment during GDA (Phase 2) up-to-date drawings of compartment boundaries, together with clarification and details for each compartment regarding ignition sources, amount of combustible material, allocation of equipment, etc, will be required.

83 In modern Fire PSA it is considered important that there are procedures in place for evaluating circuits and selecting cables required to support the operation of essential equipment. No AP1000 process, procedures or assumptions are referenced for determining potential fire impact on circuits.

84 Tables 57-1 and 57-2 of Ref. 2 provide a list of all compartments and indicate those which have been screened in or out. However, the reasons given for screening individual compartments do not always correspond to the screening criteria established, for example, 'negligible combustible loading' is used in some cases without consideration of 'fire impact'. The screening of fire compartments (including consistency with the screening criteria) should be reviewed in detail in the future.

85 For the calculation of fire frequencies for the compartments the AP1000 analysis uses the FIVE methodology and generic data. However, neither the weighting factors (to distribute generic plant-wide frequencies among the different compartments) nor their method of derivation based on compartment ignition source inventories are provided in Ref. 2. Also, the calculation of fire frequencies for all fire compartments is not documented explicitly. Whether all this information is included in the AP600 PSA report was not confirmed during

GDA Step 3. In addition, the use of the US generic data provided in the FIVE methodology has not been justified. Furthermore, such data is now superseded and should be updated with newer sources. Fire frequencies are listed in Tables 57-3 and 57-4 of Ref. 2 but these are only point estimates without characterisation of uncertainty.

86 In the AP1000 PSA no fire compartments have been quantitatively screened out. Therefore, there was no need to check the quantitative screening criteria or process.

87 In Fire PSA, once the set of compartments selected for detailed analysis has been established, the possible different fire scenarios in each compartment need to be identified and characterised together with the identification of the relevant initiating events. For this a detailed search for fire sources and targets, and analysis of fire growth and propagation, detection, human response and damage, would normally be carried out. No detailed analysis of individual ignition sources or specific fire modelling has been undertaken in the AP1000 Fire PSA. This is because four general fire scenarios have been defined for each fire compartment, all of them involving full room burnout (except for the MCR).

88 The AP1000 PSA documentation addresses spurious actuations of equipment caused by fire. However the method used to identify potential spurious actuation (and combinations) and their associated consequences is not discussed. The completeness of the current analysis is therefore in question.

89 The fact that the scenarios evaluated involve full room burnout could indicate that explosions may have been implicitly considered, however potential consequences beyond the compartment boundary have not been addressed. Equally, potential fire caused missiles and their impact are not discussed in Ref. 2.

90 Analysis of inter-compartment fire propagation has been conducted in the AP1000 PSA. For this, a deterministic screening has been applied if there is no penetration or the exposing compartment combustible loading is <20000 Btu/ft^2. This is based on the FIVE methodology. However FIVE Section 5.3.6 also requires automatic detection in the fire compartment and assurance that there is no combustible concentration at the inter compartment barrier. Neither of these criteria are considered for the AP1000. Furthermore the latest NUREG/CR 6850 methodology requires the determination of the temperature of the hot gas layer rather than relying on average combustible loading.

91 Multi-compartment scenarios which cannot be screened-out are carried onto the next stages of the Fire PSA. The initial multi-compartment analysis is performed assuming whole room damage. In general most scenarios present negligible risk with the exception of specific scenarios in the containment (which are evaluated further). No quantitative screening criterion has been specified for discontinuing the analysis.

92 The last stage of the Fire PSA analysis is the actual probabilistic modelling consisting of identification of initiating events, accident sequence modelling (including revision of the fault trees and data as appropriate) and quantification for each identified scenario. This should be documented in detail.

93 The documentation of the AP1000 Fire PSA (in Ref. 2) does not provide evidence that a systematic search for the initiating events caused by fire in each compartment has been undertaken. Evidence that the most onerous initiating event has been selected to be the basis for the quantification of each fire scenario should be provided and the rationale for this selection should be clear. The AP1000 PSA does not meet this expectation. In addition, there is no indication that the internal events PSA model has been examined to ensure that all potentially risk significant fire induced failure modes have been captured.

94 No discussion of the post fire human reliability analysis is provided in Chapter 57 of Ref. 2 for fire scenarios in the plant and containment (except for two specific actions credited post fire, i.e. ‘Operator deactivates the Protection and Safety Monitoring System, PMS, division involved in the fire’, and ‘Operator opens manual valve to sprinklers in

containment', described in Attachment 57B of Ref. 2). For the MCR scenarios it appears that a generic HEP value of 0.1 has been applied (without presenting any supporting analysis) for all HFEs to account for degraded plant conditions.

95 A discussion of contributors to fire CDF is provided in Chapter 57 of Ref. 2 together with various sensitivity analyses. No evaluation of release frequencies due to fires has been undertaken.

96 From the high level review of the AP1000 Fire PSA against ND's PSA guide (Ref. 8) undertaken during GDA Step 3, it was felt that the current analysis, that has been performed mainly using a screening method, using outdated data, and which therefore includes both conservatisms and optimisms throughout, does not provide a strong basis for the evaluation of the risk associated to fire and, thus, for the evaluation of the strengths and weaknesses of the design. In addition, during the ND / Westinghouse 'AP1000 PSA Step 3 Assessment Wrap-up Meeting' (Ref. 12), it became apparent that although Westinghouse may be able to provide answers to some of the questions raised, the current Fire PSA is not a good representation of the AP1000 risk due to internal fires since it needs significant update to incorporate design changes.

97 Therefore, in order to compile all the concerns around the AP1000 Fire PSA an RO has been raised. In response to this Westinghouse is planning to establish and provide, within GDA timeframes, a detailed programme to update the Fire PSA, however the work will not be completed until later. ND will assess Westinghouse's Fire PSA programme in GDA Step 4. Our expectation is that the review and update of the AP1000 Fire PSA should align it with up-to-date information and modern standards and, therefore, the Fire PSA programme should be accompanied by enough information on standards, approaches and data sources to be used to allow us to establish an initial judgement on whether the final Fire PSA for the AP1000 will be acceptable to ND.

Ref. 8, Table A1-2.7.3 Analysis of Internal Flooding

98 The approach to Flooding Analysis in the AP1000 PSA followed a systematic process similar to the fire analysis. However, no detailed analysis of flooding scenarios was performed, and the results are therefore bounding; this is justified based on the apparent low risk contribution from the flooding hazard. The accuracy of this conclusion will require further consideration in the detailed review during GDA Step 4.

99 Details of the compartmentalisation used in the AP1000 Flooding PSA are available in Table 56-1 of Ref. 2. Flood propagation paths are identified in Table 56-2. However inter area barriers are not described well enough to verify these or understand the basis. More detailed descriptions of inter-area barriers will be necessary in order to confirm that the compartmentalisation used as the basis for the flooding analysis is correct. Up-to-date drawings that detail the flooding compartment boundaries will be needed for the detailed review in GDA Step 4.

100 Flood compartments are listed in Table 56-2 of Ref. 2 together with information on flood sources and potential mitigating system damage and pathways, however flood sources are not characterised as high, medium or low energy and the maximum flood rates and volumes for each source are not identified. The detailed screening analysis relies on the determination of maximum flood heights and susceptibility to spray hazards but no calculations to corroborate the conclusions are presented. More detailed information is required to confirm that the screening analysis of flood scenarios is adequate.

101 For the evaluation of flooding frequencies generic pipe break frequencies combined with section of pipe have been used. Separate failure frequencies have been assigned to expansion joints. Pipe break frequencies are multiplied by a factor of 0.05 to allow for breaks which are merely leaks. Ref. 2 does not provide justification for the generic values used and, in fact, more recent generic data is available which characterises failure

frequencies according to system type, failure mechanism and severity. Having said that, the AP1000 flooding frequencies appear to be consistent with flood frequencies in more recent data sources, however, it is believed that the frequency of spraying events may have been significantly underestimated. In addition, the AP1000 study does not appear to address maintenance-induced floods. The flood frequencies from specific sources in each compartment are discussed in Section 56.4.5 of Ref. 2 but no characterisation of uncertainty is provided.

102 The general assumptions of the flooding analysis presented in Section 56.3 of Ref. 2 are broadly reasonable. However, the analysis assumes that doors remain intact and in their normal position without justification. Most flood analyses assume doors fail at some water height. Therefore, an analysis of potential propagation of the flooding through failed doors is currently missing.

103 ND's PSA guide (Ref. 8) sets up the expectation that, for each flood source, the propagation path from the source compartment to the point of accumulation should be identified, including the potential for structural failures. Table 56-2 of Ref. 2 includes brief descriptions of potential flood propagation paths. However, no indication of flood area adjacency or inter area pathways (door openings etc.) is provided. It is therefore difficult to corroborate that all affected areas to the point of final accumulation have been identified. In addition, no structural failures (including door failures) due to loads imposed by flooding or compartment pressurisation are addressed.

104 The susceptibility of various component types to flood sources is described in the general assumptions Section 56.3.1 of Ref. 2. However, only immersion and spray hazards are addressed. No discussion is provided regarding jet impingement and high temperature and / or humidity effects or over pressurisation due to high energy line breaks.

105 The initiating events for each flood scenario are identified and justified in Chapter 56 of Ref. 2. The method used to quantify conditional core damage probabilities for each flooding scenario is also described. However, no discussion of the post flood human reliability analysis is provided so it is not clear whether the potential degradation of human reliability in some flood scenarios has been addressed.

Ref. 8, Table A1-2.7.4 Seismic Analysis

106 For GDA Westinghouse has submitted a Seismic Margins Analysis (SMA) to address seismic risk. Since this is not a proper Seismic PSA, it cannot be integrated with the rest of the PSA for the evaluation of the overall risk of the AP1000 to support an assessment of the strengths and weaknesses in the design. This does not meet ND's PSA guide (Ref. 8) expectations for a seismic probabilistic safety analysis.

107 In order to perform the Seismic PSA it is necessary to have a seismic hazard curve. Westinghouse has not attempted to use a generic curve for a typical UK site relying on the margins analysis to demonstrate that the contribution to risk from seismic events is very low.

108 The seismic margins High Confidence of Low Probability of Failure (HCLPF) approach has been taken so there is no discussion of the seismic hazard. The HCLPF is defined as the 95% confidence limit of not exceeding a 5% probability of failure. In the seismic margins approach a single earthquake is assumed, in this case 0.5g Peak Ground Acceleration (PGA), and a seismic event tree constructed to determine the plant seismic damage states and hence the seismic initiating event categories.

109 The qualitative analysis shows that all the seismic plant damage states fragilities which lead directly to core damage are equal to or above the review level earthquake of 0.5g PGA. No quantitative analysis is performed. However, it is interesting to note that the seismic hazard analysis for one of the NPP sites in the UK indicates that the

exceedance frequency for a 0.5g PGA event is 5×10^{-6} /yr. This is equal to the fragility for the sequence EQ-IEV-RVFA, which is postulated to lead to core damage and large release. This represents the 95% confidence that the probability of this event is only 5%. Since the large release frequency from internal events is 1.95×10^{-8} /yr, the mean value for the seismic event will be of the same order as this.

110 Therefore, more analysis will be required to determine the seismic contribution to core damage and large release when site-specific information is available.

Ref. 8, Table A1-2.8 Low Power and Shutdown Modes

111 From the initial review of Chapter 54 of Ref. 2, it was apparent that the Shutdown PSA for the AP1000 is heavily based on the AP600 Shutdown PSA. In addition Appendix 19E of the AP1000 Design Control Document submitted for GDA (Ref. 3), which is part of Chapter 19 on 'Probabilistic Risk Assessment', presents a so-called 'Shutdown Evaluation' but it is not clear how this information links with the Shutdown PSA presented in Chapter 54 of the UK AP1000 PSA report (Ref. 2).

112 Ref. 2 in itself does not provide the summary of Plant Operational States (POS) considered or the development process to define (POSs). A justification of the applicability of the AP600 POSs to the AP1000 has not been found. Also, Ref. 2 does not provide the derivation of IEs during low power and shutdown states.

113 Therefore, problems were encountered in the Step 3 review of this particular area due to the scattered nature of the documentation of the AP1000 Shutdown PSA. In order to undertake a detailed assessment during GDA Step 4 Westinghouse has been requested to provide a reconstruction of the study from the various sources of information.

Ref. 8, Table A1-2.9 Uncertainty Analyses, Quantification and Interpretation of the Level 1 PSA Results

Ref. 8, Table A1-2.9.1 Uncertainty and Sensitivity Analyses

114 Chapter 50 of Ref. 2 documents the AP1000 Importance and Sensitivity Analyses (additional sensitivity analyses are reported throughout the PSA documentation, e.g. in Chapters 43 (Large Release Frequency), 49 (Dose), 54 (Shutdown), 56 (Internal Floods) and 57 (Internal Fires). Chapter 51 of Ref. 2 documents the AP1000 Uncertainty Analyses.

115 ND's PSA guide (Ref. 8) sets up the expectation that the sources of uncertainty should be identified explicitly. However, nowhere in Ref. 2 was an explicit discussion of the sources of uncertainty (Aleatory and Epistemic) for the AP1000 found.

116 For example, although assumptions have been made through all technical areas of the PSA, there is no easy way to clearly identify them and link them with the sensitivity analyses and uncertainty analyses presented. So, it is difficult to get an understanding on where all the sources of uncertainty are, how the sources of uncertainty impact the risk and whether the sensitivity analyses presented are sufficiently comprehensive to provide confidence that the results are adequately robust. In this respect, it is felt that key assumptions regarding the performance of passive systems (for Level 1 PSA) have not been discussed explicitly and have therefore not been captured in the sensitivity analyses.

117 The Level 1 PSA Uncertainty Analysis of Chapter 51 focuses on parametric uncertainty. There is some explanation on the uncertainty parameters that have been assigned, but these are not considered to be sufficiently justified. For example, error factor values of 3, 10, 30 have been assumed for small, large, and very large uncertainties; some of the CCF values in Table 51-A1 have error factors as low as 3, which, given the lack of data for the determination of these values, are unlikely to be appropriate.

118 The review team also believes that there is some inadequacy in the performance of the uncertainty analysis; the parametric values used to determine the value for each basic event are tabulated in Chapter 32 of Ref. 2, however, the uncertainty analysis has been performed on basic event values with no consideration of the correlation between components using the same parameter. An uncertainty analysis should be performed using the parametric values in the cut set in order to get the correct correlation and more accurate uncertainty distribution. The mean from the parametric uncertainty analysis should then be used for the comparison against numerical risk targets.

119 Finally, the results of the importance and sensitivity evaluations reported in Ref. 2 indicate significant sensitivity of the results to several parameters / components. However, there is no discussion on reducing the most important uncertainties, as it would be expected in the UK regulatory environment.

Ref. 8, Table A1-2.9.2 Quantification of the Level 1 PSA

120 The review of the quantification during GDA Step 3 has been based on the documentation provided in Ref. 2. However, as discussed earlier, Ref. 2 does not document the PSA model submitted to ND for assessment, which has been built in the CAFTA software. This model is attached to a Calculation Note which also includes some documentation. This will be reviewed during GDA Step 4.

121 The cut-off / truncation limit used for the quantification has not been found and is not provided in Chapter 33 of Ref. 2. From a review of the documentation, it appears that a truncation limit of 1.0×10^{-12} may have been used. It is felt that this value, if confirmed, is not low enough since the core damage frequency is 2.4×10^{-7} /yr. Westinghouse needs to justify the actual cut-off/s used for the quantification of the AP1000 PSA.

Ref. 8, Table A1-3 Level 2 PSA

Ref. 8, Table A1-3.1 Interface Between Level 1 and Level 2 PSA

122 The methodology used for the Level 1 – Level 2 interface is considered reasonable and is expected to be capable of correctly transferring information to the Level 2 Containment Event Trees (CET). However, concerns were raised about a lack of transparency and lack of evidence of a systematic approach to the identification of Plant Damage States (PDS) and the subsequent definition of the PDSs themselves. Specific points are summarised below:

- There is no evidence in Ref. 2 of a systematic process to select attributes or even of what attributes were considered for inclusion and why these were included / excluded. For example, there is no evidence of a list of candidate attributes which might be based on other studies, reference documents or available standards, a subsequent review of these for application to the AP1000 PSA or of any plant specific discussion leading to the choice of attributes used.
- There is no step-by-step explanation of the criteria used to determine each grouping attribute based on sequence status, which has the potential to lead to ambiguity in the grouping.

123 Note that the above points do not in themselves imply that the PDSs identified for the AP1000 are inadequate. Further detailed review would be required in Step 4 to confirm adequacy or otherwise.

Ref. 8, Table A1-3.2 Level 2 PSA Deterministic Accident Progression Analysis

124 Parametric sensitivity to selected assumptions is examined in some areas, for example: Reactor Pressure Vessel (RPV) depressurisation, In-Vessel Retention (IVR), and hydrogen combustion. However, the effects of alternate credible assumptions have not always been thoroughly demonstrated to be negligible. Technical debate within the international severe accident community remains open on some topics, such as in-vessel debris configurations, associated heat fluxes to the RPV lower head and their impact on conclusions of IVR.

125 The analyses are usually specific to AP1000. However, a considerable amount of information is drawn from earlier analysis of AP600. Scaling arguments or adjustments to calculations have been made, when necessary. The original ULPU experiments for IVR, for example, were extended to capture the power and geometric differences between the two designs.

126 A summary of MAAP4 results is presented in Chapter 34 of Ref. 2, with additional information of particular phenomena in Chapters 39, 41 and Appendix B. However, detailed documentation (and input decks) of individual MAAP4 calculations needs to be provided by Westinghouse so that it can be assessed in GDA Step 4. The experience and qualification of MAAP analysts are not known or stated.

Ref. 8, Table A1-3.3 Level 2 PSA Containment Performance Analysis

127 Westinghouse's analysis of containment performance is based on heuristic information on 'typical' containment failure mechanisms and locations. Quasi-static over-pressure (fragility curve) and dynamic events (H_2 detonation or steam explosion) are the only two mechanisms applied in the Level 2 PSA. A description of a systematic search for, and evaluation of, all plausible mechanisms and locations of containment failure (or a suitable alternative process) was not found in the PSA documentation (Ref. 2).

128 A qualitative argument is used to dismiss the contributions of smaller mechanical and electrical penetrations based on similarities in material composition and more onerous failure criteria (e.g. higher temperatures) observed in scaled experimental work. The extent to which stress intensity near small penetrations - caused by global displacement of the containment cylindrical shell - was explicitly addressed in the calculation of ultimate pressure capacity is not clear.

129 Contributors to uncertainty in ultimate capacity were apparently quantified by expert judgment, although this is not documented in available references. There is no evidence of a systematic process of eliciting expert judgment for the purposes of evaluating uncertainty in containment failure criteria or response.

130 The containment performance analysis documentation currently provided is not fully traceable.

131 According to Westinghouse, the current AP1000 LRF is not very sensitive to the ultimate capacity of the containment – this is probably due to the fact that the currently estimated low CDF allowed Westinghouse to make conservative assumptions regarding containment performance in the Level 2 PSA while still presenting a LRF that is small. This approach may be no longer adequate if future revisions of the PSA show a higher CDF. This is the reason why assessment of this aspect of the Level 2 PSA will be pursued in GDA Step 4 despite its currently perceived low importance from the risk point of view.

Ref. 8, Table A1-3.4 Probabilistic Modelling Framework – Accident Progression Event Trees (APET)

132 According to the documentation presented in Ref. 2, the Containment Event Trees (CET), referred to as APETs in Ref. 8, are linked to the Level 1 by a set of PDSs defined by their frequency and characteristics. The model is not, according to Ref. 2, linked at the fault tree level, even though fault tree top events are present in the CET. The CET is quantified numerically.

133 In principle the method used, described in Ref. 2, should be capable of correctly carrying forward and quantifying dependencies, this being achieved by a process whereby conditional split fractions are generated for the CET events, according to the specific PDS. However, it appears that human dependencies for events in the CET were not allowed for in the conditional split fraction generation process. Chapter 43 of Ref. 2 describes release frequency quantification and explains the process of quantification of systems related events.

134 Similarly to the case of the Level 1 – Level 2 Interface, it is felt that there is not sufficient evidence of a systematic process for the selection of phenomena included in the CET. For example, there is no evidence of a list of potential generic light water reactor phenomena for incorporation in the CET and / or of the process followed for deciding which events to include and exclude from the CET. Further detailed review will be required in Step 4 to confirm adequacy or otherwise of the CET structure.

135 CET quantification is only described at a high level and data files are not contained in PSA documentation, although nodal split fractions are presented, which would probably be sufficient for independent verification of the Level 2 results.

136 Finally, it is necessary to point out that Ref. 2 describes a historic Level 2 PSA model which is not in CAFTA. The CAFTA model appears to present a fully linked fault tree Level 2 model, which however is not documented in detail in any of the references reviewed during GDA Step 3. So, in order to continue with the detailed assessment of the Level 2 PSA during GDA Step 4, clarification is being sought from Westinghouse on the correspondence between the documentation of the Level 2 PSA and the model to be reviewed.

Ref. 8, Table A1-3.5 Level 2 PSA Source Term Analysis

137 During the review of this aspect of the PSA in Step 3, it was felt that the discrimination among Release Categories (RC) is not adequate. A common Source Term (ST) is developed for each RC based solely on the mode (time) of containment failure without any discrimination among accident sequence characteristics or severe accident phenomena. This precludes any evaluation or understanding of the relative contribution of systems, sequences or phenomenological issues to overall results.

138 No technical argument is offered to justify the selection of the single accident sequence used to represent each RC. The number of RCs is considered to be too small.

139 The basis for selecting the single accident sequence used to represent each RC is not known. The contribution to the frequency of each RC (Table 43-7 and 43-8 of Ref. 2) indicates that a wide variety of sequences contribute to several RCs. However, the Source Term Analysis in Chapter 45 of Ref. 2 only evaluates releases associated with a single representative sequence.

140 The PSA presents a set of Release Categories associated with containment failure at different nodes in the CET. The main focus (see Chapter 45) is on releases accompanying containment failure (or containment bypass) classified as ‘large release’ (LRF), which is associated with any CET sequence in which the containment fails or is bypassed. Large releases occurring in sequences involving containment bypass or early

containment failure are sub-categorised as a 'large early' release (Large Early Release Frequency, LERF), although this distinction is not followed through elsewhere in the PSA and the term LERF is not used later in the results section (Chapter 59). Rather, the general presentation of results uses the combined frequency of releases associated with containment failure which are collectively described as the 'Large Release Frequency' (LRF). It is noted, however, that the two terms are effectively interchangeable because LRF is dominated by the frequency of early rather than delayed containment failure sequences (see Section 59.4.1 of Ref. 2).

141 The Source Term magnitudes are presented in terms of cumulative and (for the purposes of dose assessment only) time-dependent release fractions of radionuclide groups to the environment. No information is offered to identify and characterise the efficiency of important retention mechanisms, locations of deposited material, nor the dominant factors contributing to differences in the releases among the RCs.

142 In Section 49.4 of Ref. 2, continuous release fractions from MAAP calculations are reduced to four consecutive plumes, each with a unique start time, duration and (constant) release rate. All releases are assumed to emerge from containment at ground level. Tables 49.1 and 49.2 indicate that the releases are assumed to have no internal energy (i.e. no plume rise is reflected in the offsite dispersion calculations.) Release energy is not discussed in Chapter 45 as an attribute of the Source Term.

143 Chemical forms of released radionuclides are stated (based on MAAP framework) but the assumed isotopic inventory of radionuclides used to translate the fractional releases from MAAP to offsite dose is not described.

144 The sensitivity analysis provided for the Source Term is sparse. A single sensitivity calculation is offered to examine the effects of applying a Decontamination Factor (DF) of 3 to the release associated with the RC representing releases from an intact containment. No sensitivity analysis is offered to examine impacts of assumptions or uncertainties on Source Terms calculations for risk-dominant sequences.

Ref. 8, Table A1-3.6 Presentation and Interpretation of the Level 2 PSA Results

145 Sensitivity analysis has been performed for the Level 2 PSA. This is documented in Chapter 43 of Ref. 2. However, propagation of uncertainties to LRF is not performed, either for Level 1 parametric uncertainties, Level 2 uncertainties or a combination of the two.

146 The Level 2 PSA presented in Ref. 2 presents the following numerical results:

- Large Release Frequency (LRF), which is the frequency of all Release Categories except intact containment.
- Containment Effectiveness (Ceff), which is the ratio of intact containment frequency to core damage frequency.

147 The values of these are then compared with targets derived from the US NRC Safety Goals, rather than UK targets.

148 Chapter 49 of Ref. 2 presents a limited scope Level 3 PSA analysis which uses the Level 2 PSA results (frequency and Source Term for each RC) as input, and makes certain 'generic' assumptions about demography and weather.

149 These analyses are conducted to estimate the whole-body dose and acute red bone marrow dose, both at the site boundary (0.5 miles). The population whole-body dose out to 80.5 kilometres and the downwind, centerline, ground-level thyroid dose at the site boundary (0.5 miles) are also calculated for information.

150 The estimated site boundary whole-body dose and the acute red bone marrow dose are compared to the Westinghouse goal of <25 rems (0.25 sieverts), at a frequency not to exceed 1×10^{-6} /yr. This is consistent with the goal provided in the following Reference: Advanced Light Water Reactor Utility Requirements Document, Volume III, Appendix A to Chapter 1, PRA Key Assumptions and Groundrules, EPRI, Rev. 5 & 6, December 1993.

151 These analyses are used to show compliance with the EPRI / Westinghouse targets with considerable margin, according to the supplied documentation. This is unsurprising since the CDF for the AP1000 presented by Westinghouse is $<10^{-6}$ /yr.

152 Some consideration of UK targets is provided in a document entitled 'Safety Assessment Principles (SAPs) Roadmap for AP1000 Design' (Ref. 13). The following paragraphs provide some observations on this document.

153 In Ref. 13, Numerical Targets 5 to 9 of the SAPs (corresponding to risk from accidents) are addressed based on the PSA presented in Chapter 19 of Ref. 3. Compliance is claimed on this basis without additional analysis. It was noted that there does not appear to be any consideration of sequences without core damage resulting in small releases which may contribute significantly to the low dose, higher frequency end of the dose band scale. In other words, the success sequences of the Level 1 PSA do not appear to have been considered for their potential low dose band contribution. Furthermore, it is not clear at this stage that the Level 2 PSA has been performed in a way that facilitates easy comparison with the Numerical Targets in the HSE SAPs related to offsite consequences (Targets 7 to 9). For example, it is not clear that a mapping of RCs to Dose Bands (Target 8) could be established, or that a mapping of RCs corresponding to a 'large accident' (societal risk in Target 9) could be established.

154 The scope of the Level 2 PSA presented in Ref. 2 has the following omissions:

- Fires, floods and external hazards are not included.
- The shutdown assessment for Level 2 PSA is simplified being a scaling of the AP600 analysis to the AP1000 CDF.
- Low consequence sequences (Level 1 non-core damage sequences) are not included in the scope meaning that their radiological risk contribution is not taken into account.
- The Level 2 PSA does not cover all sources of radioactivity (only the reactor core is included; fuel ponds, fuel handling facilities, waste storage tanks, etc, are not included).

155 The documentation provided by Westinghouse does not provide a detailed justification on this last point, rather it states:

"The AP1000 PRA considers the reactor core as the largest source of radioactivity in the AP1000. Thus, the PRA quantifies risk due to initiating events that may challenge the core integrity"

156 It is also stated that additional sources of radioactivity (spent fuel) are discussed in the DCD Chapter 19 and the PSA but this discussion was not found in Ref. 2 (PSA) or Ref. 3 (DCD). However, it has been noted before in this assessment report that a document entitled 'AP1000 PRA Spent Fuel Pool Evaluation' (UKP-GW-GL-743 Rev 0), submitted to ND separately from the rest of the PSA, addresses the risk associated with the spent fuel pond. This will be reviewed during GDA Step 4.

157 Westinghouse has presented a SAMDA (Severe Accident Management Design Alternatives) analysis which is intended to support the ALARP demonstration. Potential modifications (design alternatives) have been assessed in this analysis. No specific comments were raised on the SAMDA during the Step 3 review, however it was noted that the omissions from the scope of the Level 2 may limit the validity of the ALARP demonstration.