Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Probabilistic Safety Analysis Assessment of the Westinghouse AP1000® Reactor

Assessment Report: ONR-GDA-AR-11-003
Revision 0
10 November 2011

COPYRIGHT

First published December 2011

PREFACE

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

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process, and the submissions made by Westinghouse relating to the AP1000® reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires Westinghouse to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the Westinghouse AP1000® reactor.

EXECUTIVE SUMMARY

This report presents the findings of the assessment of the Probabilistic Safety Analysis (PSA) of the AP1000 reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the PSA that supports the 2011 Pre-construction Safety Report (PCSR), (which is an update of the PSA that supports the AP1000 European Design Control Document EPS-GW-GL-700, Rev 1, and the 2009 PCSR) and the supporting documentation submitted by Westinghouse during GDA Step 4.

To identify the scope of the GDA Step 4 assessment for the PSA, an assessment plan was set-out in advance. The GDA Step 4 review itself covered all the technical areas of the PSA, although it is important to note that the evidence supporting the PSA claims and arguments (assessed during GDA Steps 2 and 3) on how the PSA Safety Assessment Principles (SAP) are met, have been assessed on a sampling basis. For PSA, "evidence" is interpreted as the details of the PSA models and data, and the underlying supporting analyses, with the assessment focussing mainly on detailed reviews of such evidence. The sampling has been done in a focused, targeted and structured manner with a view to revealing any specific or generic weaknesses in the PSA. The GDA Step 4 assessment has been conducted following the guidance and structure established in Appendix 1 of the Nuclear Directorate's PSA guide (T/AST/030 Issue 3, February 2009).

To help to reach a conclusion of whether an AP1000 can be constructed and operated safely in the UK, and to evaluate the importance of the findings in the various PSA technical areas, a Risk Gap Analysis (RGA) was conducted. This was a complex task but it was essential for wrapping-up the results from the GDA Step 4 PSA assessment.

The AP1000 PSA comprises a Level 1, a Level 2 and a simplified Level 3 PSA. The scope includes consideration of internal initiated events and internal hazards and includes low power and shutdown operating states. Westinghouse submitted a separate PSA for the Spent Fuel Pool, which has also been assessed. In general, 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.

The high level review of all the PSA technical areas conducted during GDA Step 3 identified shortcomings in scope, methods and data. I indicated at that time that work would be required to complete and modernise the PSA so that it could provide a more adequate input into the "as low as reasonably practicable" (ALARP) demonstration. Despite that, I also indicated that the AP1000 Core Damage and Large Release Frequencies provided a degree of confidence that the Societal Risk Target (Target 9 from Numerical Target NT.1 of the Health and Safety Executive's SAPs) would lie below the Basic Safety Level (BSL) and that I did not have any reason then to believe that this position would change once the PSA has been completed and updated. The detailed GDA Step 4 review of the PSA, together with the results of the Risk Gap Analysis, has confirmed that the conclusions from GDA Step 3 remain valid.

Findings of greater or lesser importance were identified in all the technical areas of the PSA. These are listed in Annex 1 and will be carried forward as normal regulatory business. However, shortcomings in two particular areas give rise to more significant uncertainty in my understanding of the risk associated with the AP1000 design. These are "PSA Success Criteria" and "Fire PSA". These are identified in this report as GDA Issues and each one has an associated Resolution Plan proposed by Westinghouse. In order to address these GDA Issues effectively, Westinghouse will need to consider the Initiating Events identified as currently missing from the PSA. Given the nature of the PSA, relevant findings in other areas may also need to be addressed at this point. Westinghouse will also need to evaluate the implications of the new analysis on the AP1000 Core Damage Frequency (CDF) and Large Release Frequency (LRF). The two PSA GDA Issues will require resolution before the Health and Safety Executive would agree to grant a final Design Acceptance Confirmation.

The estimated risk gap addressing the review findings, which could be evaluated quantitatively in GDA, concluded that the CDF and LRF for the AP1000 are likely to be higher than the current figures estimated by Westinghouse, but are still lower than those figures of merit for currently operating PWRs. Also, it is acknowledged that there are conservatisms in some aspects of the AP1000 PSA model and data. All this suggests that the risk associated with the AP1000 design could be low enough to meet the Basic Safety Objectives (BSO) for Targets 7 and 9 from NT.1 of the Health and Safety Executive's Safety Assessment Principles. However, this conclusion is subject to the following:

- Satisfactory outcome from both GDA Issues on "PSA Success Criteria" and "Fire PSA".
- The AP1000 PSA is built on assumptions based on design documentation available at the time when the PSA was developed. This has changed since then. Also, GDA Issues have been raised in other technical areas, the outcome of which may further affect the ability of the PSA in its current form to reliably predict the risk of the AP1000 design.
- Final design, site specific characteristics and operational matters (procedures, maintenance schedule, refuelling outage strategy, etc).

The Risk Gap Analysis results also showed a potential change in the AP1000 risk profile. This is an important insight from the review as a change of this nature to the risk profile could have an impact on whether or not the risks are as low as reasonably practicable.

Overall, based on the sample undertaken, I have concluded that the AP1000 PSA needs substantial improvements to meet the expectations of HSE's SAPs and PSA Technical Assessment Guide (T/AST/030), and to be suitable to adequately support the AP1000 "generic" PCSR. Furthermore, based on the results of the Risk Gap Analysis (RGA), the AP1000 PSA in its current state does not enable a complete and reliable comparison against the numerical targets of the SAPs and an effective ALARP evaluation. However, since the results of the RGA have suggested that the risk of this reactor appears to be low in comparison with currently operating reactors, and potentially able to meet the Basic Safety Objectives for individual and societal risk, I believe that the AP1000 reactor is suitable for construction in the UK, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor.

Finally, as already mentioned above a number of potentially important risk gaps will depend on matters beyond the generic design. So, ultimately, a "site-specific" PCSR should be in place before construction begins on the nuclear island and this should be supported by an adequate PSA. Therefore, a complete and updated Level 1, 2 and 3 PSA (Fuel Pool, Reactor at Power, Low Power and Shutdown, Internal Events and Internal and External Hazards) should be available to support future stages of the Nuclear Power Plant development. This should be accompanied by ALARP evaluations to demonstrate that no further improvements to reduce the risk are reasonably practicable (or otherwise).

ABBREVIATIONS

AC	Alternating Current
ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
ALWR URD	Advanced Light Water Reactor Utility Requirements Document
APET	Accident Progression Event Tree
ATWS	Anticipated Transient without SCRAM (Reactor Shutdown)
BC	Base-case
BMS	(Nuclear Directorate) Business Management System
BPL	Bistable Processor and Logic
BSL	Basic Safety Level
BSO	Basic Safety Objective
C&I	Control and Instrumentation
CAFTA	Computer Aided Fault Tree Analysis System
CAP	Corrective Action Plan
CAS	Instrument Air System
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failure
CCS	Component Cooling Water System
CDF	Core Damage Frequency
C_{eff}	Containment Effectiveness
CET	Containment Event Tree
CHF	Critical Heat Flux
CHR	Containment Heat Removal
CIM	Component Interface Module
CLP	Cask Loading Pit
CMT	Core Make-up Tank
CST	Condensate Storage Tank
CVS	Chemical and Volume Control System
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DBA	Design Basis Analysis
DC	Direct Current
DCD	Design Control Document
DDT	Deflagration-to-Detonation Transition
DF	Decontamination Factor

ABBREVIATIONS

DG	Diesel Generator
DVI	Direct Vessel Injection
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
FA	Fault Analysis
FDF	Fuel Damage Frequency
FIVE	Fire-Induced Vulnerability Evaluation
FMEA	Failure Modes and Effects Analysis
FTC	Fuel Transfer Canal
FTO	Failure to Open
GDA	Generic Design Assessment
GRS	Gesellschaft fur Anlagen--und Reaktorsicherheit
HCLPF	High Confidence of Low Probability of Failure
HCR	Human Cognitive Reliability
HEART	Human Error Assessment and Reduction Technique
HELB	High Energy Line Break
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Analysis
HRHF	Hard Rock High Frequency
HSE	The Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IE	Initiating Event
IEC	International Electrotechnical Commission
INPO	Institute of Nuclear Power Operations
IRWST	In-containment Refuelling Water Storage Tank
IS	Interfacing System
ISLOCA	Interfacing System Loss of Coolant Accident
IVR	In-vessel Retention
JPO	Joint Programme Office
kV	Kilo Volts
LCF	Late Containment Failure
LCL	Local Coincident Logic

ABBREVIATIONS

LERF	Large Early Release Frequency
LMFW	Loss of Main Feedwater
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
LP&SD	Low Power and Shutdown
LRF	Large Release Frequency
LRP	Large Release Probability
LSTF	Large Scale Test Facility
MAAP	Modular Accident Analysis Program
MACCS	MELCOR Accident Consequence Code System
MCCI	Molten Corium-Concrete Interaction
MDEP	Multinational Design Evaluation Programme
MFW	Main Feedwater System
MGL	Multiple Greek Letter
MLOCA	Medium Loss of Coolant Accident
MOV	Motor Operated Valve
MSIV	Main Steam Isolation Valve
MSL	Main Steam Line
ND	(HSE) Nuclear Directorate
NPP	Nuclear Power Plant
NRV	Non-return Valve
NT	Numerical Target
ONR	Office for Nuclear Regulation
P&ID	Piping and Instrumentation Diagram
PCER	Pre-construction Environment Report
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PDS	Plant Damage State
PFH	Average frequency of a dangerous failure of a safety function
PGA	Peak Ground Acceleration
PID	Project Initiation Document
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal System

ABBREVIATIONS

PSA	Probabilistic Safety Analysis
psi	Pounds per Square Inch
PTQ	Proposed Technical Query
PWR	Pressurised Water Reactor
PXS	Passive Cooling System
RAT	Reserve Auxiliary Transformer
RC	Release Category
RCA	Radioactive Controlled Area
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RGA	Risk Gap Analysis
RHR	Residual Heat Removal
RI	Regulatory Issue
RIA	Regulatory Issue Action
RNS	Normal Residual Heat Removal System
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RPV	Reactor Pressure Vessel
SAMDA	Severe Accident Management Design Alternatives
SAMG	Severe Accident Management Guideline
SAP	Safety Assessment Principle
SFP	Spent Fuel Pool (or Pond)
SFW	Start-up Feedwater System
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIL	Safety Integrity Level
SLB	Steam Line Break
SLB-U	Steam Line Break Upstream of the MSIVs
SLOCA	Small Loss of Coolant Accident
SMA	Seismic Margins Analysis
SPADS	(Large LOCA due to) Spurious Actuation of ADS
SRO	Senior Reactor Operator
SRV	Safety Relief Valve
SSC	Structures, Systems and Components

ABBREVIATIONS

ST	Source Term
STA	Shift Technical Advisor
STC	Source Term Category
SWS	Service Water System
T&M	Testing and Maintenance
TAG	(Nuclear Directorate) Technical Assessment Guide
T-Cold	Temperature in the (RCS) Cold Leg
TCS	Turbine Building Closed Cooling Water System
THERP	Technique for Human Error Rate Prediction
TQ	Technical Query
TSC	Technical Support Contractor
UAT	Unit Auxiliary Transformer
URD	Utility Requirements Document
US NRC	United States Nuclear Regulatory Commission
V	Volts
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

Annexes

Annex 1: Assessment Findings to be Addressed During the Forward Programme of This Reactor as Normal Regulatory Business – Probabilistic Safety Analysis – AP1000

Annex 2: GDA Issues - Probabilistic Safety Analysis – AP1000

Definitions

1 INTRODUCTION

1 This report presents the findings of the assessment of the Probabilistic Safety Analysis (PSA) of the AP1000 reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). The assessment has been carried out on the PSA that supports the 2011 Pre-construction Safety Report (PCSR), (which is an update of the PSA that supports the AP1000 European Design Control Document EPS-GW-GL-700, Rev 1, and the 2009 PCSR) and the supporting documentation submitted by Westinghouse during GDA Step 4.

2 The Safety Assessment Principles (SAP) (Ref. 4) have been used as the basis for this assessment. Ultimately, the goal of assessment was to reach an independent and informed judgment on the adequacy of a nuclear safety case. In order to achieve this goal, the assessment of the AP1000 PSA has been conducted following the guidance and structure established in Appendix 1 of the Nuclear Directorate's (ND) PSA Technical Assessment Guide (TAG), T/AST/030 Issue 3, February 2009 (Ref. 15).

3 During the assessment a number of Technical Queries (TQ) and Regulatory Observations (RO) were issued and the responses made by Westinghouse assessed. Where relevant, detailed information from other areas of the AP1000 submission has been looked at to build confidence and assist in forming a view as to whether the risk associated with the AP1000 design submitted for GDA is low enough to make this reactor suitable for construction in the UK.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR PROBABILISTIC SAFETY ANALYSIS

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

2.1 Assessment Plan

5 ND's GDA process calls for a step-wise assessment of the Requesting Party's (RP) safety submission. As with the other technical areas, the PSA assessment is following the claims-argument-evidence hierarchy. In GDA Step 2 the claims made by Westinghouse were examined, in GDA Step 3 the arguments that underpin those claims were assessed, and in GDA Step 4 the evidence that supports those claims and arguments has been evaluated and a judgement has been made of the adequacy of the PSA contained within the PCSR and Supporting Documentation.

6 The detailed PSA assessment plan for the AP1000 within Step 4 is laid down in Ref. 1.

2.2 Standards and Criteria

7 The main standards and criteria used are HSE's Safety Assessment Principles (SAP) (Ref. 4). The PSA GDA Step 3 assessment strategy (Ref. 16) identified SAPs FA.10 to FA.14 and Targets 7 to 9 of Numerical Target 1 (NT.1) as the relevant parts of that document. Attention has also been paid to the relevant standards of the International Atomic Energy Agency (IAEA) (Refs 14, 17 and 18) and the Western European Nuclear Regulators' Association (WENRA) reference levels (Ref. 7).

8 The above PSA related SAPs, IAEA standards and WENRA reference levels are embodied and enlarged in ND's Technical Assessment Guide (TAG) on PSA (Ref. 15) and it is this guide that provides the principal means for assessing the PSA in practice.

9 For GDA Step 4 it is important to note that the PSA has not been assessed in its entirety; rather, the evidence that supports the arguments (assessed in Step 3, Ref. 6) that support high level claims (assessed in Step 2, Ref. 19) on how the PSA SAPs are met, have been looked at.

10 For PSA "evidence" is interpreted as the details of the PSA models and data and the underlying supporting analyses. The assessment conducted during GDA Step 4 has focused mainly on detailed reviews (on a sampling basis) of such evidence.

2.3 Assessment Scope

11 As anticipated in Ref. 6, the GDA Step 4 assessment of the AP1000 PSA has looked in detail at all of the areas reviewed at a high level in GDA Step 3, using, as the basis, the original PSA documentation and all the additional information received in response to the TQs and ROs raised. In GDA Step 4 the AP1000 Spent Fuel Pool (SFP) PSA submitted by Westinghouse has also been reviewed in detail.

12 All the technical areas of PSA have been addressed following the guidance and structure established in Appendix 1 of ND's PSA TAG (Ref. 15). However, not each and every fault tree, event tree, supporting analysis or item of reliability data, has been examined in

detail. Rather, the aim has been to establish, by reviewing in detail a representative sample, whether the implementation of the methods and techniques used was adequate.

13 As well as the detailed review of all the technical areas of the PSA, during GDA Step 4 I have undertaken a Risk Gap Analysis (RGA). The objectives and strategy of the RGA are described in Section 2.3.2 below.

14 The versions of the PSA models and documentation submitted by Westinghouse for review during GDA Step 4 are listed in letter UN REG WEC 000131 (Ref. 20). This letter was prepared by Westinghouse upon my request to ensure clarity on the scope of Westinghouse's PSA-related material that needed to be referred to during the GDA Step 4 review of the AP1000 PSA. Therefore, this letter has been the key reference that delineates the top layer of the PSA models, documentation, supporting analyses, etc, reviewed during GDA Step 4. In GDA Step 4 Westinghouse has also submitted, or referred to, additional documents in responses to TQs and ROs that I have raised. These are not listed in Ref. 20 but they are mentioned on a case by case basis, as necessary, in the description of the assessment of the different technical aspects of the PSA (Section 4 below).

15 Thus, based on the above, the key references used during the GDA Step 4 review of the AP1000 PSA which have constituted the scope of the assessment are:

- Full documentation of the Reactor PSA: UKP-GW-GL-022 Rev 0, "UK AP1000 Probabilistic Risk Assessment" (Ref. 21). Chapter 26 of this document (Protection and Safety Monitoring System, PMS) has been replaced by APP-PRA-GSC-222, Rev 1. (Ref. 22). Chapter 28 of Ref. 21 (Plant Control System Model, PLS) has been replaced by APP-PRA-GSC-228, Rev 0. (Ref. 23).
- PSA Model (Reactor) 3B in CAFTA documented in UKP-GW-GLR-102 Rev 0 "UK AP1000 Probabilistic Risk Assessment Update Report" (Ref. 24) and attached to APP-PRA-GSC-236 Rev 1 "AP1000 PRA Quantification" (Ref. 25).
- PSA Model (Fuel Pool) in CAFTA documented in UKP-GW-GL-743 Rev 1 "AP1000 PRA Spent Fuel Evaluation" (Ref. 29) and attached to APP-PRA-GSC-400 Rev C "AP1000 Spent Fuel Pool Probabilistic Risk Assessment (PRA)" (Ref. 28).

2.3.1 Results from GDA Step 3

2.3.1.1 Strengths

16 My GDA Step 3 PSA report (Ref. 6) highlighted the following AP1000 PSA strengths:

- 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.
- The AP1000 PSA appears to be supported by a considerable amount of analysis. This is particularly the case for the Level 2 PSA.
- 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).
- Westinghouse's PSA team are dealing with a PSA that was originally developed in the early nineties 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 my team. Discussions between ND and Westinghouse's PSA team have been open and positive throughout the whole period of our assessment.

2.3.1.2 Findings

17 During GDA Step 3 I carried out a high level review of all the AP1000 PSA technical tasks against the expectations in T/AST/030 (Table A1) (Ref. 15). The shortfalls found in the review led me to issue Technical Queries in all areas of the PSA. My GDA Step 3 PSA report (Ref. 6) describes all the limitations found. These are also briefly summarised in the respective sub-sections in Section 4 below.

18 During my GDA Step 3 assessment two areas were identified where the shortfalls were such that could not be clarified via TQs and led to issuing two Regulatory Observations. These were "PSA Systems Analysis Guidelines and Systems Models" (RO-AP1000-045) and "Fire PSA" (RO-AP1000-044).

19 In the PSA area I did not identify any failings or shortfalls of sufficient magnitude to warrant the issue of Regulatory Issues.

20 My GDA Step 3 assessment (Ref. 6) concluded that the AP1000 PSA reviewed provided 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 my assessment indicated that work would 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 As Low As Reasonably Practicable (ALARP). In addition, further development would 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

21 My GDA Step 3 report also indicated in its conclusions (Ref. 6) that the AP1000 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 from NT.1 of the SAPs) lies below the Basic Safety Level (BSL). At the end of my GDA Step 3 assessment, I did not have any reason to believe that this position would change dramatically once the PSA has been completed and updated.

2.3.2 Additional Areas for GDA Step 4 Probabilistic Safety Analysis Assessment

22 As well as the detailed review of all the technical areas of the PSA, during GDA Step 4 I have undertaken a "Risk Gap Analysis" (RGA). The RGA was designed to meet the following objectives:

- Key objective: Help to reach a conclusion, by June 2011, of whether an AP1000 can be constructed and operated safely in the UK.
- Subsidiary objective 1: Evaluation of the importance of the findings in the various PSA technical areas.
- Subsidiary objective 2: Evaluation of the overall gap between the AP1000 risk claimed by Westinghouse and an understanding of the AP1000 risk based on a more realistic and complete evaluation.

23 The items for RGA evaluation were identified during the GDA reviews of the individual technical areas in the PSA. A preliminary screening of these items for further RGA evaluation was undertaken based on qualitative aspects and / or preliminary quantitative information. Numerical importance of the items under evaluation (risk contributions and risk increase factors) and conditional core damage probabilities as well as engineering judgement were used for this purpose. Screening criteria and some preliminary results of the screening process were discussed with Westinghouse in an RGA Workshop held in August 2010 and during the 2nd PSA Technical Exchange Workshop in October 2010.

24 The screened-in items were retained for further RGA evaluation, mostly quantitative. Decisions on how the screened-in findings would be addressed were taken on a case-by-case basis. In some cases, because of the gaps of information in the current PSA documentation and / or the need to simplify the analysis, RGA quantification was based on assumptions. These assumptions, RGA results and key findings were presented and discussed with Westinghouse during the 3rd Technical Exchange Workshop held in February 2011.

25 Two different approaches were used to conduct the RGA evaluations:

- A so called "Base-case (BC) RGA Model" was created from the original AP1000 PSA, by modifying models and data, as appropriate, addressing the various findings screened-in in the different technical areas which could be implemented in the model. Variations of the BC RGA Model were implemented, as appropriate, to understand separate impacts per technical area.
- The importance of a number of screened-in findings not included in the BC RGA Model was explored via individual sensitivity analyses.

26 It should be noted that a number of findings initially perceived to be important were finally left out of the quantitative RGA evaluation, either because the gap in knowledge was large enough to preclude a meaningful RGA, or because the modelling effort required to address the finding would be beyond the available time and resources.

27 The RGA is documented in Section 4 below as follows:

- For each technical area, where relevant, a short description of the RGA undertaken is included in the sub-section on "Assessment" and a summary of RGA results and insights is included in the sub-section on "Findings".
- Section 4.20 on "Overall Conclusions from the PSA" presents an overall summary of the work done, the results obtained and how these are used to support the final conclusions from the GDA assessment of the AP1000 PSA.

28 It should be noted that the RGA was not intended to produce alternative PSA results and therefore the precise numbers are not presented here. The presentation focuses on obtaining qualitative insights from the results of the analysis to aid the understanding of the importance of the findings. This together with an appreciation of the influence that the PSA should have in future stages of the Nuclear Power Plant (NPP) development has been used to establish priorities for their resolution post GDA.

2.3.3 Use of Technical Support Contractors

29 Technical Support Contractors (TSC) were engaged to assist with the PSA assessment work throughout GDA. Whilst the TSCs undertook detailed technical reviews, this was done under close direction and supervision by ND and the regulatory judgment on the

adequacy or otherwise of the AP1000 PSA in this report has been made exclusively by ND.

30 In GDA Step 4, in the area of PSA, Technical Service Framework Support was used in accordance with the plan outlined in Ref. 1, i.e.:

- Lead PSA Review.
- Thermal-hydraulic Analysis (to support the assessment of the Level 1 PSA Success Criteria).
- Severe Accident Analysis (to support the assessment of the Level 2 PSA).
- Consequence Analysis (to support the assessment of the Level 3 PSA).
- In addition, TSCs were engaged to support the assessment of the Containment Structural Analysis (for the Level 2 PSA assessment), the analysis of fragilities of structures and components (for the assessment of the Seismic Margins Analysis) and to provide advice on hazards curves.

31 The Lead PSA TSC undertook the following key tasks:

- Assessment of specific PSA technical aspects according to a specification agreed with ND.
- Drafting of proposed Technical Queries (PTQ).
- Evaluating the responses provided by Westinghouse to relevant TQs and ROs.
- Documenting the assessment work done and the findings.
- Coordinating external inputs to the PSA assessment (Success Criteria, Severe Accident, Structural Integrity, Civils and External Hazards) into the overall PSA assessment.
- Conducting the Risk Gap Analysis (RGA) taking into account all the information compiled during the assessment.
- Preparing, attending and evaluating the outcome of the following meetings with Westinghouse: Technical Exchange Workshops in May and October 2010, Coordinated Reviews of the Success Criteria and Event Trees in March and June 2010, Risk Gap Analysis Workshop in August 2010, Third Technical Exchange Workshop and PSA Assessment Wrap-up Meeting in February 2011.
- Production of a Final Report following the structure agreed in advance.

32 Visibility of TSC work and feedback on progress and outcomes of TSC work was provided to Westinghouse throughout the process.

2.3.4 Cross-cutting Topics

33 The PSA covers all the technical areas addressed by other teams during GDA (as discussed in Section 2.3.5 below). In this sense the quality of the PSA relies on the quality of the input, and the adequacy of the substantiation, provided in the other technical areas. Therefore, GDA Issues and Findings in other areas may impact the ability of the current PSA to predict the risk of the AP1000. Of particular concern are GDA Issues raised in relation to the spent fuel pool and internal hazards.

34 The milestones assigned to the Assessment Findings (Annex 1) have been chosen to ensure that future updates of the PSA capture all the developments in the cross-cutting areas.

2.3.5 Integration with Other Assessment Topics

35 The interactions between PSA and some other technical areas were formalised since aspects of the assessment in those areas have constituted formal inputs to the PSA assessment. For the AP1000 PSA these were:

- Human Factors: provided input to the HRA assessment. This work was led by ND's Human Factors team and is reported elsewhere (Ref. 26).
- Fault Studies: provided input to the assessment of the Level 1 PSA Success Criteria. This work was led by ND's PSA team in coordination with the Fault Studies team.
- Severe Accident Analysis: the aim of this task was to provide input to the assessment of the Level 2 PSA by carrying out confirmatory analyses with a separate computer code of some severe accident scenarios selected by the PSA assessment team. This work was led by ND's Fault Studies (Severe Accidents) team with input from my team. At the time of writing this report the work had not yet been completed and therefore it is not reported here. See instead Ref. 27.
- Structural Integrity: provided input to the assessment of the Containment Structural Analysis for the Level 2 PSA. This work was led by my team in coordination with the Structural Integrity team.
- Structural Integrity: provided input to the assessment of the Seismic Margins Analysis (SMA) regarding fragilities of metal components. This work was led by ND's External Hazards team in coordination with the Structural Integrity and PSA teams.
- Civil Engineering / External Hazards: provided inputs to the assessment of the screening of external hazards and of the Seismic Margins Analysis regarding definition of hazard curves, and fragilities of structures. This assessment task was led by ND's Civil Engineering and External Hazards team in coordination with my PSA team.
- Radiological Protection: provided input to the assessment of the Level 3 PSA. This work was led by ND's Radiological Protection team.

36 Another interaction that was formalised was between PSA and Control and Instrumentation (C&I) since the PSA assessment of the C&I modelling and related sensitivity analyses constitutes an input to ND's assessment of the C&I.

37 In addition to the above, there were interactions between PSA and the rest of the technical areas. These interactions happened continuously during GDA Step 4, they were two-way, and they were, mostly, of an informal nature. It should be highlighted that the interactions with Mechanical and Electrical Engineering and Internal Hazards were of particular benefit to the PSA assessment.

2.3.6 Out of Scope Items

38 No PSA related items have been left out of the scope of the PSA review in GDA. However, as discussed in relevant sections in this report, the following should be noted:

- Detailed review of the PSA Human Reliability Analysis (HRA) has been undertaken by ND's Human Factors assessment team and is reported elsewhere (Ref. 26)
- Some RO responses arrived too late in the GDA process for my team to be able to assess them in detail, i.e. responses to RO-AP1000-099 on "Steam Generator Tube Rupture PSA Model" (Ref. 37) and RO-AP1000-044-A1 on "Fire PSA" (Ref. 32).
- A new evaluation of the risk associated with the Spent Fuel Pool was included in the response to RO-AP1000-054 raised by ND's Fault Studies team (Ref. 38). This also arrived too late in the GDA process and was not taken into consideration within the PSA assessment.

39 In addition, the review did not cover in detail the following PSA-related technical aspects:

- Validation and verification of the various computer codes used to support the PSA (see Section 4.3 below for further discussion).
- Detailed review of the PSA quantification (see Section 4.3 below for further discussion).
- Compliance against Target 8 "Frequency dose for accidents on an individual facility – any person off the site" from NT.1 of the SAPs (Ref. 4). A supplementary PSA study to properly address compliance with this target has not been presented by Westinghouse. See Sections 4.18 and 4.19 for further discussion.
- Compliance against Numerical Target NT.2 "Time at risk" of the SAPs (Ref. 4) during operation at power. A supplementary PSA study to properly address compliance with this target has not been presented by Westinghouse but the low CDF and LRF currently estimated provide confidence that, with good management of testing and maintenance, the future licensees will be able to comply with NT.2.

3 REQUESTING PARTY'S SAFETY CASE

40 Westinghouse developed a PSA to support the design of the AP600 in the 1990s. This practice was carried over to the design of the AP1000.

41 The construction of the PSA is based on the standard small event tree / large fault tree approach, and is a Level 1 PSA, Level 2 PSA and a simplified Level 3 PSA.

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

43 A separate PSA of the Spent Fuel Pool has also been submitted by Westinghouse.

44 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.

45 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).

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

Table 1: AP1000 PSA Results (from Refs 25 and 28)

Item	AP1000
Core Damage Frequency (CDF) internal events at power	2.13×10^{-7} /yr
Frequency of Plant Damage State (PDS) "1A": Core damage with Reactor Coolant System (RCS) at high pressure following transient or Small Loss of Coolant Accident (SLOCA)	5.46×10^{-9} /yr
Frequency of PDS "1P": Core damage with RCS at high pressure following transient with PRHR operating or Medium Loss of Coolant Accident (MLOCA)	3.92×10^{-9} /yr
Frequency of PDS "2L": Core damage with RCS depressurised, successful gravity injection and failure of recirculation	1.65×10^{-8} /yr
Frequency of PDS "2E": Core damage with RCS depressurised	7.87×10^{-8} /yr
Frequency of PDS "2R": Core damage with RCS depressurised, and failure of Core Make-up Tank and Accumulators	4.39×10^{-8} /yr
Frequency of PDS "3A": Core damage with high RCS pressure and Anticipated Transient without SCRAM (ATWS)	9.05×10^{-10} /yr
Frequency of PDS "3C": Core damage following Reactor Pressure Vessel (RPV) rupture	10^{-8} /yr
Frequency of PDS "3D": Core damage with partial RCS depressurisation	4.04×10^{-8} /yr
Frequency of PDS "6": Core damage following Steam Generator tube rupture	9.67×10^{-9} /yr
Other (1.65% of the CDF unaccounted for in the L2 PSA)	3.52×10^{-9} /yr

Item	AP1000
Large Release Frequency (LRF) (reactor internal events at power)	1.86×10^{-8} /yr
Frequency of Release Category (RC) “BP”: Containment bypass	1.28×10^{-8} /yr
Frequency of RC “CI”: Containment isolation failure	4.97×10^{-10} /yr
Frequency of RC “CFE”: Early containment failure	4.41×10^{-9} /yr
Frequency of RC “CFI”: Intermediate containment failure	7.15×10^{-11} /yr
Frequency of RC “CFL”: Late containment failure	8.69×10^{-10} /yr
CDF internal hazards (fires and floods) at power	5.69×10^{-8} /yr
CDF internal events during low power and shutdown	1.03×10^{-7} /yr
CDF internal hazards (fires and floods) during low power and shutdown	8.8×10^{-8} /yr
LRF (reactor internal events during low power and shutdown)	2.05×10^{-8} /yr (**)
Fuel Damage Frequency (internal events in the spent fuel pool)	1.59×10^{-10} /yr
(**) This value is a scaling of the AP600 analysis to the AP1000 CDF	

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT OF THE AP1000 PROBABILISTIC SAFETY ANALYSIS

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

48 For each of the relevant "assessment expectations" in the tables contained in Appendix 1 of T/AST/030 (Ref.15), a view on the adequacy or otherwise of the submitted documentation, including any appropriate TQ and RO responses, has been taken. In cases where limitations and / or potential findings have emerged there has been dialogue with Westinghouse in an effort to resolve the problem or identify if further information could be provided within the GDA timeframe.

49 My GDA Step 3 PSA assessment identified shortfalls in all the technical areas of the PSA. These shortfalls generally led to the issue of TQs. With a number of exceptions, the responses to these TQs have rarely been accompanied by new analysis or purpose written documentation but have however often acknowledged the potential PSA limitation pointed out in the TQ and the need to include new analysis in the future update of the PSA.

50 Similarly, Westinghouse has not provided new analysis in responses to some of the Regulatory Observations I raised. These affected the following areas of the PSA: Systems Analysis (RO-AP1000-045), Sequence Analysis (RO-AP1000-072) and Fire PSA (RO-AP1000-044).

51 New PSA analysis has however been performed by Westinghouse in response to RO-AP1000-099 (Steam Generator Tube Rupture PSA Model), and in response to RO-AP1000-068, related to In-vessel Retention (IVR), raised by the Severe Accident assessment team. The response to RO-AP1000-068 has been assessed by my PSA assessment team. The results of this review are reported in Section 4.18 below. The response to RO-AP1000-099 arrived too late in the GDA process for ND's PSA assessment team to be able to review it in detail. However, an initial look at it appears to show significantly enhanced traceability between the new event tree and the supporting analyses.

52 Details of my assessment of the AP1000 PSA, and the conclusions and findings are given in the following sections. To help traceability, the section number (A1.i.i) of the Table of Assessment Expectations in Appendix 1 of T/AST/030 (Ref. 15) is included.

4.1 General Expectations – Approaches and Methodologies (A1-1.1) and Freeze Date (A1-1.3)

53 The methods and data used in the AP1000 PSA are well known, although not always up-to-date or aligned with the latest international good practices. This is discussed in more detail for each individual technical area of the PSA in the following sub-sections.

54 In July 2010 Westinghouse sent letter WEC 000258 including a draft "AP1000 PSA Update High Level Plan" (Ref. 30). This shows specific tasks for development of Guidebooks for the various PSA technical areas. Although in principle this provided certain degree of confidence that future work on PSA would take into account modern standards, I requested to see several examples within GDA timeframes. Two draft task procedures for PSA systems analysis and Fire PSA were submitted by Westinghouse in

responses to RO-AP1000-045-A1 and RO-AP1000-044-A1 respectively (Refs 31 and 32). From this the following should be noted:

- The PRA System Analysis Guidebook (Ref. 31) is an improvement from the existing Fault Tree Guidelines presented in Chapter 7 of the PSA documentation (Ref. 21). It was noted that the new PRA System Analysis Guidebook includes in Section 8 a mapping with table A1-2.4 of ND's PSA TAG – this is considered positive however it does not ensure total consistency with my expectations. In fact, the assessment of Ref. 31 has shown that many of the general concerns raised in my GDA Step 3 review have not been solved by Westinghouse. The new PRA System Analysis Guidebook is considered to be limited in scope and not specific enough in expressing some of the instructions included. In addition, the guidance on mission times and the rules for including or excluding failure modes from the fault trees do not appear consistent with modern standards and expectations in ND's PSA TAG (Ref. 15).
- The Fire PRA Guidebook (Ref. 32) arrived too late in the GDA process for my assessment team to be able to review it in detail. However, Action **GI-AP1000-PSA.02.01** of the Fire PSA GDA Issue (see Annex 2) requires Westinghouse to provide the final approved version of this Guidebook – my PSA team will review it in detail at that time.

  Assessment Finding AF-AP1000-PSA-001: *The Licensee shall provide an enhanced PRA System Analysis Guidebook to provide wider and more detailed guidance and to remove instructions potentially leading to models which are optimistic or limited to support operational decisions.*

  Assessment Finding AF-AP1000-PSA-002: *The Licensee shall implement and provide task procedures for all the technical areas of the PSA.*

55 As discussed in Section 2.3 (Assessment Scope) above, I requested Westinghouse to clearly establish what PSA models and documentation would be put forward by Westinghouse for my review during GDA Step 4. In response to this, Westinghouse submitted letter UN REG WEC 000131 (Ref. 20). This letter lists the versions of the PSA models, documentation and supporting analyses to be reviewed during GDA Step 4. Nonetheless, it should be stressed that there is no guarantee or confidence that the AP1000 PSA reviewed is consistent with the design and safety documentation reviewed by GDA teams in other technical areas. This is not considered a limitation of the PSA review itself since many of the findings described in the following sub-sections are valid and applicable despite the lack of consistency between the AP1000 design status and the PSA models. However, a site-specific, complete and updated PSA should be available before the pouring of nuclear island safety related concrete starts – at that point the freeze date for the design and other operational features reflected in the "site-specific" PCSR should be clear and the PSA and its supporting documentation should be consistent with the design freeze date.

Assessment Finding AF-AP1000-PSA-003: *The Licensee shall provide a "site-specific" PCSR PSA whose freeze date is consistent with the design freeze date.*

4.2 General Expectations – PSA Scope (A1-1.2)

4.2.1 Assessment

56 It was already identified in GDA Step 3 that the purpose of the PSA stated in Chapter 1 of the PSA documentation (Ref. 21) was 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)).

57 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. 15).

58 No further assessment has been undertaken in GDA Step 4 in terms of appraisal of the PSA scope. Strengths and findings from GDA Step 3 remain valid. These are summarised in the following sub-sections.

59 During GDA Step 4 I performed a Risk Gap Analysis (RGA) to address the findings in all the PSA technical areas and to understand their potential risk significance. To some extent the RGA has addressed some of the limitations in the scope of the PSA, such as the current omission of external hazards (see Sections 4.13 and 4.14 below). Quantitative evaluation of other limitations in the scope of the AP1000 PSA could not be done due to lack of resources, within the scope and timeframes of GDA, to develop new models and / or extend the existing ones (for example, to propagate Level 1 PSA internal hazards sequences into the Level 2 containment event trees). This however has not precluded the RGA from providing useful insights to understanding the risk of the AP1000.

4.2.2 Strengths

60 The AP1000 PSA comprises Level 1 PSA (Core Damage Frequency, CDF), Level 2 PSA (Large Release Frequency, LRF) and a simplified Level 3 PSA.

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

62 A PSA for the Spent Fuel Pool has also been submitted.

4.2.3 Findings

63 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 6, 33, 34 and 35.

64 From the review I have identified the following shortcomings in relation to the scope of the PSA:

- The PSA documentation (Ref. 21) 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.
- The risk associated with non-core damage sequences has not been evaluated and integrated with the overall PSA results.
- Sequences where core damage / containment failure may happen in the long term are excluded from the evaluation of the risk.
- Formal screening of internal hazards has not been undertaken. 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 is 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).

Assessment Finding AF-AP1000-PSA-004: *Before pouring nuclear island safety related concrete the Licensee shall provide evidence that a full scope site-specific PSA is in place or a demonstration that the scope of the PSA at the start of nuclear safety related construction is representative of the installation being constructed, is bounding and provides sufficient insights into the relative vulnerabilities and strengths of the plant design in the specific site.*

Assessment Finding AF-AP1000-PSA-005: *The Licensee shall provide a full scope PSA for the AP1000.*

Assessment Finding AF-AP1000-PSA-006: *The Licensee shall provide an evaluation of the frequency of, and radiological releases and consequences from, AP1000 accident sequences without core damage.*

4.2.4 Conclusions

65 The scope of the AP1000 PSA (together with the Seismic Margins Analysis) is considered to be too limited to support the AP1000 "generic" PCSR PSA. However my work during GDA has allowed an initial understanding of the potential impact of the scope limitations – this is discussed in the following sub-sections. In any case, the limitations identified by the review need to be addressed as part of the next update of the PSA (see Section 5 below).

4.3 General Expectations – Computer Codes and Inputs (A1-1.4)

4.3.1 Assessment

66 During the review of the different technical areas of the PSA, my team looked at the various codes used by Westinghouse but did not undertake extensive in-depth reviews of the code validations, input decks and qualifications and experience of the code analysts. Instead, the judgement regarding the adequacy of the codes and their use by Westinghouse for the PSA was based on:

- The review team members' knowledge of the codes and their international status.
- Spot checks of some calculations and input data files.
- Some confirmatory calculations.
- Interactions with Westinghouse's code users.
- Input from ND's Fault Studies assessment team (Ref. 36).
- Confirmatory analyses with MELCOR of some severe accident scenarios selected by my team (It should be noted that at the time of writing this report the work had not yet been completed and therefore it is not reported here. Instead refer to the Severe Accidents Assessment Report, Ref. 27).

- Confirmatory consequence analyses with PC-COSYMA.

67 The original PSA model was built using Westinghouse's in-house software and later transferred to the well established internationally used CAFTA software developed by the Electric Power Research Institute (EPRI). While no concerns were raised regarding the CAFTA code itself, the way in which Westinghouse had used the code was questioned.

68 The majority of the thermal-hydraulic calculations for the Level 1 PSA success criteria have been performed with the MAAP4 code. The PSA documentation (Ref. 21) indicates that MAAP4 was chosen for its speed, flexibility and ease to use. In addition, MAAP4 provides an integrated reactor and containment response. MAAP4 is a code originally developed for severe accident analysis but can also be used to determine the thermal-hydraulic behaviour prior to core damage. Westinghouse has used MAAP4 to support the Level 1 PSA success criteria analysis for the AP1000 on the basis of the following:

- MAAP4 was benchmarked for its use for the AP600 against the more detailed models in NOTRUMP, the Westinghouse-validated code for AP600 small-break Loss of Coolant Accidents (LOCA). This benchmarking was evaluated by US NRC who concluded that MAAP4 was an adequate screening tool for evaluating PRA success criteria for the AP600, subject to the limitations discussed by Westinghouse in WCAP-14869 (Ref. 39). It seems that the use of MAAP4 as a "screening tool" means that for cases where acceptance criteria were not clearly met confirmatory analyses for the AP600 were performed with design basis codes (Ref. 40).
- Westinghouse performed an evaluation for the AP1000 to determine the thermal-hydraulic uncertainty resulting from the use of MAAP4 to support the Level 1 PSA success criteria. This work identified risk important sequences with low margins. For these, further analyses with other codes such as NOTRUMP were undertaken which provided Westinghouse with additional confidence on the suitability of MAAP4.

The suitability and use of MAAP4 to support the AP1000 Level 1 PSA was addressed in my review of the PSA success criteria during GDA Step 4 (Section 4.5 below). It should be noted that my team did not review the results of the MAAP4 validation believed to be described in the code's User's Manual. In addition, the code NOTRUMP has been considered in the Fault Studies assessment (Ref. 36).

69 The AP1000 success criteria analysis for Anticipated Transients Without SCRAM (ATWS) is supported by calculations with the computer codes LOFT4AP and LOFTRAN. As explained below in Section 4.5, a detailed review of the success criteria for ATWS was conducted but not followed-up within GDA because Westinghouse was at that time conducting new ATWS analysis. Therefore my team did not look in detail at the use of these codes and their applicability to support PSA. LOFTRAN has however been considered in the review conducted by ND's Fault Studies team (Ref. 36).

70 Westinghouse methodology to address the success criteria for long term cooling was based on the use of the WCOBRA-TRAC and WGOTHIC computer codes. The two codes were not reviewed in detail but the application of those codes was considered appropriate by the review team. These two codes have however been looked at in detail during the review conducted by ND's Fault Studies team (Ref. 36).

71 For the Level 2 PSA Westinghouse has used MAAP4 to support the severe accident progression analyses and a stand-alone model to support the analysis of In-Vessel Retention (IVR). As indicated above and discussed in more detail in Section 4.18 below, confirmatory analysis with the MELCOR code of some severe accident scenarios had been planned to support my assessment of the Level 2 PSA. For example, these

confirmatory analyses would have helped me to understand and judge whether the MAAP4 code had been used by Westinghouse within its limit of applicability and also whether the AP1000 nodalization for the MAAP4 severe accident evaluations was appropriate for the application. At the time of preparing this report the MELCOR analysis work was not complete; this limited my assessment of the adequacy of Westinghouse's use of MAAP4 for the AP1000 Level 2 PSA.

4.3.2 Strengths

72 MAAP4 is a well recognised and widely used code, which was originally developed for severe accident analysis. Despite the fact that Westinghouse has not provided specific evidence (requested via a TQ) that the analysts who carried out the MAAP4 calculations for the Level 2 PSA were suitably qualified and experienced, during the review of the Level 2 PSA and the interactions between my team and Westinghouse's severe accident specialists, the knowledge and expertise of Westinghouse's lead MAAP4 analyst was apparent.

4.3.3 Findings

73 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 36 and 41.

74 Westinghouse has used the modern PSA software CAFTA, however, many gates are not described and many event descriptions are too general or ambiguous, which impairs the understanding of the model. The CAFTA model does not include the Fire and Flooding PSA models or models for those initiating events analysed via fault trees. 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).

> ***Assessment Finding AF-AP1000-PSA-007:*** *The Licensee shall provide an electronic model of the complete AP1000 PSA making the best possible use of the PSA software capabilities regarding the integration between event trees and fault trees and including clear descriptions for all the basic events and gates.*

75 My review team looked at the reactor nodalization for MAAP4 and the benchmarks between MAAP4 and NOTRUMP undertaken to justify the use of MAAP4 for the AP600 Level 1 PSA success criteria (Ref. 39) and observed that in the MAAP4 analyses, the water inventory in the primary circuit appears to be overestimated with respect to the NOTRUMP results. This may be due to simplifications in the physical model for MAAP4. Because of this shortcoming, the analyses with MAAP4 could lead to optimisms in the estimation of the timings to core uncovery and peak cladding temperatures. Additional concerns were raised regarding MAAP4's lack of a two-phase flow model which could have an impact in the prediction of mass loss during blowdown. Therefore, despite Westinghouse's AP1000 analyses, discussed in 4.3.1 above, addressing the thermal-hydraulic uncertainties associated with the use of MAAP4 to support the Level 1 PSA success criteria, concerns remained in this area.

> ***Assessment Finding AF-AP1000-PSA-008:*** *The Licensee shall provide a revised demonstration that the limitations of the codes selected to undertake the thermal-hydraulic and neutronics analyses for the PSA do not impact the AP1000 PSA success criteria.*

76 It was noted that MAAP4 was chosen to support the Level 1 PSA for its speed, flexibility and ease of use. One would therefore think that this would provide the ideal tool for

analyzing a much wider range of AP1000 specific scenarios, supplemented by extensive sensitivity analyses to ensure that the success criteria for each event tree sequence were bounding without undue conservatism. In fact, Westinghouse only conducted some LOCA calculations for the AP1000 and my team felt that Westinghouse did not take full advantage of a code that was fast running to provide a more complete understanding of the sequence modelling. This failing to use a highly efficient code ultimately left the event sequence modelling weakly supported by specific success criteria analysis (as discussed in Section 4.5 below).

77 LOFTRAN has been looked at by ND's Fault Studies team who has concluded that this code is too conservative and simplified to be used to support PSA best estimate success criteria evaluations (Ref. 36).

> ***Assessment Finding AF-AP1000-PSA-009:*** *The Licensee shall provide revised ATWS success criteria analyses using a best estimate code.*

78 Westinghouse did not provide a detailed description of the validation work for the MAAP4 model of the AP1000, as used to support the Level 2 PSA. According to information provided by Westinghouse the validation work was done by the code developers and is described in the code's User's Manual. This is considered to be a documentation gap in the PSA documentation. In addition, in response to a Technical Query from the review of the Level 2 PSA, Westinghouse provided the MAAP4 input parameter file. However, scenario definitions, full outputs and a tabulation of runs, input files and outputs (i.e., configuration control and cross reference information) were not provided. This hindered the traceability between the sequences and nodes in the Containment Event Tree and the supporting code calculations. It also raised a concern regarding the auditability of the input data files for the code calculations.

> ***Assessment Finding AF-AP1000-PSA-010:*** *The Licensee shall provide revised PSA documentation including information on: 1) validation and verification for all the codes used; 2) plant nodalization and plant parameter files for all the codes used; and 3) showing full traceability between the PSA models and the supporting analyses.*

4.3.4 Conclusions

79 Based on the outcome of this assessment, I have concluded the following:

- Most of the codes supporting the PSA and the way they have been used are sufficient to support the AP1000 "generic" PCSR PSA.
- A GDA Issue has been raised in the area of success criteria analysis which also refers to the codes used by Westinghouse for that purpose (see Section 4.5 below).

4.4 Level 1 PSA: Identification and Grouping of Initiating Events (A1-2.1)

4.4.1 Assessment

80 A detailed review was conducted during GDA Step 3 to confirm whether the bases of the PSA were robust and to gain confidence on its completeness. From this review a number of Technical Queries were raised.

81 During GDA Step 4 my team evaluated in detail Westinghouse's responses to the TQs issued in GDA Step 3 and identified the findings discussed in the following sub-section. This review confirmed what had already been anticipated in my GDA Step 3 PSA report

(Ref. 6), i.e. that there are a number of Initiating Events (IE) missing from the PSA's Fault Schedule and that some IEs have been grouped incorrectly.

82 The detailed review of the "Identification and Grouping of Initiating Events" discussed in this section of the report focuses on internal initiating events that can occur in the full power operating mode. The reviews of the initiating events in low power and shutdown, those related to the fuel ponds and of the initiating events that can occur as a consequence of external and internal hazards are documented in other parts of this report.

83 I performed a Risk Gap Analysis to address the findings in this area and to understand their potential risk significance. An initial screening of findings was conducted using qualitative arguments and applicable quantitative information from the PSA. This resulted in a list of those IEs missing from the PSA and those IEs grouped wrongly which were judged to have a non-negligible numerical risk impact. These were subject to further quantitative evaluation as follows:

- IE frequencies were estimated using current PSA data, C&I conservative estimations and engineering judgement.
- Conditional Core Damage Probabilities (CCDP) were estimated by conducting re-evaluations with the existing PSA models or cutsets, using surrogate event trees, i.e. transients or LOCAs as appropriate and setting to "true" those basic events failed by the IE itself.
- The "loss of support systems" IEs screened in were evaluated semi-quantitatively. For this I assumed a high frequency of occurrence of the first failure or precursor. I then assigned a probability of recovery and assumed plant impacts believed to be conservative.
- Only the impact on CDF was explored.

4.4.2 Strengths

84 Despite the limitations found (discussed below), Table 2.1 of the PSA report (Ref. 21) presents a well organised list of IEs. Early in GDA Step 3 when ND's Fault Studies team discussed with Westinghouse the lack of a formal Fault Schedule for the AP1000 that would meet UK expectations (which finally led to issuing RO-AP1000-046), ND's PSA team was able to help Westinghouse's Design Basis Analysis (DBA) specialists to understand the UK expectations using the information in the PSA document. So, this part of the PSA documentation has already proved useful for the development of the AP1000 Fault Schedule. It will be a good basis for the future development of a more comprehensive and up-to-date list of IEs for future updates of the AP1000 PSA.

4.4.3 Findings

85 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35 and 42.

86 In my GDA Step 3 PSA report (Ref. 6) I indicated that Westinghouse should enhance the documentation of the "Identification and Grouping of Initiating Events" so that the traceability and completeness are evident. In particular, on completion of the review, the following general concerns have been highlighted:

- The PSA report does not describe a systematic assessment process to identify initiating events. A "core damage logic diagram" is presented, but it does not seem to be used in practice.
- The identification process for "generic" initiating events relies almost completely on NUREG/CR-3862 (May 1985). It is not apparent that any other sources of initiating events from other plant PSAs or more recent industry operating experience were used.
- The process for grouping initiating events is not clear, i.e. the grouping criteria and the mapping to derive the final initiating event groups are not transparent.

Assessment Finding AF-AP1000-PSA-011: *The Licensee shall put in place a robust process for identification and grouping of Initiating Events and shall provide revised PSA documentation describing in detail such process*

87 The review has concluded that the following IEs are missing from the PSA and should be included:

- Rupture of multiple tubes in the Passive Residual Heat Removal System (PRHR).
- Interfacing System Loss of Coolant Accident (LOCA) in the low pressure letdown piping of the Chemical and Volume Control System (CVS).
- Loss or reduction in feedwater flow (one loop).
- Spurious opening of turbine bypass valves.
- Spurious Core Makeup Tank (CMT) actuation.
- Spurious draining of the In-containment Refuelling Water Storage Tank (IRWST).
- Spurious actuation of the PRHR.
- Spurious CVS actuation.
- Loss of High Capacity Chilled Water System.
- Loss of Low Capacity Chilled Water System.
- Loss of the Heating, Ventilation and Air Conditioning System (HVAC).
- Loss of power at individual 11kV Busbars.
- High Voltage Transformer Failures (UATs & RATs).
- Loss of power at 125 Vdc Busbars.
- Spurious Low Steam Line Pressure Signal.
- Spurious Low T-Cold Signal.
- Spurious protection signals and feedwater control faults that disable the flow from both the Main Feedwater System (MFW) and Startup Feedwater System (SFW) to one or both Steam Generators (SG).
- Anticipated Transient without Reactor Shutdown (ATWS) following Loss of Offsite Power (LOOP).
- LOOP as a consequence of any other IE is also missing.
- Secondary steam line break or feed water line break occurring as a consequence of the various steam line breaks (inside or outside containment respectively) are also

missing. These missing consequential events have been identified during the review of the AP1000 Internal Flooding PSA (see Sub-section 4.12 below).

- As well as the above missing IEs identified during my review, additional IEs identified by Westinghouse during the work done to respond to RO-AP1000-046 also need to be included in the PSA.

Assessment Finding AF-AP1000-PSA-012: *The Licensee shall provide a revised PSA taking into consideration all the Initiating Events and consequential Initiating Events which have been identified as missing (both by the GDA review and by themselves using the enhanced process for identification and grouping of IEs as per previous finding).*

88 My review team identified cases in which either the plant response would not be the same for all the IEs grouped together, or the success criteria used in the event tree for the IE group was not applicable to all the IEs included in the group. The review has therefore concluded that a number of IEs have been grouped wrongly. The implications are that the PSA models (event trees) used for the IEs assigned to the wrong group are not representative. Findings related to inadequate grouping of IEs are as follows:

- Grouping of "(relevant) Spurious Actuations of the Automatic Depressurisation System (ADS)" and "Pressuriser LOCAs" into the "Medium LOCA" IE group.
- Grouping of "Small Breaks in Pressuriser" and "Small Breaks in PRHR" into the "Small LOCA" IE group.
- Comments have been raised regarding the number of tube breaks included in the "Steam Generator Tube Rupture (SGTR)" group (also raised in the Event Tree and Success Criteria reviews and discussed in more detail in the corresponding sections below) and inadequate grouping of SGTR and Consequential SGTR (following Steam Line Break, SLB) in the same event tree.
- Grouping of "Leakage from Control Rods", "Leakage in Primary System" and "Pressuriser Water Leakage" into the "Transient with MFW" IE group.
- Grouping of "Turbine Trip", "Closure of a Main Steam Isolation Valve (MSIV)", "High-2 Containment Pressure", and "Spurious Opening of Pressuriser Spray" under the IE group "Transient with MFW".
- Grouping of "Loss of Turbine Building Closed Cooling Water System" into the "Loss of MFW Flow to Both SGs" IE group.
- (Apparent) grouping of "Loss of Offsite Power with successful grid recovery within 30 minutes" into the "Loss of MFW Flow to Both SGs" IE group.
- Grouping of "Inadvertent Closure of all MSIVs" into the "Loss of MFW Flow to Both SGs" IE group.
- Grouping of "Increase in Feedwater Flow (1 loop)" and "Increase in Feedwater Flow (all loop)" into the "Loss of MFW Flow to Both SGs" IE group.
- Concerns regarding grouping (and modelling) of the various "Transformer Failures" into the "LOOP" IE group.
- Grouping of "ATWS following SLB" into the "ATWS with Safety Injection (SI)" IE group.

- Grouping of “SLB Upstream of the MSIVs Outside Containment” and “Main Steam Line Safety Valve Stuck Open” in the same event tree “SLB-V”.

Assessment Finding AF-AP1000-PSA-013: *The Licensee shall provide a revised list of Initiating Events for the PSA correctly grouped.*

89 In addition to the above, it should be noted that in response to TQs that I raised in this area Westinghouse made some commitments to address identified shortcomings. Also, Westinghouse provided relevant technical information which should be formally included in the PSA documentation.

Assessment Finding AF-AP1000-PSA-014: *The Licensee shall provide revised documentation of the PSA task on Identification and Grouping of Initiating Events taking into account commitments made and relevant technical information provided in responses to TQ-AP1000-094 to 127.*

90 The RGA for this particular area of the PSA has shown that the most significant numerical gaps could be associated with the following IEs currently not included in the PSA or incorrectly grouped:

- Spurious IRWST draining: In this case the gap may depend on the results of specific analysis of the event (which is currently unavailable), and also on specific indications, procedures and training (which could impact the operator ability to detect and isolate draining events). At the time of writing this report it was not clear what signals could be produced by such an event and how the various mitigating systems could be affected by such signals.
- Loss of support systems (HVAC, Chilled Water Systems, 125Vdc): In these cases the risk gaps may depend on the final design of support systems, site specific characteristics (i.e. temperatures), and procedures and training to deal with the specific losses of support systems.
- Small LOCA in the PRHR (system) for which, unlike for Small LOCAs (SLOCA) in other locations, the PRHR would be unable to meet its function and therefore it cannot be credited.

4.4.4 Conclusions

91 Based on the outcome of this assessment, I have concluded that the current list of IEs together with the results of the RGA, are enough for my team to get a reasonable understanding (sufficient for the “generic” PCSR stage) of the AP1000 risk associated with internal events at power.

92 There is however a caveat to the above. As discussed below in Sub-sections 4.5 (Success Criteria) and 4.11 (Fire PSA), my team has found sufficient shortcomings in those two particular areas that have led to raising GDA Issues to address them. It is my judgement that any further work on success criteria or Fire PSA will be incomplete and inadequate if it is based on the current incomplete list of IEs. Therefore, Westinghouse needs to address the findings from the review of the “AP1000 Identification and Grouping of IEs” to effectively respond to the GDA Issues on “Success Criteria” and “Fire PSA”. This has been captured in GDA Issue Actions **GI-AP1000-PSA.01.03** (PSA Success Criteria GDA Issue), and **GI-AP1000-PSA.02.03** (Fire PSA GDA Issue).

93 This part of the AP1000 PSA is insufficient to support further stages of the NPP development and a more complete list of IEs correctly grouped should be available before any other developments of the PSA are undertaken.

4.5 Level 1 PSA: Accident Sequence Development – Determination of Success Criteria (A1-2.2)

4.5.1 Assessment

94 A high level review of the AP1000 PSA task on "Success Criteria Analysis" against the expectations in T/AST/030 (Ref. 15) was conducted during GDA Step 3. This review raised general concerns in the following areas:

- Traceability of the success criteria to the supporting analyses.
- Justification of timing for operator actions.
- Conservatisms in the success criteria analysis for the PSA.
- Reliance on the AP600 PSA documentation and supporting analyses.

95 The objective of the Step 4 PSA assessment was to undertake a detailed review (on a sampling basis) of all the PSA technical areas in order to confirm or otherwise the concerns raised during my GDA Step 3 assessment. For the assessment of the AP1000 PSA Success Criteria the following Initiating Event Groups in the PSA were selected:

- Small LOCA.
- Loss of Main Feedwater.
- Steam Generator Tube Rupture.
- Medium LOCA.
- ATWS without Main Feedwater.
- Steamline Break Upstream of the MSIVs.

96 The above selection provided a good representation of all the types of Initiating Events that can occur in an AP1000 reactor and would ensure that my review would address the thermal-hydraulic behaviour of the reactor in a comprehensive manner.

97 In order to support my GDA Step 4 review I requested Westinghouse to develop Routemaps of the success criteria in the selected event trees to the specific calculations carried out to justify these, and to provide all the supporting documentation (Ref. 43).

98 My GDA Step 4 review of the PSA success criteria and event trees identified that the success criteria supporting the "Steam Generator Tube Rupture" model was based solely on AP600 analyses, the applicability of which was not apparent. Also the analyses had not been extended to cover multiple tube ruptures despite the fact that ruptures of up to five tubes are grouped under the same IE group "SGTR" in the PSA. These findings related to the SGTR success criteria, the concerns raised during the detailed review of the SGTR event tree (see Section 4.6 below) and the high significance of this IE to the overall AP1000 risk, were the reasons why in September 2010 I issued RO-AP1000-099. RO-AP1000-099 requested Westinghouse to provide a revised and documented SGTR event tree based on AP1000 specific success criteria with sufficient coverage for all sequences delineated in the event tree and for all sizes of SGTRs included in the IE group.

99 Although a detailed review of the success criteria for "ATWS without Main Feedwater" was conducted, I decided not to follow that up with formal TQs / ROs. This is because Westinghouse was at the time doing new ATWS analyses, and that could have a significant impact on the PSA success criteria. However, the initial review of the success

criteria for "ATWS without Main Feedwater", which identified a number of shortcomings, was provided to Westinghouse with the expectation that the information and comments included in the review should be taken on board when conducting the new analyses.

100 As discussed in Section 4.5.4 below, a GDA Issue has been raised in this area and therefore Westinghouse's response to this will provide the risk gap in relation to the PSA success criteria analysis. Because of this, general cross-cutting success criteria findings (e.g. degree of applicability of AP600 analysis) were left out of the RGA and only a limited scope gap evaluation was performed to address qualitatively some specific findings screened in up front. In addition, the findings related to the success criteria for SGTR were not addressed in the RGA either. Instead, as indicated above, RO-AP1000-099 was raised for Westinghouse to conduct new SGTR analysis. The limited scope RGA to address success criteria was combined with the RGA to address findings from the review of the event trees because of the similar nature and consistency of some of the findings from both reviews. The results are discussed in Section 4.6.3 below.

4.5.2 Strengths

101 For each initiating event group, the safety functions, the systems which can perform each of the functions, and any need for operator intervention, are identified in tables in the PSA documentation (Ref. 21). For the six Initiating Events selected for GDA Step 4 assessment, Westinghouse's Routemap (Ref. 43) provided further relevant information. In fact the Routemap provided systematic documentation of the derivation of the success criteria for the system functions and it was an important effort that facilitated the review.

102 The limiting conditions defined for success / failure (for example, cladding temperature, coolant system pressure, coolant system level, enthalpy in fuel pellets, containment temperature and pressure, etc.) are stated, justified, and are realistic. These are documented in Chapter 6 and Appendix A of the PSA documentation (Ref. 21).

103 The success criteria for each safety function for each initiating event group are stated and include minimum equipment requirements and mission times, as well as details of the specific operator actuations required. It should be noted however that several cases have been found in which the starting point for manual action is unclear.

104 The detailed review of a representative subset of analyses supporting the selected success criteria showed no significant errors. The detailed review showed only some discrepancies which appeared to be editorial. Westinghouse's methodology to address the success criteria for long term cooling based on the use of the WCOBRA-TRAC and WGOTHIC computer codes was not reviewed in detail but the application of those codes is considered appropriate. Initial concerns raised by the review team regarding the modelling of water inventories in the containment (allocation, relocation, losses) for recirculation were effectively cleared by Westinghouse's specialists.

105 The systems success criteria are clearly stated in the systems Chapters 8 to 28 of the PSA documentation (Ref. 21).

106 In the cases that could be traced (see discussion on limitations below), the success criteria applied in the PSA model (e.g. the front-line system success criteria) are consistent with those obtained in the task on determination of success criteria.

107 Westinghouse's response to RO-AP1000-099 (SGTR) arrived too late in the GDA process for my assessment team to be able to review it in detail. However, an initial look at it appears to show significantly enhanced traceability between the new SGTR event tree and the supporting success criteria analyses.

4.5.3 Findings

108 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35, 41 and 44.

109 The detailed review of the success criteria for the 6 selected event trees has provided evidence that the original concerns raised in GDA Step 3 were valid. Despite the strengths discussed above, the review found sufficient evidence to conclude that the AP1000 PSA Success Criteria does not meet the expectations for a new reactor in the UK. Key findings are discussed in the following paragraphs. It should be noted that although some specific examples are provided in the discussions below, my review team found that many of the findings were cross-cutting through the IEs reviewed and there was no reason to believe that these would not be equally applicable to the rest of the PSA.

110 Not all the analyses used for derivation of success criteria have been performed on a best-estimate basis. The AP1000 PSA success criteria has been undertaken by examining bounding scenarios for a given category of events and assigning the resulting limiting success criteria to the entire event category. So they are not best estimate throughout. The conservatisms in the PSA are, in principle, considered limitations with a potential to affect the calculated risk profile. However, the extent and impact of the conservatisms in the AP1000 PSA success criteria were not clear at the time of the review.

111 The thermal-hydraulic analyses that support the AP1000 PSA success criteria were not always sufficient or fully representative. For example:

- The PSA event tree for Loss of Main Feedwater is not supported by AP1000-specific calculations for transients. This does not imply that there are no AP1000 calculations for transients; indeed it is believed that AP1000 analyses were undertaken by Westinghouse to support the design of systems such as the Start-up Feedwater and the Passive Residual Heat Removal systems.
- For several sequences thermal-hydraulic analyses are missing (see next paragraph).
- The PSA IE group MLOCA also includes LOCAs in the pressuriser. However, the reviewers could not find specific calculations for pressuriser LOCA in the documentation provided. The reviewers had concerns about this grouping because the thermal-hydraulic behaviour of both events is likely to be different, and the success criteria could therefore be different for both initiating events. This particular concern had also been raised during the review of the identification and grouping of IEs as discussed in Section 4.4.3 above.
- At the time of the review, there were no AP1000-specific calculations to support the event tree for Steam Generator Tube Ruptures. AP1000 SGTR calculations were provided by Westinghouse in GDA Step 4 in response to RO-AP1000-099, as discussed elsewhere in this report.
- There are no AP1000-specific calculations for steam line breaks (SLB) to support the various SLB event trees. Instead thermal-hydraulic analyses for Small LOCA for the AP1000 and / or AP600 analyses for transient initiators are used to support some of the AP1000 SLB event tree sequences. There are concerns about the applicability of these analyses in general, also considering the criticality issues associated with steam line breaks.

112 The way in which the PSA success criteria analyses have been reported (separately for the event tree headings) was addressed in detail during the review. My review team did not find sufficient evidence that the analyses undertaken in this way were sufficient to demonstrate success for each (overall) sequence taking the whole sequence into account. My team found that neither the documentation supporting the PSA, nor the Routemap (Ref. 43) were able to show that fully limiting conditions had been used to justify sequence success. In addition it appeared that there was no analysis available for some success sequences in the event trees. Overall, the review concluded that the lack of traceability and justification of the success criteria along the success paths was an important concern and has led to mismatches between the success criteria analyses and the event tree models. Some examples are as follows:

- The thermal-hydraulic analyses provided are not sufficient to justify that SLOCA success sequence SLO-OK1 as depicted in the PSA is a success path. Similar concerns were raised for other sequences in the SLOCA event tree (SLO-OK4, 8, 12 and 16).
- The review team questioned whether sequence MLO-OK1 is a possible success path for the whole range of Medium LOCAs. Also, manual backup of the Core Make-up Tanks (CMT) is credited in the MLOCA event tree based on the fact that Accumulator injection can support core cooling for 20 minutes, however, in the MLOCA event tree the Accumulators are not called for in the relevant sequences. Similarly, PRHR is credited in the analyses that support the Medium LOCA success sequences MLOCA-OK7 and OK8, however the event tree does not reflect this. Also, MAAP4 analysis shows that steam relief is required in some Medium LOCAs, but the event tree does not reflect this.
- Success sequences SLB-OK3, OK-4, OK5, OK7 and OK8 in the steam line break event tree are not justified by the analyses provided.
- No analyses were found to justify the success sequences ATW-OK2, OK3 and OK4 in the event tree for ATWS following loss of feedwater.

113 A significant number of analyses used for derivation of success criteria have been done for AP600 and applied to AP1000 without visible justification or evidence of applicability (except for four LOCA scenarios). Westinghouse's statements in relation to this, regarding similarity of designs, capability of systems, etc, were noted but not considered sufficient to provide the required evidence of applicability. In fact, the transferability of the thermal-hydraulic calculations from AP600 to AP1000 was questioned by the review in some cases (e.g. SLB and SGTR). Even the comparisons between the AP600 and AP1000 behaviour in four LOCA scenarios showed different performance between AP600 and AP1000 (better) which was not explained. My review raised concerns regarding the applicability of the AP600 analyses for the AP1000 Steam Line Breaks and Steam Generator Tube Ruptures.

114 Timing for operator actions is in general not well justified by sufficient and representative thermal-hydraulic analyses. Justification of operator time windows has only been done for the AP1000 for depressurization cases following two LOCA sizes. The assessment team has identified cases for which the operator time windows are not traceable or not justified. In addition the delineation of time windows was, in general, unclear. For example:

- The time window for automatic depressurisation system (ADS) actuation considered in transient scenarios in the PSA (longer than for SLOCAs) is not justified with AP1000 specific analysis.

- The time window for actuation of the Normal Residual Heat Removal System (RNS) in transient and LOCA sequences is not adequately delineated.
- The time window for manual isolation of containment (which affects the success criteria for recirculation) is not properly justified.
- The time window for ADS actuation in some Small LOCA sequences is not correctly delineated in the documentation provided.
- The basis for the 10 min time window for manual actuation of the main steam isolation valves (MSIVs) from the occurrence of a steam line break was not traceable.

115 The analyses used for derivation of success criteria are not thoroughly documented and fully traceable. Relevant trend plots are presented in support documentation, however the documentation does not provide references between specific calculations (input-output files, parameter files etc.) and the success sequence designators in the event trees. Westinghouse's Routemap (Ref. 43) was an important attempt to establish the traceability but it also proved that full traceability is not completely achievable with the current documentation and showed that lack of traceability is, in particular, a significant concern for the AP600 analyses used to support the AP1000 PSA.

116 Finally, the review team requested Westinghouse to explain how the influence of the physical conditions that arise during the evolution of the sequences on the functionality and operability of the systems and the functions had been taken into consideration in the evaluation of the success criteria for the PSA. For example, how the injection of nitrogen that follows the discharge of the Accumulators had been considered in the success criteria evaluation, or how the influence of the IRWST temperature evolution had been accounted for in sequences with IRWST injection and recirculation. At the time of the review Westinghouse did not produce a convincing answer. This is not to say that the success criteria evaluations fail in this regard, however my review team was not provided with evidence to ascertain that a systematic treatment has been done of the potential influence on the success criteria of the physical conditions that arise in the sequences.

117 The results of the RGA for both success criteria and event trees are discussed in Section 4.6.3 below.

4.5.4 Conclusions

118 The PSA for a new reactor design in the UK should be supported by a fully traceable design specific analysis of sufficient detail and scope. My review has compiled evidence that the success criteria analysis for the AP1000 PSA does not meet these expectations. On the basis of the findings in this area it cannot be concluded that the current prediction of the risk for the AP1000 reported in the PCSR is fully representative. Because of this a GDA Issue has been raised **(GI-AP1000-PSA-01)**. The complete GDA Issue and associated actions are formally defined in Annex 2.

119 I should also indicate that it is my judgement that any further work on PSA success criteria will be incomplete and inadequate if it is based on the current incomplete list of IEs. Therefore, Westinghouse needs to address the findings from the reviews of the AP1000 identification and grouping of IEs and internal flooding to effectively respond to the GDA Issue on "Success Criteria". This has been captured in a GDA Issue Action **(GI-AP1000-PSA.01.03)**.

4.6 Level 1 PSA: Accident Sequence Development – Event Sequence Modelling (A1-2.3)

4.6.1 Assessment

120 A high level review of the AP1000 PSA task on "Event Sequence Modelling" (Event Trees) against the expectations in T/AST/030 (Table A1-2.3) was conducted during GDA Step 3. My review found that in general the AP1000 event trees structure looked reasonable however it also raised specific concerns in the following areas:

- Missing links between the accident sequences delineated in the PSA and the procedures used by the operators during the course of an accident.
- Lack of treatment of dependencies between initiating events and mitigating systems due to failures of digital systems.
- Incomplete treatment of late containment failure sequences caused by failure of containment heat removal.

121 The objective of my GDA Step 4 PSA assessment was to undertake a detailed review (on a sampling basis) of all the PSA technical areas in order to confirm or otherwise the findings during my GDA Step 3 assessment. For the assessment of the AP1000 PSA event trees my team selected the same Initiating Event Groups as for the assessment of the PSA Success Criteria with the aim of conducting both reviews with a high degree of coordination. The event tees selected were:

- Small LOCA.
- Loss of Main Feedwater.
- Steam Generator Tube Rupture.
- Medium LOCA.
- ATWS without Main Feedwater.
- Steamline Break Upstream of the MSIVs.

122 The above selection provided a good representation of all the types of Initiating Events (LOCA, transient, secondary side faults, primary to secondary leakage, reactivity transients) and ensured that the review addressed the various aspects related to the evolution of accident sequences in a comprehensive manner. Furthermore, the previous experience of my review team suggested that some of these events, in particular steam line breaks and SGTR, were event trees in which modelling problems tended to be more common.

123 Although a detailed review of one of the ATWS event trees was conducted, I decided not to follow that up with formal TQs / ROs. This is because Westinghouse was at the time doing new ATWS analyses and the relevant PSA models might change considerably as a result of these. However, the initial review of the event tree for "ATWS without Main Feedwater", which identified a number of shortcomings, was provided to Westinghouse with the expectation that the information and comments included in the review should be taken on board when revising the ATWS event tree models (Ref. 44) – this is captured in the table of findings (Annex 1). The information was also provided to ND's Human Factors assessment team because my team considered that the chain/s of Human Failure Events in ATWS sequences and the dependencies between them should be reviewed in detail by human factors specialists.

124 My GDA Step 4 review of the PSA accident sequence development task identified that the event tree for "Steam Generator Tube Rupture" was inconsistent with the strategy to deal with an AP1000 SGTR according to the relevant Emergency Operating Procedure (EOP). This was later reinforced when attending an SGTR simulation in the AP1000 simulator. This inconsistency, the numerous additional concerns raised by my team during the detailed review of the SGTR success criteria and event tree, and the high significance of this initiating event to the overall AP1000 risk, were the reasons why in September 2010 I issued RO-AP1000-099 requesting Westinghouse to provide a revised and documented SGTR event tree.

125 A Risk Gap Analysis was performed to address the findings in this area and to understand their potential risk significance. As already discussed in Section 4.5.1 above, the limited scope RGA to address success criteria was combined with the event tree RGA because of the similar nature and consistency of some of the findings from both reviews. An initial screening of findings was conducted using qualitative arguments and applicable quantitative information from the PSA. This resulted in a list of those shortcomings which were judged to have a non-negligible numerical risk impact and were therefore selected for further evaluation as follows:

- Some modifications to the model and data stemming from the findings in these areas were implemented in the Base-case (BC) RGA Model (discussed in Section 2.3.2 above), or added to the results obtained from the quantification of the BC RGA Model. For example:
    - Modification of some Human Error Probabilities to account for reduced time windows.
    - Modification of the CAFTA quantification rules to account for missing human dependencies and missing cognitive Human Failure Events (HFE).
    - Modification of the reactor trip fault tree model to account for mechanical failure of the control rods to insert.
    - Modification of the top-logic fault tree to add sequences with failure of containment heat removal.
    - Addition of contributions to the baseline CDF and LRF to account for failures of pressuriser relief valves to open when challenged.
- I considered that there was a need to address the finding regarding lack of consideration of dependencies between initiating events and mitigating systems due to failures of digital systems. In this regard, my team conducted a study of the dependencies that we considered would have the highest safety significance, i.e. those failures of the Protection and Safety Monitoring System (PMS) that could lead both to initiating events as well as failure or degradation of the mitigation systems. In particular, spurious actuations of the PMS accompanied by freezing of the actuation signal to the mitigation systems were addressed. In addition, sensitivity analyses were performed by my team to understand the potential impact of dependencies between failures of the Plant Control System (PLS) that cause initiating events and degradation of relevant mitigation systems.
- Individual analyses were conducted to address the sensitivity of the risk to the following items:
    - Probability of induced SGTR.

  - Human Error Probability (HEP) of the operator action to control PRHR in some steam line break sequences, if such action was not supported by procedures.
  - Failure to trip of the main turbine following reactor trip (currently not considered in the model).

- In these two areas of the review (success criteria and event trees) numerous items originally screened in could not be analysed quantitatively either because the lack of information about the evolution of the sequences would preclude a meaningful RGA, or because addressing them would have required significant modelling effort well beyond the available resources. The limitations in the AP1000 success criteria supporting analyses (discussed in Section 4.5 above) and the fact that the AP1000 PSA model does not have event trees and fault trees linked, were the main reasons why a number of screened-in items could not be evaluated in RGA. Examples of these were:
  - Fault tree logic of ADS headings.
  - Screening criteria for containment isolation.
  - Modelling of steam line break sequences requiring containment heat removal.
  - Possible return to power in some steam line break sequences and associated requirement for shutdown control.
  - Impact of insertion of nitrogen from the Accumulators.
  - Requirements for Accumulator injection in some SLOCA sequences.
  - Special treatment of sequences with steam line break and induced SGTR.
  - Time windows for operator actions taking into account the evolution of each individual sequence.

  It should be noted that most of the above findings not addressed by the RGA should be resolved in response to the GDA Issue on “Success Criteria” (Section 4.5 above)
- Findings raised during the review of the SGTR event tree were not addressed in the event tree RGA. Instead, as indicated above, RO-AP1000-099 was raised for Westinghouse to develop a new SGTR event tree representative of the AP1000.

4.6.2 Strengths

126 My review team found that, at a high level, the AP1000 event trees (except for SGTR) provided a good representation of the potential accident sequences for the AP1000.

127 Furthermore, it was concluded that a number of the TAG requirements were fulfilled by the accident sequence analysis carried out by Westinghouse.

128 Westinghouse’s response to RO-AP1000-099 (SGTR) arrived too late in the GDA process for my team to be able to review it in detail. However, an initial look at it appears to show a significantly improved SGTR event tree which is traceable to the relevant EOPs and to the supporting success criteria analyses.

4.6.3 Findings

129 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35, 44 and 46.

130 A general problem observed in the success criteria (Section 4.5 above) was the difficulty of identifying specific justifying analyses for success criteria and operator action timings. The review of the event sequence models consistently highlighted the same type of problems. For example, in response to some queries raised during the review of the event trees, Westinghouse was unable to provide specific analyses to justify the time windows applied for several operator actions. Also, regarding reactivity control requirements following a steam line break, Westinghouse stated that the PSA had used more relaxed assumptions than those obtained from the Design Control Document (DCD), but failed to provide a reference to a calculation justifying the more relaxed assumptions. Finally, as already discussed extensively in Section 4.5 above, clear links between headings in the event trees and specific relevant thermal-hydraulic analyses are missing from the PSA documentation.

> ***Assessment Finding AF-AP1000-PSA-015:*** *The Licensee shall provide revised documentation of the PSA Event Sequence Modelling presenting justification and full traceability between all aspects of the event sequence models and the supporting analyses.*

131 Another general concern was the scattering through several chapters of the PSA report (Ref. 21) of the documentation and justification of general assumptions used in the event tree modelling.

> ***Assessment Finding AF-AP1000-PSA-016:*** *The Licensee shall provide revised documentation of the PSA Event Sequence Modelling including a collated and clear description of general assumptions used.*

132 Table A1-2.3.2 of ND's PSA TAG (Ref. 15) expects that the dependencies (human actions, equipment, environmental, spatial, common mode failure, fluid medium), including subtle dependencies, should be identified and treated correctly. Specific examples of findings in this regard are:

- There was no task documented in the PSA to identify dependencies (spatial, environmental, subtle, etc).
- The review of the Identification and Grouping of IEs (Section 4.4 above) identified potentially significant initiating events with dependent environmental impacts which have not been considered in the current PSA (e.g. loss of HVAC).
- The review of the Internal Flooding PSA (Section 4.12 below) identified potentially significant spatial impacts from steam line breaks leading to scenarios which have not been considered in the current PSA.
- Dependencies between initiating events and mitigating systems due to failures of digital systems have not been considered in the current PSA.
- Lack of treatment in the PSA of the possibility of an impact of RCS shrinkage on PRHR operability following a steam line break or, alternatively, weak justification for not modelling this potential dependency.

> ***Assessment Finding AF-AP1000-PSA-017:*** *The Licensee shall provide revised documentation of the PSA Event Sequence Modelling including a complete and clear description of the treatment of dependencies. The Licensee shall provide revised AP1000 PSA event sequence models, as appropriate, with correct treatment of dependencies.*

133 Concerns were raised regarding the missing links between event tree headings and operating and emergency procedures (either existing procedures or assumptions about

potential operating / emergency procedures to be developed). In particular, the basis for the modelled mitigation actions was not clear in general. Chapter 30 of the PSA (Ref. 21) on HRA explains that the AP1000 PSA models the same human actions as the AP600 PSA. Given this statement, there is not confidence that the current AP1000 operating procedures at the time of GDA are represented in the AP1000 PSA. The following two examples illustrate this concern:

- The Steam Line Break model includes an operator action to control PRHR cooling, allow primary temperature to increase, and thereby reduce core power; the review asked a specific question about this action. While Westinghouse's response to this query referred to procedures E0 and E1 (in a general way) it was noted that the documentation of Chapter 30 of Ref. 21 does neither identify these procedures nor the specific steps that would lead the operators to manually control PRHR.
- As indicated in Section 4.6.1 above, the review identified that the event tree for "Steam Generator Tube Rupture" in Ref. 21 was inconsistent with the strategy to deal with an AP1000 SGTR according to the relevant Emergency Operating Procedure (EOP).

Assessment Finding AF-AP1000-PSA-018: *The Licensee shall provide revised documentation of the PSA Event Sequence Modelling showing clear links between all aspects of the event sequence models and relevant operating and emergency procedures.*

134 Although end states representing consequential initiators are represented and carried through the event tree models, my team identified specific cases of concern about the detailed adequacy of treatment or absence of some consequential events. Examples of these are:

- The consequences of failure of pressuriser safety valves to open when challenged are not modelled in the PSA.
- The consequences of failure of steam relief valves to open when challenged are not modelled in the PSA.
- Loss of off-site power following any IE is not modelled in the PSA.
- Treatment of stuck open secondary side safety valves together with steam line break upstream of the MSIVs outside containment.
- Use of an old reference for evaluating the probability of induced SGTR following steam line break.

Assessment Finding AF-AP1000-PSA-019: *The Licensee shall provide revised and documented PSA event sequence models including adequate treatment of consequential events.*

135 The review raised queries regarding the correctness of the functional fault tree models supporting the event trees. A brief summary of some key findings is given below:

- There was a concern that the combined solution of top events for failure of partial and full ADS in the same sequence did not generate correct cutsets. It was noted that the modelling applied in the PSA appeared to be conservative for some sequences, although it was inconsistent with respect to others and in any case the logic of one of the fault trees representing partial depressurisation was incorrect.
- Some inconsistencies and apparent errors were identified in the fault trees developed for the CHR (Containment Heat Removal) heading. For example it was unclear

whether, for one of the long term cooling configurations considered in the PSA involving pumped flow through the normal RHR system, the operator would need to throttle RNS flow to maintain adequate suction if both RNS pumps were running aligned to IRWST. Also, the lack of modelling of failures of the gutter drain valves in one of the containment heat removal fault trees appeared to be incorrect. It should be however noted that in practical terms the CHR heading is not used in the PSA for the evaluation of the CDF. This in itself is a separate finding discussed below.

- The event tree models for transient initiators do not account for failures of secondary steam relief if the main condenser is not available (i.e. failure to open a sufficient number of main steam safety / relief valves on a steam generator that is being fed by SFW).
- Some causes of failure of secondary side steam relief as well as some causes of uncontrolled secondary side depressurisation were missing from the fault tree used for the event tree heading modelling "No Stuck-Open Main Steam Line Safety Valve". The fault tree incorrectly reflects the number of turbine bypass valves and condenser circulating water pumps in the UK AP1000 design. The fault tree should also include relevant failures of the condenser vacuum pumps.
- The models for secondary heat removal appear to neglect the requirement to trip at least 3 RCPs in order to prevent a more rapid depletion of condensate storage tank water.
- Some failures of PRHR valves for regulating PRHR flow (if required) after steam line break in order to maintain reactivity control appear to be missing.
- The fault trees representing failure of containment isolation have been developed based on screening criteria for penetrations that have been questioned in the review (see also discussion in Section 4.18 below). In addition Westinghouse acknowledged that some valve failures have been wrongly omitted from the fault tree model.
- The wrong fault tree was used for the sump recirculation heading in some SLOCA sequences with failure of CMT (although it appears that this particular error would not affect the results).
- Mechanical failures that may prevent insertion of the control rods are not modelled. The justification for this was considered weak.

Assessment Finding AF-AP1000-PSA-020: *The Licensee shall provide revised and documented PSA event sequence heading models (functional fault trees) addressing all the errors and inconsistencies identified in the GDA review and ensuring that all the PSA heading models that could be affected (as well as those reviewed during GDA) are also revised.*

136 My review raised some queries regarding the correct construction of event trees. Some example concerns arising from the review are listed below:

- Accumulator injection is missing from the event tree models for some Small LOCA sequences with successful PRHR and failed CMTs.
- The requirement for containment heat removal (PCS) to operate following some steam line break sequences is missing.
- Lack of justification for modelling assumptions of sequences with potential return to power after steam line break and heat removal via PRHR.

Assessment Finding AF-AP1000-PSA-021: *The Licensee shall provide revised and documented PSA event trees addressing all the errors and inconsistencies identified in the GDA review and ensuring that all the PSA event trees that could be affected (as well as those reviewed during GDA) are also revised.*

137 My review noted that late containment failure sequences caused by failure of containment heat removal were not added to the core damage frequency. This topic is discussed in more detail in the review of the Level 2 PSA (Section 4.18 below), since the overall concern was addressed from the global point of view of the impact on the large release frequency (LRF). The conclusion of my review was that in sequences which rely on air cooling to remove heat from the containment, the containment pressurisation is expected to be sufficient to generate a possible challenge to the containment integrity, and hence a contribution to both CDF and LRF is expected from these cases. Westinghouse has indicated that the risk impact should be small because of the reliability of the containment cooling system; although this may be so, I do not consider this to be a justification for not treating these sequences in the PSA in a rigorous manner.

Assessment Finding AF-AP1000-PSA-022: *The Licensee shall provide revised PSA event trees where the Late Containment Failure sequences are treated as core damage sequences and are transferred to the Level 2 PSA.*

138 In addition to the above, the following should be noted:

- Additional specific and detailed shortcomings were raised formally via TQs.
- In response to TQs and ROs raised in this area Westinghouse made some commitments to address identified shortcomings.
- Westinghouse provided relevant technical information in response to TQs and ROs that I raised in relation to Event Sequence Modelling and Success Criteria, which should be formally included in the PSA documentation.
- Additional specific and detailed shortcomings were identified by the TSCs during the reviews of the Event Sequence Modelling and Success Criteria for ATWS without Main Feedwater. These are documented in the form of Proposed Technical Queries (PTQ) in Refs 41 and 44. Although at the time of the review I decided not to formally issue them as TQs or ROs, they should be taken into consideration in a future update of the PSA.

Assessment Finding AF-AP1000-PSA-023: *The Licensee shall provide revised and documented PSA event trees taking into account 1) specific shortcomings identified in TQs raised in this area; 2) shortcomings relevant to the sequence modelling identified in TQs related to PSA success criteria, 3) commitments made by Westinghouse in the TQ responses; and 4) relevant technical information provided in response to the TQs and ROs. Relevant TQs and ROs in this area are: TQ-AP1000-348, 351, 352, 433, 517, 572 to 582, 584 to 589, 863 to 876, 880 to 898, 914 to 924, 1006 to 1008, 1012 to 1015, 1020, 1025 to 1027, RO-AP1000-072 and RO-AP1000-099.*

Assessment Finding AF-AP1000-PSA-024: *The Licensee shall provide revised and documented PSA event trees for ATWS Initiating Events taking into account specific shortcomings identified by the TSCs during the reviews of the AP1000 PSA Event Sequence Modelling and Success Criteria. These are documented in Ref. 44, PTQ-AP1000-AS-38 to 49, and in Ref. 41, Part-2-PTQs 73 to 95.*

139 The limited RGA conducted for the success criteria and event trees has shown that numerical risk gaps could be associated with the following findings:

- Failure to open of the pressuriser safety valves when challenged is not explicitly modelled in the event trees but it is assumed successful in the success criteria analyses. Westinghouse has indicated in their response to a query in this regard that this scenario could have various possible Reactor Coolant System (RCS) responses, including a LOCA that cannot be compensated (direct core damage). Therefore, further analysis and correct modelling of these sequences in the PSA is warranted.
- Containment heat removal is required in the long term to keep the reactor cooled in sequences with depressurisation, IRWST injection and recirculation. These sequences are currently assigned to a consequence called Late Containment Failure (LCF) and are not taken forward as core damage or through the Level 2 PSA. Including these sequences as core damage would have a small impact on the CDF but a measurable impact on the LRF.
- Mechanical failure of the control rods to insert is currently not modelled in the PSA. Inclusion of this failure could have a measurable impact on the CDF and LRF.
- The models do not account for dependencies between initiating events caused by spurious PMS actuations and the mitigation systems actuated by PMS. Explicitly accounting for these dependencies could have a measurable risk impact.
- The LRF is sensitive to the probability assigned to the occurrence of consequential SGTR following steam line break. The method used to evaluate this probability for the AP1000 has been questioned by my review team because it does not use the more accurate modern approaches.
- In addition to the above, the new SGTR analysis conducted by Westinghouse in response to RO-AP1000-099 has shown an increase in the CDF associated with SGTR (of approximately a factor of 3) and a 35% increase in the total LRF (associated with internal initiating events during operation at power). The observed risk increase appeared to be due to the following: 1) AP1000 specific success criteria were used; 2) the event tree was modified to reflect the strategy to deal with SGTR in an AP1000; and 3) other review findings were addressed.

4.6.4 Conclusions

140 Based on the outcome of this assessment, I have concluded that, providing the resolution of the GDA Issue on “Success Criteria” (discussed in Section 4.5) does not lead to significant alterations in the current event trees, these are sufficient to support the AP1000 “generic” PCSR PSA. This conclusion is also supported by the limited RGA conducted in this area of the PSA which has allowed an initial understanding of the potential impact of the limitations found in the event trees.

141 In any case, this part of the AP1000 PSA needs improvements to support further stages of the NPP development, i.e. improvements in the event tree models should be undertaken as part of the next update of the PSA (see Section 5 below).

4.7 Level 1 PSA: System Analysis (A1-2.4)

4.7.1 Assessment

142 I conducted a high level review of the AP1000 PSA task on "Systems Analysis" (Fault Trees) against the expectations in T/AST/030 (Table A1-2.4) during GDA Step 3. My review raised general concerns regarding completeness of the system fault tree models and on how the models had been built. To address these concerns I raised a Regulatory Observation (RO-AP1000-045) and a number of TQs.

143 My detailed review of System Analysis element of the AP1000 PSA in GDA Step 4 has been performed following on from the review I conducted in GDA Step 3 by looking at the application of the methods and techniques used in the specific PSA task to several example systems. The systems selected for detailed review were:

- Passive Cooling System (PXS): Passive Residual Heat Removal System (PRHR), Core Make-up Tanks (CMT), Accumulators, Automatic Depressurization System (ADS), In-containment Refuelling Water Storage Tank (IRWST) and Passive Containments Cooling System (PCS).
- Start-up Feed Water System (SFW).
- Alternating Current (AC) Electrical Power.
- Component Cooling Water System (CCS) and Service Water System (SWS).
- Control and Instrumentation (C&I): Protection and Safety Monitoring System (PMS), Diverse Actuation System (DAS) and Plant Control System (PLS).

144 The above selection provided a good representation of all the types of systems and components in an AP1000 reactor and would ensure that the review would cover the various aspects of system performance modelled in the PSA in a comprehensive manner.

145 In addition to the above, the Containment Isolation System and the Hydrogen Igniters System models were reviewed in the framework of the Level 2 PSA assessment. The result of these reviews is reported in the Level 2 PSA Section 4.18 below.

146 A Risk Gap Analysis was performed to address the findings in this area and to understand their potential risk significance. An initial screening of findings was conducted using qualitative arguments and applicable quantitative information from the PSA. This resulted in a list of those findings from the review of the systems fault trees which were judged to have a non-negligible numerical risk impact. These were subject to further quantitative evaluation as follows:

- Modifications to the model and data stemming from the findings in this area were implemented in the Base-case (BC) RGA Model (discussed in Section 2.3.2 above). For example:
    - Fault trees were modified to explicitly include missing events perceived to be important (e.g. pre-initiating event human errors also called Type A HFEs, Common Cause Failures, IRWST tank failures). The Type A HFEs included in the fault trees were selected among those identified by Westinghouse in their Human Factors submission (Ref. 47), based on risk significance of surrogate events already modelled in the fault trees. Also, in the RGA probabilities for the Type A HFEs calculated by Westinghouse have been used (see Section 4.8 below).
    - Probabilities of events considered to be appropriate surrogates were modified to implicitly account for missing events (e.g. the probability of the module

event representing failures of sump recirculation lines were increased to account for the possible HFEs associated with the Motor Operated Valves MOVs 117A and B).

- The CAFTA recovery rule file used for the quantification of the PSA was modified to account for missing events representing cognitive human errors.
- The error found in the fault tree for sump recirculation was amended.

- A separate sensitivity analysis was carried out to explore the current omission of consequential LOOP following any initiating event. This was done by modifying the corresponding AC Power fault trees.
- In addition, during the "PSA Convergence Meeting" held in October 2010, Westinghouse was requested to evaluate the numerical significance of the errors found during the review of the PSA model (fault trees), including confirmation of whether the errors were systematic and affected other parts of the model not covered in my GDA Step 4 review. A table with the specific details of the errors found during the review was provided to Westinghouse. Westinghouse undertook to do this work but with a limited scope because addressing some of the items might have required significant modelling effort not possible within the available time.

4.7.2 Strengths

147 The PSA system models have been built in the fault tree software CAFTA developed by the Electric Power Research Institute (EPRI). CAFTA is well known and widely used worldwide. The CAFTA 3B PSA model (Ref. 25) is composed of fault trees that are integrated and linked throughout (except for the fault tree models developed to support IE frequency calculation). Dependencies on support systems are modelled explicitly and in detail.

148 Each of the sub-systems that in combination make up the Passive Core Cooling System (PXS) has been modelled using detailed fault trees. The electrical and C&I dependencies have been included. The system descriptions are detailed, including top event success criteria and tables of Common Cause Failures (CCF), Human Failure Events (HFE) and Test Intervals. Unavailabilities due to testing and maintenance have also been included in the system models.

149 The models for the PMS and PLS have been developed to a level of detail which is unusual at the PCSR stage and considering the current status of the systems designs. Despite the limitations in these models discussed below, the high level of detail is considered a strength of the analysis and a demonstration that detailed fault trees for the C&I systems are feasible. This has helped to better establish the link between the C&I engineering and the risk of the facility at this early stage. It has also helped to establish early the interactions between Westinghouse's PSA and C&I teams which are considered key by ND.

4.7.3 Findings

150 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35, 48 and 49.

151 My high level review of the AP1000 PSA task on "Systems Analysis" (Fault Trees) conducted during GDA Step 3 raised general and methodological concerns regarding this aspect of the PSA. These are not discussed in detail here (see instead Ref. 6). My

review of Westinghouse's response to RO-AP1000-045 and my detailed review of the models for a selection of systems conducted in GDA Step 4 have provided evidence that the methodological concerns raised earlier were valid. These are captured in the following two assessment findings:

> ***Assessment Finding AF-AP1000-PSA-025:*** *The Licensee shall provide revised PSA Systems Analysis documentation including the following: system boundaries and interfaces, component boundaries, FMEAs, complete dependency matrices, details of system testing and maintenance.*
>
> ***Assessment Finding AF-AP1000-PSA-026:*** *The Licensee shall provide revised systems fault trees consistent with the UK-AP1000 design and including complete modelling of failures (pre-accident human errors, structural failures, passive failures, indication failures, unavailabilities due to testing and maintenance, common cause failures), and removal of modular events, unnecessary simplifications and asymmetries.*

152 The review of the PSA models for the Passive Core Cooling System/s has raised a number of concerns of different nature, one of the key ones being related to the adequacy of the CCF modelling in the fault trees. The main limitations identified are discussed below:

- The CCF modelling has been found inadequate to represent the plant in all operating configurations. For example, within the Passive Core Cooling System, several cases arise where the CCF is considered to be underestimated due to not considering reduced system availability following some initiating events such as Direct Vessel Injection Line Break.
- The CCF analysis omitted some possible combinations of failures of components in redundant trains. For example, the fault tree for the Accumulator does not include all the possible common cause failures between the Non-return Valves (NRV) in both trains. Other examples of missing CCF combinations are related to the Motor Operated Valves (MOV) in ADS Stage 1 to 3, and ADS Stage 4 Squib valves.
- The review found incompleteness in CCF modelling of valves that use the same functional means of operation such as the Recirculation Squib Valves. In this particular case, my team in discussions with ND's mechanical engineering assessment team considered that Westinghouse's claims of diversity between the high pressure and low-pressure squib valves in the recirculation lines are insufficient to justify not modelling CCFs.
- At the end of my GDA Step 4 assessment there was still an unresolved question regarding the potential for CCF between the Air Operated Valves (AOV) in the PRHR and CMTs. The relevant inter-system CCFs have not been included in the model. Westinghouse has indicated that the AOVs in both systems have completely different size, design, etc. However, my team believes that there could be coupling factors present other than design leading to CCF (e.g. operating regime, maintenance, etc). The justification for excluding CCFs should be strong and cover all coupling mechanisms and defences in place against these.
- The AOVs in the CMT open automatically on actuation signals from the PMS to an air solenoid valve associated with each AOV. The CMT and PRHR AOVs can also be opened through actuation signals from the DAS to air solenoid valves in the compressed and instrument air system (CAS). The CMT DAS air solenoid valve vents the air from all four of the CMT AOVs. The air solenoid valves actuated by DAS

have not been included explicitly in the models, which we consider to be incorrect. In addition, the potential for CCF between the solenoid valves actuated by PMS and DAS has not been considered. Similar concerns apply to the models of the PRHR and IRWST Gutter Drain Isolation valves.

- No evidence has been found to justify current omissions of pre-accident human errors such as misalignments, also called Type A HFEs, and passive failures in the models for the Passive Cooling Systems. In GDA Step 4 specific examples have been identified which are potentially of high safety significance, these are latent failures (valves have been left closed or closed de-energised) and / or passive failures (internal catastrophic failure or spurious closure) of valves in PRHR, CMT, Accumulator, IRWST Injection and Recirculation and ADS. Omissions of this nature will almost certainly impair the adequacy of the PSA to support decision-making and, therefore, not modelling those failure modes has to be supported by robust justifications.
- The failures leading to loss of IRWST inventory have been the subject of extensive discussions between my team and Westinghouse. Failures leading to loss of IRWST inventory are currently modelled as a failure of the PRHR only. However it is not clear why the IRWST failure modes should not be modelled also under the IRWST Injection / Recirculation fault trees. Leakages and other IRWST failures would bring the time to recirculation forward but there is no analysis to justify that this is a success sequence for all initiating events. Westinghouse needs to provide further analysis to justify the current model or alternatively they need to complete the model by including the missing failures as appropriate.
- The model exclude all failures associated with the mechanisms to ensure that there is sufficient nitrogen pressure in the Accumulators at all times e.g. drifting or wrong calibration of Accumulator pressure instruments. This is considered incorrect.

Assessment Finding AF-AP1000-PSA-027: *The Licensee shall provide revised and documented PSA fault trees for the Passive Cooling Systems taking into account the shortcomings identified by the GDA review.*

153 The review of the PSA models for the Start-up Feedwater System (SFW) has raised a number of concerns of a different nature. The main limitations identified are discussed below:

- The SFW provides feedwater for decay heat removal following loss of main feedwater. This also requires steam removal from the steam generator which is being supplied with feedwater. The fault tree does not model steam relief and in the PSA documentation there is no discussion or justification for omitting the steam relief path.
- The models include credit for SFW suction from the condensate storage tank (CST) without the need to top it up. Also the failure probability used for the CST (based on 24hr mission) assumes that at the time of the initiating event there is sufficient water for 24 hrs in all conditions. Westinghouse has not provided evidence on how sufficiency of CST water has been determined for all IEs and all sequences (including in the presence of undetected leaks). In fact, information provided by Westinghouse indicates that, following a LMFW event, operation beyond eight hours with four Reactor Coolant Pumps (RCP) in service would result in a loss of CST capability before the Normal Residual Heat Removal System (RNS) function is available. This is not reflected in the PSA model.

- If one SFW pump fails to start then there is the potential for loss of flow if the NRV in the discharge of the failed pump fails to close against the returning flow from the healthy pump. This is not modelled in the fault tree.
- Errors were found in some parts of the SFW fault tree. For example, the fault tree gates modelling failure of (automatic and manual) start of the SFW pumps have the same inputs from the PLS, which seems to imply that if the automatic initiation fails (due to the signal), so does the manual, which seems incorrect. Also, the model for the failure to regulate flow is incomplete and / or incorrect. Finally, there are some unexplained and apparently inconsistent PMS failures in the SFW model (believed to refer to the PLS-PMS interface). At the time of the review Westinghouse was unable to explain the inconsistencies found in this part of the model.

Assessment Finding AF-AP1000-PSA-028: *The Licensee shall provide revised documented PSA Fault Trees for the Start-up Feedwater System taking into account the shortcomings identified by the GDA review.*

154 In relation to the AC Power System and Diesel Generators (DG), the review team raised the following concerns:

- The electrical systems selected for the Step 4 detailed review are among those originally classified by Westinghouse as non-Class 1E systems despite the fact that they support safety functions post reactor trip. As such it is not clear how the data used for the reliability of electrical components has been derived to reflect this considering that most data sources, which are based on operating experience of electrical systems supporting post trip cooling and long term heat removal, will only include data for Class 1E components. This is discussed further in the section on reliability data (below).
- The 2.5 hrs Mission Time for the DGs is not justifiable for LOOP events caused by failures non-recoverable in 2.5 hrs. The PSA needs to correctly and explicitly model the events related to losses of power supply. Indeed Westinghouse has agreed that the modelling of LOOP in the PSA is not complete and needs reviewing. This is also the case for the (failure of the) AP1000 load rejection capability which has not been modelled explicitly. Implicitly, it has been considered as fully reliable in some parts of the model, or has not been given credit in some others.
- Some other inconsistencies were found in the model that could not be explained or justified by Westinghouse at the time of the review. For example, the model appeared to double count DG failure probabilities by modelling DG auxiliary systems both implicitly (within the component boundary) and explicitly; the model for the control power supplies for the DGs is asymmetric and my review team believed that this was incorrect; the failure probability of the breakers that have to open to shed loads for DG operation have been calculated on the basis of a 24hr mission time instead of considering their test intervals (during outages), which leads to a significant underestimation of the probability; finally, CCF of the two Auxiliary Transformers was not included in the model but should be.

Assessment Finding AF-AP1000-PSA-029: *The Licensee shall provide revised documented PSA Fault Trees for the AC Power System and Diesel Generators taking into account the shortcomings identified by the GDA review.*

155 In relation to the Component Cooling Water System (CCS) and the Service Water System (SWS), my review team raised the following concerns:

- The drawing for the CCS in the PSA documentation (Ref. 21) and in the Piping and Instrumentation Diagram (P&ID) provided by Westinghouse to support the PSA review (Ref. 50) are totally different to the system diagram shown in the European DCD Rev 1 (Ref. 51). This is because the PSA has not been updated yet to reflect the UK design changes for the CCS / SWS. The problem for the PSA review in GDA is the lack of confidence that the AP1000 PSA reviewed is a good representation of the design that other inspectors in other technical areas have assessed in GDA. Although, in this particular case, one would expect that the design improvements would lead to lower failure probability for this system, it has not been feasible to ascertain this via a risk gap evaluation within GDA timescales.
- The boundary of the CCS defined to underpin the PSA model is not described in the PSA documentation. This was a generic finding already identified in GDA Step 3. The reason why it is highlighted here is because this finding is of particular concern for the CCS which has interfaces with a number of other systems in the plant. Because of this limitation and the extensive use of modular components without specific component identifiers (another generic finding identified in GDA Step 3), the review could not ascertain whether there are missing failures in the fault tree, some of which could even be single failures for this system.
- Errors were found in some parts of the CCS and SWS fault trees. For example, the fault tree gates modelling failure of (automatic and manual) start of the CCS pump B have the same inputs from the PLS, which seems to imply that if the automatic initiation fails (due to the signal), so does the manual, which seems incorrect; The fault tree or the SWS erroneously includes a HFE belonging to the Start-up Feedwater system instead; Failures of the surge tanks are missing from the model. Inconsistencies were found in the modelling of the CCS heat exchangers and their assigned failure probabilities are questionable.

  Assessment Finding AF-AP1000-PSA-030: *The Licensee shall provide revised documented PSA Fault Trees for the Component Cooling Water (CCS) and Service Water (SWS) Systems taking into account the shortcomings identified by the GDA review.*

156 The review of the fault tree models for the C&I systems (PMS, DAS and PLS) could not establish whether the PSA models for these systems were a good representation of the status of the PMS, PLS and DAS designs reviewed in GDA by the C&I team. In fact, inconsistencies were found between the PMS and DAS PSA models and the design documentation provided. This is not considered a limitation of the PSA review itself. Indeed, Westinghouse's responses to the TQs raised in this area accept that the findings from my review are valid and will be taken into consideration as appropriate for future model developments. The main limitations identified during the review of the fault trees for the C&I are as follows:

- The modelling of sensors is inconsistent and incomplete throughout the C&I PSA models. Some inconsistencies found may lead to cutsets that contain combinations of events with different names which however correspond to the same sensors. It seems that specific design details on sensors-component actuation was not available at the time of the model development which may justify the incompleteness of the modelling of sensors, but not the model inconsistencies found.
- The PMS dependency on cabinet cooling has not been considered in the model, which is inconsistent with the documentation. In general HVAC failures should be included in the C&I fault trees as appropriate.

- The early stage of the design of the DAS at the time of the model development is shown in a fault tree model that reflects the concept rather than the engineering. In this regard the model for the DAS will need to be fully developed in the future. It should also be noted that the DAS has been redesigned during GDA but this is not discussed here.
- The PLS model does not reflect in detail its interface with the PMS. This has led to unexplained inconsistencies in the model and a potential gap in the modelling of dependencies.
- Some errors were found in the PSA models for the C&I. For example the modelling of the reactor trip breakers is inconsistent resulting in wrong cutsets; incorrect cutsets are also obtained from the fault tree model for the Local Coincident Logics (LCL); the reactor trip function shares Bistable Processor and Logic (BPL) and LCL hardware and logic with other PMS functions, but this has not been modelled explicitly which leads to missing dependencies; the models for the failures of the signals to open the recirculation squib valves are incorrect; the PSA model erroneously combines under "and" gates CCFs of instrumentation sensors and switches.
- Some other inconsistencies were found, for example, the steam generators are referred to inconsistently in the model which could have led to including in the model basic events with different names representing the same failure modes; in the SFW fault tree, sensor instrument line failures are modelled inconsistently in the two trains and are assigned inconsistent failure probabilities; failures of Component Interface Modules (CIM) have been included inconsistently in the SFW fault trees. The cognitive HFEs between PMS and DAS common functions are missing from the DAS model.
- Finally, some inconsistencies between the fault tree model and the design documentation were identified which were not explained at the time of the review. For example, it was not clear how the reactor trip via DAS is produced, i.e. whether DAS trips the reactor, in which case the PSA model would be inaccurate, or the turbine, in which case there would be failures missing from the reactor trip model (reflecting the means by which Turbine Trip trips the reactor). The gate described as "permissive on power > 70% failure" currently included in the DAS fault tree, appears to be irrelevant for reactor trip according to the design documentation. All this needs to be confirmed and the model corrected as / if appropriate.

  Assessment Finding AF-AP1000-PSA-031: *The Licensee shall provide revised documented PSA Fault Trees for the Protection and Safety Monitoring System (PMS), Plant Control System (PLS) and Diverse Actuation System (DAS) taking into account the shortcomings identified by the GDA review.*

157 In addition to the above, the following should be noted:

- Additional specific and detailed shortcomings were raised formally via TQs.
- In response to TQs and the RO raised in this area Westinghouse made some commitments to address identified shortcomings.
- Westinghouse provided relevant technical information in response to TQs that I raised in relation to Systems Analysis (Fault Trees), which should be formally included in the PSA documentation.

  Assessment Finding AF-AP1000-PSA-032: *The Licensee shall provide revised documented PSA Fault Trees taking into account 1) specific shortcomings identified*

in TQs raised in this area; 2) commitments made by Westinghouse in the TQ and RO responses; and 3) relevant technical information provided in response to the TQs. Relevant TQs and ROs in this area are: TQ-AP1000-359 to 365, TQ-AP1000-854 to 861, and RO-AP1000-045.

158 The RGA for this particular area of the PSA has shown that the most significant numerical gaps could be associated with the following findings:

- Omission of Type A HFEs (e.g. mis-alignments and mis-calibrations). When the most important missing pre-accident human errors were included in the system fault trees, an increase in the CDF was observed. It is interesting to note that similar results have been obtained independently by Westinghouse, as reported in Chapter 10 of the 2010 draft version of the PCSR (Ref. 12). The RGA also showed that the impact on LRF was higher than on CDF.
- Omission of Common Cause Failures between the high pressure and low pressure squib valves in the sump recirculation lines.
- Omission of failures leading to loss of IRWST inventory in the IRWST injection and sump recirculation fault trees.
- The modelling of loss of off-site power as a consequence of any reactor trip increases the CDF by a small percentage.
- Westinghouse's evaluation of the numerical significance of the errors found during the review of the PSA model (fault trees) was of limited use since first, a significant number of errors were left out of the scope of this exercise, and second, each fault tree correction was evaluated individually. However, it was noted that some non negligible gaps were observed, e.g. when the failure of the make-up to the Condensate Storage Tank was included in the SFW fault trees.

4.7.4 Conclusions

159 Based on the outcome of this assessment, I have concluded that, despite the deficiencies found, the current system fault trees are sufficient to support the AP1000 "generic" PCSR PSA because the RGA has provided clarity on the impact of the key limitations identified.

160 However this part of the AP1000 PSA needs significant enhancements to support further stages of the NPP development. It should also be noted that there may be limitations in other system fault trees that were not sampled in GDA so the totality of the AP1000 PSA fault trees should be revised as appropriate. Thus, improvements in the fault tree models should be undertaken as part of the next update of the PSA (see Section 5 below).

4.8 Level 1 PSA: Human Reliability Analysis (A1-2.5)

4.8.1 Assessment

161 I conducted an initial review of the AP1000 PSA task on "Human Reliability Analysis (HRA)" against the expectations in T/AST/030 (Table A1-2.5) GDA Step 3. My review raised concerns in the following areas:

- Lack of modelling / consideration of pre-initiator HFEs (also raised in the systems assessment).
- Assessment of time windows for operator actuation.
- Consideration of post-fault diagnosis (cognitive errors).

- Recovery model used in the Human Error Probability (HEP) calculations (recoveries by other members of the operating team and consideration of dependencies).
- Applicability of the Technique for Human Error Rate Prediction (THERP) data for AP1000 digital interfaces and facilities.

162 ND's Human Factors assessment team has conducted detailed reviews in GDA Step 4 to follow up the above concerns and expand the assessment to address the expectations of ND's Technical Assessment Guide on HRA T/AST/063 (Ref. 52). The results of this review are reported in the Human Factors Assessment Report (Ref. 26).

163 During GDA Step 4, my assessment team has supported the Human Factors team's assessment of the AP1000 PSA HRA as follows:

- The Human Error Probabilities (HEP) used in the AP1000 PSA have been extracted from the THERP method in NUREG/CR-1278 (Ref. 53). These probabilities are medians of lognormal distributions. However, for these to be used in PSA quantification, they need to be transformed into means. My review team has assessed Westinghouse's calculations to convert the THERP medians into means.
- As already raised in my GDA Step 3 PSA review, the AP1000 PSA does not include pre-accident human errors, also called Type A HFEs (e.g. mis-alignments and mis-calibrations) and the criteria for their exclusion were not considered adequate. In GDA Step 4 this was also considered by ND's Human Factors team an important limitation in Westinghouse's Human Factors submission. In response to this concern Westinghouse made a significant effort to identify credible Type A HFEs and to developed a method to calculate HEPs for these (Ref. 47). The method and its application were reviewed by my PSA assessment team.

164 A Risk Gap Analysis has been performed to address the general findings in this area and to understand their potential risk significance. The GDA Step 4 review of the HRA by ND's Human Factors team (Ref. 26) was not completed in time to be subject to an RGA evaluation of findings. Thus, the RGA in this area mainly addressed the findings from my GDA Step 3 and Step 4 reviews of the PSA that were related or were judged to have an impact on the HRA. An initial screening of findings was conducted using qualitative arguments and applicable quantitative information from the PSA. This resulted in a list of those perceived deficiencies in the HRA which were judged to have a non-negligible numerical risk impact. These were subject to further quantitative evaluation as described in the following bullet points:

- As already explained in Section 4.7.1 above, some fault trees were modified to explicitly include missing Type A HFEs. These were selected from among those identified by Westinghouse in their Human Factors submission (Ref. 47), based on risk significance of surrogate events already modelled in the fault trees. Human Error Probabilities calculated by Westinghouse for the Type A HFEs have been used for the purpose of the RGA.
- In the PSA the cognitive HFEs (failures to recognise the need to perform required actions) are evaluated by considering omissions (e.g. failure to respond to alarms), commission errors (e.g. misread of displays) and recovery failures by other control room members depending on the time window. Cognitive time-dependent failures to recognise and identify the event (diagnose) and take the relevant decisions on time have not been considered. To address this limitation of the HRA the Type C HEPs with cognitive elements were first identified. The most important ones were then selected for further manipulation. A probability value of 2×10^{-3} was added on to the

HEPs for the selected HFEs based on the THERP (Ref. 53) non-response curves assuming a 30 min time window.

- A more bounding case to further explore the possible gap associated to non consideration of cognitive errors, was carried out, as a sensitivity analysis, by adding to the HEPs for the 5 most important HFEs with cognitive elements values in the range of 0.03 to 0.2 based on time-reliability curves in the literature (Ref. 54) using Westinghouse's time windows and stated "actual" (median) time from Chapter 30 of Ref. 21. It should be noted that Ref. 54 was selected, only for the purpose of a sensitivity analysis, because it is easy to use, but its limitations are recognised.
- In the PSA, recovery by the Senior Reactor Operator (SRO) with a HEP of 0.1 is applied in general to any initial operator error when the time window is greater than 5 minutes, if the estimated actual time does not exceed the available time window. The PSA also considers a recovery function of the Shift Technical Advisor (STA), who is assumed to arrive in the control room within 5 to 10 minutes of the event and whose role is to monitor the overall status of the plant parameters. A HEP of 8.1×10^{-2} is applied for the STA when the time window and slack time criteria are satisfied. The adequacy or otherwise of assuming these recoveries is not judged here. This has been addressed by ND's Human Factors team and is discussed elsewhere (Ref. 26). For the purpose of RGA, these recoveries were removed, as appropriate, to account for findings related to time windows.
- Finally, the CAFTA recovery rule file was modified to account for missing cognitive HFEs identified in the reviews of the event trees and fault tree systems models, and missing or underestimated dependencies between HFEs.

4.8.2 Strengths

165 The review of the conversion of THERP data from medians to means has concluded that the method applied is correct.

166 Although pre-accident HFEs (Type A) have not been included in the AP1000 PSA, an identification of this type of human error and a human error probability analysis is presented in Westinghouse's Human Factors submission to GDA (Ref. 47). This has confirmed that the human errors of this type are credible for the AP1000 and cannot be disregarded or considered negligible as implied by their omission in the current PSA model.

167 My team has reviewed the method and formulae used by Westinghouse for the calculation of the human error probabilities for the identified Type A HFEs and found them to be correct. Some spot checks on the application of the method were carried out and found the results to be also correct.

4.8.3 Findings

168 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34 and 35.

169 Although the review of the conversion of THERP data from medians to means has concluded that the method applied is correct, a small number of errors were found in the application of the method.

Assessment Finding AF-AP1000-PSA-033: *The Licensee shall provide revised values for the Human Error Probabilities in the PSA with correct conversion of medians into means.*

170 In relation to the HEP analysis for pre-accident human errors included in Westinghouse's Human Factors submission, the following concerns were raised:

- Regarding the values used in developing the HEP tables (that are then used for further analysis), the PSA review team identified that the probabilities obtained are sensitive to the choice of HRA method. Westinghouse has selected HEART (Ref. 55) to support the Type A HFE probability evaluation for the Human Factors submission, rather than the HRA method used in the AP1000 PSA (THERP). The review found, for example, that the use of a HEART probability value of 0.02 (HEART generic task E) for the failure to identify the error in an immediate checking is quite significant. THERP probability values for failure of checking are higher (around 5 times greater). It was also noted that had THERP been applied to assign a probability to the initial human action lo leave the component misaligned (or mis-calibrated), values a little higher than 0.003 would have been obtained, with some variation depending on the specific details of the task. Therefore, it was concluded that THERP would give slightly higher initial error probabilities and would give values around 5 times higher for probabilities of non-recovery of initial errors.
- Although the spot checks of individual calculations found the results to be correct, my team raised concerns regarding the unclear basis for some assumptions, for example the assumed frequency of component manipulations and timing of verifications (checks).
- I raised additional concerns about the ability of some visual checks claimed to be able to recover the initial error (misalignment or mis-calibration), to actually identify and correct the error. For example it was unclear whether visual checks of the squib valves power supply connections, detonator assembly and charges (installation) can reasonably be claimed to have a reliability as high as 98% as assumed in Westinghouse's submission.
- The identified Type A HFEs are in fact a number of individual HFEs (for different components) lumped together; however, the overall HEP calculations have not been done taking all the specific events into account. It was therefore felt that some of the overall HEPs could well be optimistic.
- Detailed HRA evaluations were only conducted for a number of HFEs selected from the compete list of identified HFEs. All HFEs without impact on CDF were screened out of the evaluation. This led to removal from detailed analysis of those HFEs affecting the Level 2 PSA only. This screening would not be acceptable for a PSA submission.
- Finally, my team made an attempt to map the Type A HFEs identified in Westinghouse's Human Factors submission to specific components in the PSA model. The aim was to make use of this part of the submission as a direct input to the Risk Gap Analysis. This effort was not completely successful because the HFE boundaries referred to systems rather than components and therefore they were not detailed enough to allow a quick, unambiguous and realistic link between the HFEs and individual events in the PSA model.

Assessment Finding AF-AP1000-PSA-034: *The Licensee shall provide a revised method for the evaluation of probabilities for pre-accident HFEs using an HRA*

method consistent with the one used in the rest of the HRA in the PSA. The method should be applied to all the Type A HFEs in the PSA and should realistically take into account the frequency and ability of the credited tests and surveillances to identify and correct latent human errors.

Assessment Finding AF-AP1000-PSA-035: *The Licensee shall provide PSA documentation with a clear mapping between the specific aspects of the PSA model and any supporting Human Factors analyses.*

171 The following insights were obtained from the RGA for this particular area of the PSA:

- The CDF was sensitive to changes in the Type C HFEs to include an additional cognitive element but the CDF values remained low.
- Corrections and changes in the CAFTA recovery rule file to account for missing cognitive HFEs and missing or underestimated dependencies between HFEs led to a very small increment in the CDF.
- As already discussed in 4.7.3 above, the inclusion of Type A HFEs (e.g. mis-alignments and mis-calibrations) has a potentially higher impact on the CDF and a more significant one on LRF.

4.8.4 Conclusions

172 Based on the outcome of this assessment, the Human Factors assessment (Ref. 26), and the results of the RGA, I have concluded that the current human reliability analysis (supplemented by the study of pre-accident human errors in Westinghouse's Human Factors submission, Ref. 47) is sufficient to support the AP1000 "generic" PCSR PSA.

173 However this part of the AP1000 PSA needs enhancements to support further stages of the NPP development, i.e. improvements in the HRA should be implemented as part of the next update of the PSA (see Section 5 below).

4.9 Level 1 PSA: Data Analysis (A1-2.6)

4.9.1 Assessment

174 I conducted a high level review of the AP1000 PSA task on "Data Analysis" against the expectations in T/AST/030 (Table A1-2.6) during GDA Step 3. This review raised general concerns in the following areas:

- Criteria for selection of data sources and order of precedence of data sources.
- Scope and age of the data used for the evaluation of initiating event frequencies and justification of frequencies of LOCAs and SGTR.
- Age of data used for component reliability and CCF parameters.
- Mission times.

175 My detailed review of the data analysis element of the AP1000 PSA in GDA Step 4 has been performed following on from the review conducted in GDA Step 3 by looking in detail at a large sample of the reliability data used in the PSA. My review has examined the specific values used in the AP1000 PSA (with almost full coverage) as well as any relevant assumptions and calculations performed in support of the data analysis.

176 My review of the initiating event frequencies was based on Chapter 2 of the AP1000 PSA (Ref. 21). This also covered Chapter 3 of Ref. 21 entitled "Modelling of Special Initiators"

which documents the evaluation of some system failures which result in a reactor trip, i.e. loss of Component Cooling Water System (CCS) / Service Water System (SWS), loss of Compressed and Instrument Air System (CAS) and spurious actuation of the Automatic Depressurization System (ADS).

177 My review of the random component failure data and maintenance unavailabilities was based on Chapter 32 of Ref. 21. For this review significant use was made of the AP1000 PSA CAFTA model (Ref. 25) to ensure consistency throughout the assessment between the data and the basic events and modules included in the model.

178 The data assigned to special events for event tree nodes (according to Chapter 31 of Ref. 21) and other data elements found in the new CAFTA model (Ref. 25) have also been addressed in the review.

179 Finally my review has examined in detail both the methods used to calculate the common cause failure probabilities as well as the CCF parameters used in determining the CCF probabilities used in the AP1000 PSA model as documented in Chapter 29 of Ref. 21. The assumptions for screening CCFs have also been reviewed.

180 A Risk Gap Analysis was performed to address the findings from the review of the AP1000 reliability data. This was undertaken by a global update on the AP1000 reliability data base covering all those events in the PSA for which the review considered that their probabilities had been underestimated when compared against modern sources of data (Refs 56 and 57). This was a time consuming task due to the huge number of modular events in the PSA whose individual components needed to be addressed on a case by case basis. The resulting changes in the reliability database were implemented in the Base-case (BC) RGA Model (discussed in Section 2.3.2 above). As well as updating the failure rates of a number of components, the following additional specific items are worth highlighting:

- The frequency of Interfacing System (IS) LOCA was recalculated and, since this IE is assumed to directly lead to core damage and large release, the single event cutset was directly added to the revised CDF and LRF. Other than this, no other IEs were identified for which the frequencies needed to be reassessed or modified for the RGA.
- The mission time for the Diesel Generators was increased to address the GDA Step 3 review finding.
- The unavailability due to testing and / or maintenance of the air compressors in the PSA was modified because it appeared optimistic when compared against generic data.
- The probabilities of individual components in the C&I systems were not reviewed or changed (e.g. PMS input and output modules, processor modules, etc; PLS ovation controllers, data highway, etc). Instead, the probabilities of the three events representing common cause failures of the PMS software, PLS software and PMS-PLS software were increased, based on reviewers' judgement, to account for potential optimisms in the reliability credited for those systems.

4.9.2 Strengths

181 The basis for the selection of the reliability data values assigned to most basic events and modules in the AP1000 PSA have been documented in the PSA report (Ref. 21).

182 Although the data sources for most data items are dated, the review has identified that apart from a few exceptions the data values used in the AP1000 PSA appear to be

reasonable or, sometimes, even a bit conservative. In fact a comparison with one of the most recent generic data sources NUREG/CR-6928 (Ref. 56) has demonstrated that the values used in the AP1000 PSA for initiating events frequencies, component random failure probabilities, and equipment test and maintenance unavailabilities are not optimistic in comparison with the generic data source. The exceptions to this are discussed in the following sub-sections.

183 The review team has compared the CCF parameters used in the AP1000 PSA with a recent update of the US Generic CCF Database (Ref. 57) and has found that in general the AP1000 PSA CCF parameters are not lower than those in Ref. 57.

184 In response to a number of TQs issued in GDA Step 3, raising general and methodological findings from the review of the AP1000 PSA data analysis, Westinghouse has committed to address the findings and to extensively review the AP1000 PSA data.

4.9.3 Findings

185 The detailed technical reviews that support the findings discussed in the following sub-sections are documented in Refs 34, 35 and 58.

4.9.3.1 Initiating Event Frequencies (A1-2.6.1)

186 In GDA Step 3, my review team raised general concerns about the AP1000 IE frequency analysis, including general lack of auditability. My more detailed review in GDA Step 4 has confirmed that these methodological concerns were valid.

187 The review judged that the value for the frequency of the initiating event IEV-ISLOC (Interface System LOCA, ISLOCA, via the RNS) used in the AP1000 PSA (Ref. 25), $5x10^{-11}$ /yr, was underestimated. The basis of this finding was an independent evaluation of the ISLOCA frequency done by the review team using data from Ref. 56.

188 My team considered that the frequency of the initiating event IEV-SPADS (Large LOCA due to Spurious Actuation of ADS) used in the AP1000 PSA (Ref. 25), 1.5×10^{-8} /yr, was underestimated. Information on failures of safety critical software based systems found in the literature (Ref. 59) suggests that (software related) unsafe failure rates lower than 10^{-7} /hr cannot be easily justified based on available data. This is not inconsistent with the upper value (10^{-7} /hr) given in Table 2 of Chapter 7.6.2.9.of the Standard of the International Electrotechnical Commission (IEC) IEC61508 (Ref. 60) for “average frequency of a dangerous failure of the safety function (PFH)” for systems considered to have a Safety Integrity Level (SIL) of 3. Based on this information the PSA team judged that a frequency of 1.5×10^{-8} /yr for spurious opening of the ADS valves (one of the main causes being malfunction of the software based PMS) was an optimistic value considering the system design at the time of the review. It should be mentioned however that modifications to the ADS valves actuation have been proposed during GDA that would reduce the frequency of spurious opening of ADS valves significantly. This is discussed in more detail in the C&I Assessment Report (Ref. 61).

189 Westinghouse uses 1988’s NUREG-0844 (Ref. 62) to evaluate the probability of consequential steam generator tube rupture following SG depressurisation transients. My team judged that this methodology is now out of date. In addition, the review found that the assumptions made by Westinghouse in the application were not justified.

Assessment Finding AF-AP1000-PSA-036: *The Licensee shall provide revised frequencies, properly justified and documented, for all the Initiating Events in the PSA.*

Assessment Finding AF-AP1000-PSA-037: *The Licensee shall provide revised probabilities, properly justified and documented, for all the consequential Initiating Events in the PSA.*

4.9.3.2 Random Component Failures (A1-2.6.2)

190 In GDA Step 3, my review team raised general concerns about the AP1000 analysis of component reliability. In particular concerns were raised in relation to the identification of component boundaries, applicability of data sources, traceability of the data, mission times, etc. The detailed review in Step 4 has confirmed that the general concerns were valid.

Assessment Finding AF-AP1000-PSA-038: *The Licensee shall provide revised mission times consistent with the evolution of the accident sequences.*

191 For the AP1000 PSA, hourly failure rates have been derived from demand failure rates (taken from generic data sources) assuming that the components are actuated once per month. This is potentially incorrect as the test intervals of the source data are not known. Also, this implicitly assumes that the failure modes are time related rather than demand related which is not necessarily correct in all cases. On the other hand, Westinghouse has used the failure on demand probability model for explosively operated valves (squib valves). In this particular case my review team considered that, due to the long test intervals for these valves, using the method to obtain standby failure rates consistently with what has been done for the other components, would have resulted in higher failure probabilities than those currently assigned to the squib valves in the PSA.

192 My review identified that test intervals for components that are tested during the refuelling outage are not explicitly modelled in the PSA using the correct reliability model approximation, i.e. $1/2*\lambda T$. Although the model used instead to evaluate the reliability of the relevant components produced results that are mathematically correct, this modelling is not transparent. Also, a discrepancy in relation with test intervals was identified. Chapter 54.2 of the PSA (Ref. 21) indicates that for the AP1000 a refuelling outage will take place every 18 months. However, for components in the AP1000 which have a test interval based on the refuelling outage, a test interval of 24 months has been used instead. This appears to be based on the AP600 refuelling cycle and not the UK AP1000 refuelling cycle.

193 In the AP1000 reliability data analysis there is a specific assumption that reads as follows: “if the water chemistry is controlled and there are devices to prevent the drop of plugging material (e.g. screen), the failure rate of orifice plugging in a system with normally stagnant water is assumed to be 0.1 of the failure rate for continuously flushed lines”. No attempt to justify this assumption is made in the documentation reviewed. This unjustified reduction in failure rate is of particular concern for orifices in systems with borated stagnant water where plugging may occur more frequently, rather than less frequently.

194 Failure probability values used in the AP1000 PSA for the components listed below are lower than those in NUREG/CR-6928 (Ref. 56), which is one of the more recent generic data sources available. The review team therefore judged that the AP1000 PSA values are optimistic for the following components:

- Explosive Operated Valves;
- Air Operated Valves;
- Circuit Breakers;
- Check Valves;
- Chiller Units (both failures to start and to run);
- Relays;
- Motor Driven Pumps;
- Orifice Plugging;
- Blower / Fan (both failures to start and to run);
- Electrical Busses;
- Transformers;
- Diesel Generators (failure to start and run for the 1st hour);
- Batteries; and
- Compressor (Standby).

195 From the above components, squib valves are of particular interest due to the limited operating experience for this type of valve which makes the values obtained from generic data sources also not strong. Note that NUREG/CR-6928 (Ref. 56) reports a probability of failure to open on demand for explosive operated valves of 1.07×10^{-3}. This estimate is based on 0 failures in 468 demands. In the AP1000 PSA the squib valves have been assigned probabilities of failure to open on demand of 5.8×10^{-4}. This value seems only slightly optimistic compared to the generic data; however one should bear in mind that the AP1000 squib valves are much larger in size than those used previously in nuclear applications and this demands a much more transparent justification of the probability values used in the PSA.

196 The probability of failure to open both pressuriser safety valves “PRES“ (used in the model of ATWS following loss of main feedwater) is calculated from the probability of failure of 2 safety valves. The failure probability for a safety valve has been assumed to be 10^{-3} per demand from an unidentified source. This value is lower than 2.47×10^{-3} which is the value for the probability of failure to open a safety valve (SVV FTO) in NUREG/CR-6928 (Ref. 56). The review judged that the AP1000 PSA figure was optimistic.

> ***Assessment Finding AF-AP1000-PSA-039:*** *The Licensee shall provide revised reliability data, properly justified and documented, for all the random component failures in the PSA. The Licensee shall justify the reliability model used on a case by case basis.*

4.9.3.3 Unavailabilities Due to Testing and Maintenance (A1-2.6.3)

197 General concerns regarding the way in which unavailabilities due to Testing and Maintenance (T&M) are included in the AP1000 PSA model were already raised in GDA Step 3. During GDA Step 4 my detailed review found a number of inconsistencies in the modelling on T&M unavailabilities which could not always be understood:

- In some cases all T&M unavailabilities for multiple trains of a system have been embedded into a single basic event, but from the basic event descriptions it was not clear when this is applied.
- In other cases, separate T&M unavailability events are modelled for the individual trains. However the PSA documentation does not discuss T&M events which should not occur simultaneously although potential coincident maintenance events have been excluded in the quantification of the UK AP1000 PSA 3B model (Ref. 25) using rules which are not sufficiently explained in the documentation reviewed.

198 The T&M unavailabilities are based on assumptions listed in tables in Chapter 32 of the PSA (Ref. 21), and in some cases, the bases of T&M events are also described in the relevant system chapters. However, the outage times for the Normal Residual Heat Removal System (RNS), Component Cooling Water System (CCS), Service Water System (SWS), Start-up Feedwater System (SFW), and Chemical and Volume Control System (CVS) are based on unreferenced Westinghouse data. My review team therefore considered that the T&M unavailabilities for those systems are not justified. This was a concern in particular because these are some of the systems that for the AP1000 were originally classified as "non-safety" systems. Therefore, Westinghouse's unavailability data for equivalent systems in existing PWRs which are safety systems controlled by Technical Specifications may be optimistic for the AP1000. It should be noted that it is now believed that for the UK some of these systems will be reclassified and included in UK Technical Specifications. In any case, all sources of T&M unavailability data should be appropriately referenced and justified.

199 The comparison between T&M unavailabilities used in the AP1000 PSA and maintenance unavailability data in NUREG/CR-6928 (Ref. 56) showed that values lower than those in the generic data source had been used in the AP1000 PSA for the compressors. The review considered this to be unjustified and potentially optimistic.

> ***Assessment Finding AF-AP1000-PSA-040:*** *The Licensee shall provide revised unavailabilities due to testing and maintenance properly justified and documented.*

4.9.3.4 Common Cause Failures (A1-2.6.4)

200 In GDA Step 3, my review team identified that the AP1000 CCF analysis had assumed and taken into account some features that could serve as defences against CCF in order to screen out certain types of CCFs but did not look in detail at this part of the analysis. These are listed in Sub-chapter 29.3.1 of Ref. 21. These assumptions have been looked at in detail in GDA Step 4. From this review the following can be highlighted:

- The review has concluded that most of the assumptions made for screening out some CCF types are not justified for application in all cases. ND's PSA team considers that each assumption should be tested individually for each system or group of systems for which the assumption is to be applied.
- Chapter 29 of Ref. 21 indicates the following: "CCFs of Heat Exchangers (HX) belonging to different systems to plug or leak are not considered because the water characteristics and system operation conditions (pressure, temperature, and flow) are different for HXs used in different systems. Furthermore, within the same system, one HX is in operation and the other is in standby. Therefore, it is unlikely to have more than one HX fail at the same time". My team considers that CCFs (plugging or leaking) of HXs belonging to different systems should not be excluded. Instead, explicit justification should be provided to demonstrate that sufficient defences against

CCF are in place. The same would apply to CCFs of HXs or other equipment between standby and running trains, CCFs (plugging) of orifices, etc.

- In order to screen out CCFs based on low probabilities, conservative screening values should be used (rather than realistic figures). This is to ensure that screening out those CCFs is not optimistic (in the lifetime of the PSA and for all possible applications). Apparently the low failure probability approach has been used by Westinghouse to screen out CCFs affecting only electrical components. My team consider this to be inadequate.
- Despite the concerns above, my team identified that, in practice, some of these assumptions are not applied consistently, which makes the PSA documentation and model inconsistent and confusing. For example Chapter 29 of Ref. 21 indicates that plugging is assumed credible only within the IRWST during the gravity injection phase, where the two injection lines take water from the same pool. Presumably, this assumption has been used to disregard the CCFs of plugging of tanks with high boron concentration such as Accumulators and CMTs, which, my review team judges, should have also been included in the model. On the other hand, the PSA model correctly includes, although against the assumption, an event REX-FL-GP "Plugging of both recirculation lines due to CCF of sump screens". Also the PSA model includes CCF of the HXs in the component cooling water system. My team agrees that this is correct although it contradicts one of Westinghouse's CCF assumptions discussed above.

  Assessment Finding AF-AP1000-PSA-041: *The Licensee shall provide revised and documented Common Cause Failure modelling taking into account all component types, and considering, on a case by case basis, all coupling mechanisms and defences in place against these.*

201 Detailed review of the calculations performed for the CCFs identified various issues that can be summarised as follows:

- Chapter 29 of Ref. 21 documents the calculations performed to evaluate CCF probabilities. Detailed reviews of these have identified that some CCF probabilities had been calculated using an incorrect number of possible combinations of failures. This particular problem was found in the CCF probability calculations for Accumulator check valves, containment isolation AOVs to operate to de-energised position, CMT check valves, steam dump AOVs, check valves in the RNS. In addition, the simplified Multiple Greek Letter (MGL) model used by Westinghouse for the CCF for Stages 1, 2 and 3 ADS (i.e. a group of components subject to CCF larger than 4) is optimistic. However, it should be noted that recalculations performed by my team for these particular cases using the correct amount of combinations together with up to date data from Refs 56 and / or 57, did not result in increases to CCF probabilities.
- On the other hand, the review team revisited the CCF modelling and the CCF probability calculations for the IRWST injection and recirculation squib valves. This re-evaluation resulted in an overall increase in CCF probability.
- The CCF probability for reactor trip breakers used in the AP1000 model reviewed is lower than the result of the calculation presented in Chapter 29 of Ref. 21. No justification was found in the PSA documentation accompanying the version 3B of the CAFTA model (Ref. 25) for this reduction.
- In the PSA the following values are assigned for Software CCFs: 1.1×10^{-5} /demand for PMS software, 1.1×10^{-5} /demand for the PLS software and 1.2×10^{-6} /demand for

the CCF between the PMS and PLS software. No convincing justification for these values has been found in any of the documentation reviewed. It should be noted that sensitivity analyses have been conducted both by Westinghouse (Ref. 63) and my team (Ref. 35) which show that even significant increases in these probabilities did have an impact on the risk but did not result in unacceptable risk levels.

Assessment Finding AF-AP1000-PSA-042: *The Licensee shall provide revised CCF probabilities properly justified and documented.*

4.9.3.5 Results of the Risk Gap Analysis

202 The RGA for this particular area of the PSA showed that the most significant numerical gaps were associated with the following:

- Revised frequency of Interfacing System LOCA. This had a small impact on the CDF but a much more significant impact on the LRF.
- Revised probabilities of the three events representing common cause failures of the PMS software, PLS software and PMS-PLS software. These changes had larger impact on the LRF than on the CDF.
- The rest of the changes in reliability data had a small overall risk impact.

4.9.4 Conclusions

203 Based on the outcome of this assessment, I have concluded that overall the current AP1000 PSA reliability data is sufficiently adequate to support the AP1000 "generic" PCSR PSA.

204 However this part of the AP1000 PSA needs enhancements to support further stages of the NPP development, i.e. an improved reliability database should be developed as part of the next update of the PSA (see Section 5 below).

4.10 Level 1 PSA: Analysis of Hazards – Screening of Internal Hazards (A1-2.7-1)

4.10.1 Assessment

205 An initial review of the AP1000 PSA task on "Screening of Internal Hazards" against the expectations in T/AST/030 was conducted in GDA Step 3 by my PSA assessment team. This review identified that the analysis of hazards for the AP1000 PSA did 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) had been presented in the PSA documentation.

206 In order to support my GDA Step 4 assessment effort and get a better understanding of the AP1000 risk associated with internal hazards events, I requested Westinghouse to provide justification for the apparent lack of formal screening of internal hazards (other than flood and fire) for inclusion in the PSA. However, the response provided by Westinghouse was largely based on comparisons with generic screening methods for conventional PWRs (Refs 64 and 65) and did not present any systematic quantitative or qualitative evaluation to justify that the risk from the internal hazards screened out was insignificant.

207 In light of this, my team has performed in GDA Step 4 a review of the deterministic arguments in this regard presented by Westinghouse in Chapter 11 of the 2010 draft

version of the AP1000 PCSR (Ref. 12) and in the Internal Hazards Topic Report (Ref. 68) to explore whether there are specific vulnerabilities which may be potentially risk significant for the AP1000. The following internal hazards were reviewed:

- Internal explosions.
- Internal missiles.
- Release of toxic chemicals.
- Dropped loads.
- Biological hazards.
- Onsite transport.
- Electro magnetic interference (onsite).

208 No quantitative risk gap analysis was feasible due to the generic nature of the information gathered during the review of the deterministic analysis.

4.10.2 Strengths

209 With respect to the assessment of the Screening of Internal Hazards there are no strengths to report due to the incomplete state of the analysis.

4.10.3 Findings

210 The detailed technical review that support the findings discussed in the following paragraphs is documented in Ref. 34.

211 No comprehensive list of potential internal hazards has been provided in the AP1000 PSA. 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. The rationale provided as justification for this position is based on comparisons with generic screening methods for conventional PWRs (Refs 64 and 65). In the absence of further information, I do not consider this is sufficient to justify a low risk contribution from other internal hazards for the AP1000 design for the following two reasons:

- Previous generic reviews of internal hazards which provide a basis for screening internal hazards were performed assuming a baseline CDF for conventional PWRs of 10^{-5} to 10^{-4}/yr. In those cases, internal hazards could be screened out by demonstrating that the risk contribution was <10% of the CDF (i.e. 10^{-6} to 10^{-5}/yr). Given the current AP1000 total CDF claimed by Westinghouse, the corresponding screening threshold would need to be much lower than in previous generic reviews to demonstrate that the risk associated with "other" internal hazards would be insignificant.
- The design and layout of the AP1000 is substantially different to a conventional PWR. Further justification is therefore required in order to consider the effect of differences in the context of internal hazards.

Assessment Finding AF-AP1000-PSA-043: *The Licensee shall provide a systematic screening of all internal hazards, representative of the design and layout of the AP1000 and a demonstration that the risk associated with all the screened out internal hazards would be insignificant compared to the AP1000 total risk.*

Assessment Finding AF-AP1000-PSA-044: *The Licensee shall provide a PSA for the internal hazards that have been screened in according to the stated criteria.*

212 In order to get a further understanding of the potential risk associated with internal hazards other than fire and flood, my team looked at Chapter 11 of the 2010 draft version of the PCSR (Ref. 12). This identified that the deterministic arguments presented in relation to the releases of toxic chemicals appear to rely upon operators donning respirators within a few minutes of the release. From a risk perspective the reliability of operators recognising that a release has occurred and protecting themselves in a timely fashion would need to be justified.

213 Other than the above, the review of the deterministic analysis of internal hazards conducted by my team has concluded that the design intent provides a substantial level of defence in depth against a wide variety of internal hazards. Furthermore, provided the design intent can be met to the satisfaction of ND's Internal Hazards assessment team (for example, the capability of hazard barriers can be adequately demonstrated) there do not appear to be any obvious risk vulnerabilities.

214 However, it should be noted that there are uncertainties in the engineering substantiation of the AP1000 design intent in relation to the internal hazards safety case. These are discussed in the GDA Step 4 review of the AP1000 Internal Hazards submission (Ref. 67). In particular GDA Issues have been proposed by ND's Internal Hazards team as Westinghouse has not provided an adequate internal hazards safety case in time for GDA assessment. These uncertainties and the outcome of the GDA Issues on internal hazards, could impact my team's understanding of the risk associated with these events.

4.10.4 Conclusions

215 Based on the outcome of my team's review of the Internal Hazards Topic Report (Ref. 68) and the draft PCSR Chapter 11 (Ref. 12), I have concluded that there is sufficient information in the documentation provided by Westinghouse to support the current claim that the risk associated with internal hazards (other than fire and flooding) for the AP1000 design intent is low, which has led to their exclusion from the PSA. This conclusion is only valid for an AP1000 "generic" PCSR PSA and relies on the substantiation of the design intent reviewed by ND's Internal Hazards assessment team (Ref. 67).

216 Overall, this part of the AP1000 PSA needs improvements and substantiation to support further stages of the NPP development. A systematic screening of all internal hazards should be provided, together with a technically sound evaluation of the risk associated with them, as part of the next update of the PSA (see Section 5 below for specific expectations).

4.11 Level 1 PSA: Analysis of Hazards – Analysis of Internal Fires (A1-2.7-2)

4.11.1 Assessment

217 During GDA Step 3 I conducted a high level review of the AP1000 PSA task on "Internal Fires" against the expectations in T/AST/030 (Table A1-2.7.2). My review identified that the current analysis, that had been performed mainly using a screening method, included both conservatisms and optimisms throughout and needed significant update to incorporate design changes. Overall I reached the conclusion that the Fire PSA was not a good representation of the AP1000 risk due to internal fires and hence did not provide a good basis for the evaluation of the strengths and weaknesses of the design. Specific concerns were raised in the following areas of the analysis:

- Method.
- Compartment detailed specific information and assumptions.
- Evaluation of circuits and selection of cables.
- Fire frequencies.
- Spurious actuations of equipment caused by fire.
- Fire induced phenomena with impact outside the compartment boundaries.
- Multi-compartment fires.
- Probabilistic model (including selection of fire-induced initiating events and human reliability analysis for fire scenarios).
- Fire PSA electronic model (not available).
- Level 2 PSA evaluation for internal fire scenarios (not provided).
- Applicability of the Fire PSA provided to the AP1000 design submitted for GDA.

218 In view of the above concerns in September 2009 I issued RO-AP1000-044 requesting Westinghouse to provide a programme for the review and update of the AP1000 Fire PSA to align it with up-to-date information and modern standards. The RO also requested the Fire PSA programme to be accompanied by enough information on standards, approaches and data sources to be used to allow my team to establish an initial judgement on whether the final Fire PSA for the AP1000 would be acceptable. The response to this RO indicated that Westinghouse was planning to develop a new Fire PSA for the AP1000 aligned with modern standards; however the work would not be completed until after GDA. This left my team with a lack of understanding of the AP1000 risk associated with internal fires and little information to further the assessment in GDA Step 4.

219 One of the objectives of the GDA Step 4 PSA assessment was to undertake a Risk Gap Analysis to help ND reach a conclusion on whether an AP1000 can be constructed and operated safely in the UK, to evaluate the importance of the findings in the various PSA technical areas, and to evaluate the overall gap between the "AP1000 risk" claimed by Westinghouse and an understanding of the AP1000 risk (based on a more realistic and complete evaluation). In order to support this GDA Step 4 assessment effort and get a better understanding of the AP1000 risk associated with internal fires, my team requested Westinghouse to provide:

- A White Paper with a (qualitative and / or quantitative) review of the “fire risk gap” addressing the risk significance associated with the concerns raised during my GDA Step 3 review of the Fire PSA.
- A CAFTA model for the top 5 fire scenarios with up-to-date plant information available and addressing, if possible, the gaps identified in the White Paper. This was requested so that my team could design and undertake an independent set of sensitivity analyses addressing the most significant uncertainties, i.e. addressing the areas perceived to contribute mostly to the fire risk gap.

4.11.2 Strengths

220 The general steps of the Fire PSA methodology, as implemented for the AP1000, are generally embodied within the more modern methods (such as that in NUREG/CR-6850).

In this respect the AP1000 Fire PSA is more systematic and detailed than equivalent studies prepared for the PCSR stage.

221 Although substantial enhancements are required within the detailed implementation of the Fire PSA, as discussed below, Westinghouse has committed to upgrading all aspects of the AP1000 PSA and associated documentation to the standard required by NUREG/CR-6850.

4.11.3 Findings

222 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34 and 35.

223 The review of Westinghouse's White Paper on "Internal Fire PSA" concluded that this had been written at a fairly high level and did not provide sufficient insights into the potential "fire risk gap". For example:

- No additional analysis had been performed to further investigate the specific deficiencies identified during my GDA Step 3 review of the Fire PSA.
- No discussion was provided of the impact on risk of the post 2002 design changes (including fire barriers).
- The paper compared the general design features of the AP1000 which are pertinent to fire vulnerability with a conventional PWR. In particular it considered the passive core cooling systems and the digital C&I features, which together minimize the amount of equipment vulnerable to fires, the potential for spurious actuations, the reliance on operator actions and potential for operator error due to erroneous signal. My team considers that the conclusions drawn are valid but are general, i.e. evidence supported by specific analysis is still lacking.
- The paper provided a task by task comparison of the AP1000 Fire PSA analysis method used with the approach in NUREG/CR-6850. Westinghouse's review confirms that the most substantial deficiencies in the AP1000 PSA method are related to the tasks on "Component Selection" and "Fire Risk Model Development". The potential implications of these limitations in the current Fire PSA are:
    - The fire-induced initiating events, system degradation mechanisms and high consequence spurious actuations may be more onerous than those currently identified.
    - The impact of fire on operator reliability due to degraded or misleading instrumentation has not been considered.
    - The potential for operator errors of commission in response to erroneous alarms has not been considered.
    - The potential for post-fire operator actions that can degrade equipment credited in the PSA has not been considered.
    - There may also be deficiencies in the circuit analysis and cable routing information although this is expected at this stage in the plant design and may be refined as the detailed design for the UK AP1000 progresses.

224 In addition to the above, in August 2010 Westinghouse informed ND that it had not been possible to re-produce the results reported in the Fire PSA documentation for the top 5 scenarios using the CAFTA model.

225 All the above left my team with a significant lack of understanding of the AP1000 risk associated with internal fires, a lack of evidence that this risk is negligible or even small, and the inability to undertake sensitivity analyses to investigate the areas of higher uncertainty and hence to evaluate the potential risk gap.

226 In addition, fire risk insights applicable to the AP1000 cannot be drawn from Fire PSAs for other PWRs because of the significant design differences that could have a direct bearing on the AP1000 fire risk. One of the features of the AP1000 is that its layout is very compact in comparison with many PWRs and this has an impact on what can be claimed from earlier PWR experience.

227 Since the current prediction of the fire CDF is 5×10^{-8} /yr (approx 25% of the CDF) the uncertainty in the fire risk translates directly into uncertainty in the overall plant risk.

4.11.4 Conclusions

228 On the basis of the outcome of my GDA Step 3 assessment of the AP1000 Fire PSA and of the evaluation of the additional information provided by Westinghouse in GDA Step 4, I could not conclude that the current prediction of the internal fire risk for the AP1000 is representative and this is why a GDA Issue **(GI-AP1000-PSA-02)** has been raised on this topic. The complete GDA Issue and associated actions are formally defined in Annex 2.

229 I should also indicate that it is my judgement that any further work on Fire PSA will be incomplete and inadequate if it is based on the current incomplete list of IEs. Therefore, Westinghouse needs to address the findings from the review of the AP1000 identification and grouping of IEs to effectively respond to the GDA Issue on “Fire PSA”.

4.12 Level 1 PSA: Analysis of Hazards – Analysis of Internal Flooding (A1-2.7-3)

4.12.1 Assessment

230 An initial review of the AP1000 PSA task on “Internal Flooding” against the expectations in T/AST/030 was conducted in GDA Step 3 by my team. The review identified that the current AP1000 flood analysis was largely based on the analysis of the AP600 and was developed during the relatively early design stages when significant amount of detail required to perform an Internal Flooding PSA was not available. Furthermore, the analysis was performed before the development of industry guidelines and data for the performance of Internal Flooding PSA (Refs 69 and 71). Overall my judgement was that an extension of the analysis was required to address concerns related to aspects of the flooding analysis that appeared to be optimistic. Specific concerns were raised in the following areas of the analysis:

- Data for flood frequencies (more modern data reflects more accurately the frequency of spraying events).
- Maintenance induced floods (not considered).
- Consideration of structural failures due to the flood load, or compartment pressurisation.
- Failure mechanisms considered (limited to immersion and spray).
- Post flood human reliability analysis.

231 My detailed review of the AP1000 Flooding PSA in GDA Step 4 has been performed following on from the review I performed in GDA Step 3. In order to support my GDA

Step 4 assessment effort and get a better understanding of the AP1000 risk associated with internal flooding events, I requested Westinghouse to provide:

- A White Paper with a (qualitative and / or quantitative) review of the "flooding risk gap" addressing the risk significance associated with the concerns raised during my GDA Step 3 review of the Flooding PSA, with the design modifications since the model was developed and considering the potential significance of High Energy Line Breaks (HELB) (currently excluded).
- The internal flooding scenarios reported in the PSA documentation that had been reproduced by Westinghouse using the CAFTA model. It was understood that the scope of this model was limited to 6 of the 14 internal flood scenarios (38% of the internal flood CDF).

232 A Risk Gap Analysis has been performed, where feasible, to address the findings in this area and to understand their potential risk significance. An initial screening of findings was conducted using qualitative arguments and applicable quantitative information from the PSA. This resulted in a list of missing scenarios or gaps in the AP1000 Flooding PSA model that were judged to have a non-negligible numerical risk impact. Re-evaluation of the identified gaps was performed using the appropriate parts of the PSA CAFTA model. In this regard the following should be noted:

- Conservative assumptions were adopted as bounding the potential plant impact when the specific flooding mitigation plant features were not known.
- When neither enough information to understand the potential plant impact nor plant conditions analysis existed, the scenarios were excluded from the quantitative RGA evaluations.

4.12.2 Strengths

233 The approach adopted in the flooding analysis in the AP1000 PSA appears to be systematic and contains most of the essential elements of a modern Flooding PSA, despite preceding development of general industry guidance.

234 The White Paper prepared by Westinghouse in response to my request (Ref. 70) adequately correlated the steps undertaken in the AP1000 analysis to those prescribed within more modern references (Ref. 69) and generally justified differences in the context of the AP1000 specific design features. Despite this, Westinghouse has committed to re-do the Flooding PSA to address omissions or deficiencies identified in the current scope.

4.12.3 Findings

235 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34 and 35.

236 The review of the overall methodology, plant partitioning and potential flood source identification tasks concluded that Westinghouse's analysis related to compartmentalisation, barrier characteristics, flood propagation pathways and flood sources would require upgrades in documentation and scope to bring it up to the current state of the art. For example:

- The analysis of plant partitioning does not identify specific barrier elements such as doors, openings, drains or seals.

- The flood source identification does not provide a detailed mapping of piping sections, potential flood flow rates and volumes and the nature of the flood source (high, medium or low energy).

237 The review of the screening of compartments could not corroborate that all of the affected areas to the point of final flood accumulation had been identified. This was because the related documentation provided was incomplete in terms of flood area adjacency or inter area pathways (door, openings etc), and also because the potential for structural failures is not addressed in the documentation reviewed.

238 The review team identified that the evaluation of the flood impacts relies on potentially optimistic assumptions adopted in the deterministic analysis, which are not necessarily applicable to the PSA. For example, the screening of compartments uses maximum flood heights which are calculated assuming positive identification and isolation of flood sources within 30 minutes, i.e. without evaluating the potential for human error (Ref. 70). This simplification should not be used for screening purposes, although the importance of this simplification is generally expected to be limited by the inherent design features which design-out infinite flood sources in certain critical areas. However, following discussions with ND's Internal Hazards assessment team it appears that in the non-Radioactive Controlled Area (RCA) of the Auxiliary Building there could be sources of flooding (fire protection system pipe ruptures) with higher discharge rates than those assumed in Westinghouse's analysis. This, if confirmed, would compromise the current screening of flooding scenarios, and it would also impact other aspects of the flooding analysis, such as:

- The evaluation of maximum flood height calculations used to assess flood impacts in a compartment and the potential for flood propagation.
- The omission in the AP1000 Internal Flooding PSA of structural failures (including door failures) due to loads imposed by flooding or compartment pressurization.

239 In GDA Step 3, the review of the Flooding PSA already pointed out that generic flood frequency values had been used without apparent justification, although the AP1000 flooding frequencies appeared to be reasonably consistent with flood frequencies in more recent data sources. However, there were two remaining concerns:

- Frequency of spraying events appeared to be underestimated compared with more recent generic data available (Ref. 69).
- AP1000 flood frequencies do not consider AP1000 piping isometrics and do not take into account maintenance / human induced flooding events.

240 It was noted in my GDA Step 3 report that the current AP1000 analysis limits the assessment of flood related consequences to immersion and spray only. The impact of high temperature, humidity, jet impingement and pipe whip had not been addressed within the PSA. During the detailed review in GDA Step 4, my team identified potentially important High Energy Line Breaks (HELB) scenarios in the Containment, MSIV Vaults and Turbine Building which are currently not considered in the AP1000 Internal Flooding PSA. In particular, specific concerns have been raised for the following scenarios, extensively discussed with ND's Internal Hazards and Structural Integrity teams, as not enough information was available to understand the AP1000 behaviour in such conditions and thus the associated risk:

- A potential may exist for a ruptured Main Steam Line (MSL) to impact the other MSL resulting in a double Main Steam Line Break due to pipe whip. At the time of writing this report, it was the understanding of my team that there was no analysis available

for such a fault of sufficient scope and detail to support a reasonable risk gap evaluation.

- The failure of the MSL in the West MSIV vault could lead to consequential failure of the feed water line due to pipe whip. This event could be possible because, according to the understanding of my team at the time of writing this report, unlike the East MSIV vault, the West MSIV vault does not have pipe whip restraints and jet barriers. At the time of writing this report, it was the understanding of my team that there was no analysis available for such a fault of sufficient scope and detail to support a reasonable risk gap evaluation.
- Main steam line or feed water line breaks in the East MSIV vault could have a potential impact on the main control room located in proximity and on the essential C&I in the compartment below. It is believed that pipe whip restraints and jet barriers are installed to mitigate the dynamic effects of a double ended guillotine rupture in this compartment. However, it should be noted that, at the time of writing this report, there were uncertainties about the protective features available in this compartment.

241 The AP1000 internal flood model does not account for the impact of flooding on human error probabilities (HEP). Instead HEPs used in the internal events analysis are used un-changed in the quantification of the internal flooding model. This is considered optimistic because in reality stresses imposed by the accidental situation and possible degradation of plant monitoring instrumentation may have detrimental impacts such as:

- Additional dependencies between the HFEs to isolate the flood and HFEs involved in the mitigation of scenarios caused by flood.
- Flooding effects on performance shaping factors used to evaluate HEPs.

242 Finally, it should be noted that there are also uncertainties in the engineering substantiation in relation to the internal flooding safety case which can impact my team's understanding of the risk associated with internal flooding. These are discussed in Ref. 67. In particular a GDA Issue has been raised by ND's Internal Hazards team as Westinghouse has not provided an adequate internal flooding safety case in time for GDA assessment.

> ***Assessment Finding AF-AP1000-PSA-045:*** *The Licensee shall provide a modern complete and well documented Internal Flooding PSA representative of the design and layout of the AP1000.*

243 The RGA has been undertaken using conservative assumptions. But, even bearing this in mind, the RGA for this particular area of the PSA has shown that the Internal Flooding PSA in its present form cannot be claimed to be a valid representation of the risk associated with internal flooding for the AP1000 design. However, it is recognized that the results of a complete Internal Flooding PSA will depend on final design and specific plant features currently not known for the UK AP1000 (e.g. restraints, isolation means, indications, etc). Additionally, more information will be required on procedures to deal with flooding scenarios and any other relevant human factors aspects in order to complete the analysis. Moreover, characteristic features of the AP1000 design could make the plant inherently less sensitive to some of the identified missing events than conventional PWRs. Additional analysis will be necessary to ascertain this.

244 The most significant gaps found, which could be numerically more important than the currently estimated AP1000 PSA risk associated with internal flooding, are the following:

- Non-isolated HELB events in the Turbine Building (currently excluded from the analysis).
- Consideration of possible degradation of human performance because of the situation created by the flood.
- Floods originating in the non RCA Auxiliary Building (currently excluded from the PSA based on the assumption that the flooding source will be isolated within 30 minutes).

245 No practical method for addressing the risk gap for the following unknown scenarios has been identified and therefore the events have remained unanalyzed:

- HELB scenarios inside containment and in the MSIV vault compartments for which no specific analysis appears to be available (secondary steam line break or feed water line break occurring as a consequence of the various steam line breaks) or / and not enough information regarding available mitigation features has been provided.
- Potential flood scenarios screened out of the AP1000 Flooding PSA based on deterministic assumptions that may be optimistic and not applicable to the PSA (e.g. flood termination assumed within 30 minutes). The RGA has not undertaken a general re-evaluation of potential flood impacts during the qualitative screening without crediting these potential optimistic assumptions.

4.12.4 Conclusions

246 Based on the outcome of this assessment, I have concluded that the current results of the AP1000 Internal Flooding PSA together with the results of the RGA provide an important input for my team to get a partial understanding of the AP1000 risk associated with internal flooding. This is however insufficient to ascertain that this risk is low and more information is necessary to understand some of the identified un-quantified gaps.

247 In particular, a secondary steam line break or feed water line break occurring as a consequence of the various steam line breaks (inside or outside containment as appropriate) have not been assessed in the RGA because there is no analysis available to understand the plant behaviour. These events have been considered as part of the list of Initiating Events currently missing from the PSA (see Sub-section 4.4). Therefore, for Westinghouse to effectively respond to the GDA Issue on “Success Criteria”, the missing HELB scenarios also need to be considered. .

248 Overall, this part of the AP1000 PSA needs improvements and substantiation to support further stages of the NPP development. Westinghouse has committed to that so it is believed that an improved and modern Internal Flooding PSA will be developed as part of the next update of the PSA (see Section 5 below for specific expectations).

4.13 Level 1 PSA: Analysis of Hazards – Screening of External Hazards (A1-2.7)

4.13.1 Assessment

249 I conducted an initial review of the AP1000 PSA task on “Screening of External Hazards” against the expectations in T/AST/030 in GDA Step 3. This review identified that the analysis of external hazards for the AP1000 PSA did not start with a complete list. From the set of hazards listed, high winds, tornadoes, external floods, transportation and nearby facility accidents had been screened out on the basis of a frequency value. This was considered inadequate given the low claimed CDF and LRF. The seismic hazard

had not been screened out but neither had it been included in the PSA. Rather, it had been addressed via a Seismic Margins Analysis (SMA).

250 In view of the GDA Step 3 findings, my team requested Westinghouse to justify the PSA screening of external hazards, specifically with regard to whether their screening of external hazards would be adequate for the AP1000 within the UK.

251 Westinghouse's response has been assessed during GDA Step 4 with the support of ND's External Hazards team. The review has looked at:

- Completeness of the list of external hazards considered by Westinghouse.
- Adequacy of the process and logic employed for the screening of external hazards.

252 In the assessment of the above, ND's External Hazards team has reviewed in detail Westinghouse's assumptions on magnitude of the hazards and associated frequencies, which resulted in screening out of the AP1000 PSA submission all external hazards other than earthquakes.

253 The review has made significant use of the AP1000 External Hazards Topic Report (Ref. 72) which is part of the suite of documents submitted for GDA.

254 It should be noted that hazards from malicious activities were not within the scope of this review.

255 A Risk Gap Analysis was performed which consisted of a revised screening of external hazards considered to be applicable to sites in the UK and with potential risk significance (a screening criteria of CDF > 10^{-9} /yr was used). For the external hazards screened-in, i.e. external flooding, external fire and extreme temperatures, a CDF estimation was undertaken using an assumed frequency of 10^{-5} /yr and assumptions about impact on systems believed to be bounding. The impact on LRF was not investigated. The risk associated with external hazards that could be correlated was not explored either.

4.13.2 Strengths

256 The approach and criteria applied to the quantitative screening process for external hazards (from a pre-selected set) is auditable and justified in the references provided by Westinghouse and the reasons for inclusion / exclusion are well documented.

257 The frequency and magnitudes of the selected external hazards are clearly stated and identified in the documentation reviewed.

4.13.3 Findings

258 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35 and 73.

259 Following the review of documentation provided by Westinghouse, it was apparent that lists of external hazards from several US documents had been condensed down to those which had been regarded as potentially significant, based only on standard guidelines. No evidence was found of a documented selection or screening process having been undertaken.

260 Generic bounding site parameters are defined in Ref. 74, however the event frequency data associated with the bounding parameters is lacking.

261 Data from the NUSTART sites (a collection of US sites considering AP1000) was collated to calculate the frequencies for the pre-selected hazards. Any hazard event with an estimated frequency of occurrence of less than 10^{-7} /yr was screened out from the analysis. No relevance for UK sites of the data compiled is evaluated anywhere in the documentation provided. Also, the review found that this criteria had not been applied consistently for all the external hazards evaluated, for example for marine accident explosions a criterion of 1 Pound per Square Inch (psi) overpressure at a frequency of less than 10^{-6} /yr is adopted while a consistent screening value would be 1psi at 10^{-7} /yr. In any case, as the AP1000 internal events CDF claimed by Westinghouse is 2.13×10^{-7} /yr, a hazard frequency screening value of 10^{-7} /yr without further exploring potential impact on CDF and LRF, is inadequate for this reactor for the purpose of PSA.

262 For external event frequencies greater than 10^{-7} /yr, a quantitative evaluation was performed. External events with associated core damage frequencies that were shown to be less than 5.08×10^{-8} /yr (approximately 10% of the CDF from internal events, at the time when the analysis was performed) were also screened out from the analysis. It should be noted that Westinghouse has modified the CDF screening value to 10^{-8} /yr, however the results of the CDF evaluations for external hazards appeared to have been compared against the older screening value, which is considered inappropriate. In any case, as the AP1000 internal events LRF claimed by Westinghouse is 1.86×10^{-8} /yr, a CDF screening value of 10^{-8} /yr, without further exploring potential impact on LRF, is inadequate for this reactor for the purpose of PSA.

263 The review judged that the specific CDF evaluations for quantitative screening were optimistic for the following reasons:

- Loss of off-site power was assumed to be the bounding initiating event for all the external hazards evaluated. Westinghouse's Conditional Core Damage Probabilities (CCDP) were based on assumptions which are not realistic in general for external hazards, i.e. 1/2 hour off-site power recovery probability based on a full recovery in 2.5 hours.
- Westinghouse's sensitivity analysis performed in support of the screening of external flooding results in a CDF of 5.85×10^{-15} /yr assuming a flood frequency of 10^{-7} /yr. The PSA review team considered this evaluation to be extremely optimistic since it was based on the assumption that the initiating event due to external flooding is LOOP with failure of non-safety systems. Depending of the specific characteristics of the site, a flooding of a 10^{-7} frequency could lead to a much more severe scenario.

264 Based on the screening and selection criteria above, Westinghouse screened out all external hazards from the PSA, apart from seismic, for which a Seismic Margins Analysis was performed, rather than a Seismic PSA.

265 The RGA for this particular area of the PSA showed that the three external hazards screened-in for RGA, i.e. external flooding, external fire and extreme temperatures could have a small contribution to the CDF but not small enough to justify screening them out of the PSA.

> ***Assessment Finding AF-AP1000-PSA-046:*** *The Licensee shall provide a systematic screening of external hazards considering the specific characteristics of the site. The analysis should also address external hazards that could be correlated. The Licensee shall provide a demonstration that the risk associated with all the external hazards screened out would be insignificant compared to the AP1000 total risk.*

Assessment Finding AF-AP1000-PSA-047: *The Licensee shall provide a PSA for the external hazards and combination of external hazards that have been screened in according to the stated criteria. The analysis should address the potential for consequential internal hazards.*

4.13.4 Conclusions

266 From the information provided by Westinghouse in responses to relevant TQs, the outcome of my assessment and the results of the Risk Gap Analysis, I have gathered an understanding of the potential risk associated with external hazards (other than seismic) for the AP1000. My current belief based on the information evaluated and the assumptions of a generic nature made for the RGA is that the individual external hazards (other than seismic) may not be dominant contributors to the AP1000 overall risk. However, this conclusion is only relevant for a "generic" AP1000 PCSR PSA but it has no validity when dealing with site specific characteristics.

267 Therefore this part of the AP1000 PSA should be done again, when appropriate, utilizing site specific characteristics. The screening of external hazards should start from a complete list of hazards (see for example Annex 1 of IAEA Level 1 PSA Safety Guide, Ref. 17, or Table 1 of T/AST/013, Ref. 75) and should provide technically sound evaluation of the risk associated with them.

4.14 Level 1 PSA: Analysis of Hazards – Seismic Analysis (A1-2.7-4)

4.14.1 Assessment

268 My GDA Step 3 report (Ref. 6) established that Westinghouse had submitted a Seismic Margins Analysis (SMA) to address seismic risk. My report stated that this was not a Seismic PSA and could not be integrated with the rest of the PSA for overall evaluation of the risk. Also during GDA Step 3, my team estimated a preliminary LRF for the seismic event for the AP1000 using the information in Westinghouse's SMA submission (Chapter 55 of Ref. 21) and the seismic hazard analysis for one of the NPP sites in the UK. This resulted in a LRF associated with seismic events of the same order as the currently calculated LRF from internal events ($> 10^{-8}$ /yr). This preliminary evaluation took at face value the seismic fragilities assumed by Westinghouse in the SMA and it therefore required further scrutiny during GDA Step 4.

269 In GDA Step 4, I conducted a detailed review of some aspects of the AP1000 SMA submitted for GDA with the support of ND's External Hazards team. This review has put emphasis on the sampling of specific fragility derivations (expressed as High Confidence of Low Probability of Failure, HCLPF, for the SMA) documented in Ref. 76.

270 To give some focus to the sampling, ND's External Hazards and PSA teams jointly decided to examine the main building structures affecting in-containment plant and those items for which seismic failure was predicted to show a large contribution to the overall probability of failure across a range of initiating events. In addition, the squib valves were included because of their novel nature. Approximately half of the fragility calculations were examined.

271 An initial detailed review of the SMA was conducted by ND's PSA team early in Step 4. In response to queries and comments from this review Westinghouse submitted an update of the SMA (Ref. 77). This has been looked at in some detail, but, mainly, this information has been used to support the Risk Gap Analysis as described in the following paragraph.

272 To understand the potential risk gap in this area, ND's PSA team has performed a simplified and bounding seismic risk evaluation. The hazard curve chosen for this purpose represents a typical curve for a UK site. The structural and component fragilities used are based on revised values following a review of the calculations submitted by Westinghouse (Ref. 76). In addition, information from the seismic event trees submitted by Westinghouse in Ref. 77 has been used to quantify core damage frequencies from seismic events. It should be noted that the potential impact of other external hazards that could occur in correlation with seismic events has not been evaluated in the RGA.

4.14.2 Strengths

273 The level of seismic hazard chosen for the AP1000 SMA is 0.5g peak ground acceleration (pga) which is 1.67 times the level of the chosen 0.3g pga safe shutdown earthquake. The SMA seismic hazard value is high compared with the level for the design basis earthquake adopted in the UK seismic assessments (0.15 – 0.25g pga). This is a strength only regarding the Seismic Margins Analysis.

274 At GDA, Westinghouse has not attempted to claim any numerical benefit from the fact that the UK site-specific uniform hazard spectra may fall below the 0.3g pga spectra they have adopted in design. This may prove to be a significant conservatism and is hence acceptable for the purpose of SMA.

275 A number of methodologies have been utilised by Westinghouse to determine the majority of high confidence of low probability of failure (HCLPF) values for the AP1000. These include probabilistic fragility analysis and a conservative deterministic failure margin method (based on guidance in EPRI documents), test results, deterministic approach and the use of generic fragility data. These methods are considered acceptable in general for the purpose of SMA.

276 Since the HCLPF values were calculated a number of issues for the AP1000 have arisen, such as redesign of the shield building, improvement to the nuclear island modelling, effect of Hard Rock High Frequency (HRHF) seismic response and effect of basemat uplift. The effect of these issues has been addressed in various documents and shown to have negligible effect on the HCLPF values used in the SMA.

277 Event trees have been developed to determine the seismic initiating events. Fault trees have been developed for each function in the event trees to identify all the seismic failures which will lead to the identified initiating event. Event trees have also been developed for each seismic initiating event which does not lead directly to core damage. Fault trees have been developed (in CAFTA) for the various functions in the seismic event trees. These fault trees include random and seismic failures. The models supporting the 2010 update of the SMA are described in detail in Ref. 77.

4.14.3 Findings

278 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35, 78 and 79.

279 The following are the main methodological concerns raised during the review of the sampled seismic fragilities:

- A variety of methods have been used for fragility derivations. This is in principle acceptable, as discussed above. However, each of these methods has its own level

of conservatism which makes comparison of HCLPF values for different systems, structures or components difficult.

- My review team identified that for some components the probabilistic fragility analysis had not been applied systematically according to the chosen EPRI guidance document and as a result of this some variables had been omitted. It appears that some conservatisms in the analyses may have compensated the impact of the omission of variables. While this may be acceptable for the purpose of the SMA, I do not consider this to be an appropriate practice for Seismic PSA.
- Where generic fragilities have been used, reliance has been placed on the use of the Utility Requirements Document (URD) (Ref. 80). It has not been possible, to date, to confirm whether the principal reference within the URD for these generic fragilities has been formally published. Hence it has not been possible to confirm the context and suitability of this generic data to a particular item.
- The documentation of the fragility analyses are spread in several revisions of one report (Ref. 76) rather than being consolidated in the latest version. My review team considered this to be inadequate and could lead to configuration problems and errors in the future seismic analyses.

  Assessment Finding AF-AP1000-PSA-048: *The Licensee shall provide a consolidated report collating all the seismic fragility analyses and a process to update it in the future as required to address the concern raised by the GDA review.*

- All the fragility analysis results are presented in the form of High Confidence of Low Probability of Failure (HCLPF). All fragilities are assumed log normal in form. In a number of cases the fragility distribution is fully enumerated by the inclusion of median values and composite standard deviation. In the remaining cases only the HCLPF value is quoted. This is because the approach adopted by Westinghouse to derive HCLPF is aimed at demonstrating a seismic margin compatible with its target, not at deriving realistic fragilities for use in a Seismic PSA. The approach with its conservatism is acceptable for SMA but not for Seismic PSA. Provision of the standard deviation for all fragilities is necessary for the performance of the Seismic PSA.

280 The detailed conclusions of the review of the seismic fragilities are that some HCLPF values should be reduced in light of the comments raised. It is probable that for a subset of these, the HCLPF value will fall below the adopted target value of 0.5g pga. In these circumstances, it is likely that a more rigorous assessment would have to be undertaken to meet the adopted target. Part of this may involve claiming the probable benefit of site-specific uniform hazard spectra, when these are available for each site. Specific findings in this regard that may affect the current conclusions of the SMA are as follows:

- The latest version of Ref. 76 still has two open items referred to in the passive containment cooling system tank and the shield building fragility calculations. Therefore those fragility calculations have to be reviewed for accuracy when the missing information becomes available.
- For the fragility analysis of the steam generator support columns it appears that there is a numerical error in the calculation of modelling error on frequency variability. However, the HCLPF is considered likely to remain above the 0.5g pga target.
- The fragility analysis of the steel containment vessel and the Reactor Pressure Vessel (RPV) supports contain omissions of some variables. However, the HCLPF is considered likely to remain above the 0.5g pga target.

- The HCLPF values for electrical equipment have been calculated on the basis of future test data using a method that does not include any uncertainty on the scale factors and does not adhere to industry standard references. Also additional over test factors are claimed which will require substantiation.
- For the fragility analysis for the shield building steel composite cylindrical wall and containment interior structure and IRWST, the review team questioned the anchorage strength for plates. The HCLPF is considered likely to fall below 0.5g pga target after correction.
- The fragility analysis of the steam generator support columns and pressuriser contain omissions of some variables. The HCLPFs are considered likely to fall below the 0.5g pga target after correction.

281 Relay chatter has not been considered by Westinghouse in the SMA on the basis that solid state relays are inherently immune to mechanical switching discontinuities and hence do not need to be considered in the SMA. This may be acceptable in principle however the robustness of this claim needs to be confirmed during future stages of the AP1000 development since so called solid state relays can sometimes still include printed circuit board mounted relays as a final output stage.

282 So called “non-safety” systems have been excluded from the SMA which also means that fragility analysis has not been performed for them. It also means that possible consequential events (e.g. fires, floods) triggered by the initiating seismic event and originating in non-safety systems have not been identified in the SMA.

283 The results from the seismic risk evaluation performed by my assessment team have shown a core damage frequency of the same order of magnitude as the AP1000 CDF from internal events. This confirms preliminary views from our GDA Step 3 assessment that the seismic risk for the AP1000 could be potentially significant. It should be noted that the Risk Gap Analysis has used conservative assumptions including the use of a hazard curve judged to be typical for UK sites. The results of the Risk Gap Analysis in this area have shown the importance of conducting a best estimate Seismic PSA specific to the site, when appropriate.

> ***Assessment Finding AF-AP1000-PSA-049:*** *The Licensee shall provide a Seismic PSA for the site. The study should address other external hazards that could occur in correlation with the seismic events, and also induced internal hazards.*

4.14.4 Conclusions

284 This assessment has provided very important insights into the potential risk associated with seismic events for the AP1000. I conclude that the risk is potentially significant (in comparison with the risk from internal events) but is dependent on specific characteristics of each site. Therefore, I do conclude that no further work can be done by Westinghouse to enhance my understanding of this risk using generic site information. I do not consider that doing a detailed generic Seismic PSA within GDA would have much added value.

285 However, considering the potential risk significance of seismic events for the AP1000, a high quality Level 1, 2 and 3 Seismic PSA should be performed, when appropriate, taking into consideration, in as a realistic manner as possible, site specific characteristics and plant specific design.

4.15 Level 1 PSA: Low Power and Shutdown Modes (A1-2.8)

4.15.1 Assessment

286 A review of the AP1000 PSA task on "Low Power and Shutdown (LP&SD)" against the expectations in T/AST/030 was started during GDA Step 3 however my 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 PSA documentation 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 appeared to be included in the documentation of the AP600 PSA, but the applicability of AP600 information was not clear. In order to undertake a detailed assessment during GDA Step 4 Westinghouse was requested to provide a reconstruction of the study from the various sources of information.

287 Because of the above, the GDA Step 4 review of the AP1000 LP&SD PSA had to make use of several sources of information in addition to the AP1000 PSA documentation (Ref. 21). As anticipated, a key reference was the AP600 Low Power and Shutdown Assessment for Revision 4 of the AP600 PRA Levels 1 and 2 (Ref. 81) developed in 1995. The review also made significant use of Westinghouse's draft response to RO-AP1000-54 on Shutdown and Spent Fuel Pool Faults, raised by ND's Fault Studies team (Refs 82 and 83) and of the draft list of Design Basis Initiating Events for the AP1000 prepared by Westinghouse in response to RO-AP000-046 also raised by ND's Fault Studies team (Ref. 84).

288 The review conducted in Step 4 has confirmed that the AP1000 PSA model for low power and shutdown operating modes is based entirely on the AP600 model with some updates to account for plant differences. Therefore, a number of the findings discussed below are based on a review of the approach used for the AP600 PSA.

289 A Risk Gap Analysis has been performed to address the findings in this area and to understand their potential risk significance. As for other areas of the PSA, an initial screening of findings was conducted using qualitative arguments and applicable quantitative information from the PSA. This resulted in a list of those findings which were judged to have a non-negligible numerical risk impact. These were subject to further quantitative evaluation as follows:

- The LP&SD PSA model was modified to explicitly include the failure modes (including operator errors) leading to the Initiating Event "Over-draining".
- A bounding evaluation was performed to address the potential impact of maintenance tasks allowed by the Technical Specifications during drained and non-drained states.
- Relevant human error probabilities were modified to account for human dependencies.

290 It should be noted that in January 2011 ND received a revised response to RO-AP1000-054 (Ref. 85). Because of the late time of this submission it was not possible for ND's PSA team to revise the assessment of the LP&SD PSA in light of the new documentation.

4.15.2 Strengths

291 The LP&SD PSA for the AP600 follows an approach in line with that recommended in IAEA-TECDOC-1144 (Ref. 86) which is considered to be a modern standards approach to LP&SD PSA and is consistent with the expectations in T/AST/030 (Ref. 15). For example, AP600 plant operating modes and equipment availability are taken into

consideration when defining the Plant Operational States (POS) to be analysed; the applicability of initiating events to the various POS and the contribution of operator errors to initiating events is included. Event trees are presented for the AP600 with success criteria based on what appeared to be sufficient thermal-hydraulic analyses; frequencies of IEs are based on assumptions relating to the time in each POS. The operator response to initiators is based on the timing from the thermal-hydraulic analysis. Component unavailability data and common cause failure data are presented.

292 According to Chapter 54.1 of the PSA documentation (Ref. 21) the CDF for the AP1000 low power and shutdown states has been obtained by requantifying the cutsets resulting from the quantification of the core damage sequences for the AP600, with data updates reflecting design differences. However, this information is misleading since the AP1000 Shutdown PSA model reviewed in GDA Step 4 has actually been created and quantified in CAFTA. The existence of this model facilitated the review to some extent.

4.15.3 Findings

293 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35 and 87.

294 Six shutdown phases were originally considered which were finally apportioned into two plant operational states carried over to the LP&SD PSA. These are “non-drained maintenance POS” and “drained maintenance POS”. The review of this part of the study has concluded that the LP&SD POSs are not sufficiently justified as there is insufficient analysis to support the definition of each POS. For example, there is no detailed analysis or explanation describing the exact relationship between the phases of shutdown and the modes of operation, and the detailed characteristics of the POSs are not listed explicitly in any of the PSA references used.

295 Faults and initiating events during LP&SD are discussed in a number of the references used. However, a clear summary of the interaction between evaluation of POS and initiating events was not found in the documentation available.

296 Chapter 54 of the AP600 PSA documentation (Ref. 81) includes a table that lists the 10 initiating events used in the PSA together with their frequencies. With the exception of boron dilution, which is analysed elsewhere in the same report, there is no discussion of the process followed to identify all the possible initiating events that could occur in each of the operating modes included within each POS. Neither is there documentation of the screening process which leads to the elimination of all faults except the five considered in each of the two POSs.

297 The causes and specific contributions to each initiating event category are documented for the AP600 and are assumed to be applicable to the AP1000. Also, specific analysis of human actions leading to initiating events has been performed for the AP600 LP&SD PSA. However, my review team did not find anywhere in the AP1000 documentation a detailed comparison of these aspects between the AP1000 and AP600 or a justification of applicability of the AP600 analyses.

298 In the shutdown PSA initiating events are made up of a combination of component failures and operator faults. In the AP1000 PSA these have been combined into single basic events for use in the CAFTA model. This is considered a significant limitation of the LP&SD PSA as it means that dependencies between the initiator and the performance of mitigating systems cannot be correctly accounted for.

299 Although it appears that sufficient thermal-hydraulic analyses may have been performed to support the current list of initiating events modelled in the shutdown PSA, these analyses were performed for the AP600. Similar analyses for the AP1000 are reported in the European DCD, but the PSA has not been updated to take these into account. Also the review of the success criteria reported in Section 4.5 above has raised sufficient general concerns which are equally applicable for the LP&SD PSA. Therefore, the AP1000 LP&SD PSA will need to be updated with AP1000 specific analyses of sufficient scope and level of detail, and using up-to-date input decks for the relevant codes.

300 The causes and specific contributions to each initiating event category are documented for the AP600 and the IE frequencies modified for the AP1000. Although the frequencies for the AP1000 seem to be revised based on the profile of the operating cycle, there is no clear discussion of the derivation of the AP1000 IE frequencies from the AP600 analysis.

301 A distinct event tree for each initiating event identified is shown in the AP600 PSA documentation (Ref. 81). This report also includes a description of each event tree, success criteria, and modelling assumptions that may apply for specific initiating events. The UK AP1000 PSA report (Ref. 21) displays the event tree drawings without further explanation or justification of their applicability.

302 The systems fault trees in the LP&SD PSA model have not been reviewed in depth but a quick check at the AP1000 LP&SD PSA CAFTA model has identified the following:

- Limitations found in the review of the system models for the at-power PSA discussed in Section 4.7 above appear to be replicated in the LP&SD PSA model.
- An apparent error was found in the IRWST injection model. It appears that manual initiation of the gravity injection lines is required in the “Drained Maintenance POS”, however no corresponding HFE is included in this system fault tree.

303 The probabilities assigned to the basic events that represent unavailabilities due to testing and maintenance appear to be the same as those for the at-power PSA. This implies that the LP&SD PSA system models do not take into account the planned maintenance allowed by the Technical Specifications in LP&SD modes and which are performed at some stage during the outage cycle. This is incorrect and because of this the CDF is potentially underestimated.

> ***Assessment Finding AF-AP1000-PSA-050:*** *The Licensee shall provide a full scope, modern and well documented Low Power and Shutdown PSA specific for the AP1000.*

304 The RGA for this particular area of the PSA has shown that significant numerical gaps could be associated with the following items:

- The most significant contribution to the risk gap was the inclusion of maintenance activities permitted by the Technical Specifications in the plant operational state with drained RCS loop. It should be noted that this is not inconsistent with the results of Westinghouse’s evaluation of Point-in-time Risks during Shutdown Operational States submitted in response to a Technical Query raised by my team during GDA Step 4 (Ref. 88) and also described in Chapter 10 of the 2010 draft version of the PCSR (Ref. 12). This risk gap highlights the importance of using the PSA (by a future licensee) to ensure that the maintenance activities are scheduled and controlled in a way that ensures that the risk is kept as low as reasonably practicable at all times.
- An increase in CDF was observed when human dependencies were considered.

Assessment Finding AF-AP1000-PSA-051: *The Licensee shall implement a risk monitor (covering full power, low power, shutdown, reactor and spent fuel pool) and the necessary procedure/s to manage the risk at all times.*

4.15.4 Conclusions

305 Based on the outcome of this assessment, I have concluded that the current study is sufficient to support the AP1000 "generic" PCSR but falls far short of the requirements for a site specific PCSR.

306 As indicated in the previous paragraph the current Low Power and Shutdown PSA is inadequate to support further stages of the NPP development and an AP1000 specific study should be developed as part of the next update of the PSA (see Section 5 below).

4.16 Level 1 PSA: Spent Fuel Pool PSA (A1-2.8)

4.16.1 Assessment

307 Report "AP1000 PRA Spent Fuel Pool Evaluation" (Ref. 29) submitted to ND separately from the rest of the PSA, addresses the risk associated with the spent fuel pool. No high level or detailed review of this study was conducted during GDA Step 3. Instead, this has been done in Step 4.

308 The PSA performed for the AP1000 assessing the potential frequency of damage to fuel elements in the Spent Fuel Pool (Fuel Damage Frequency, FDF) is, in principle, a simplified bounding analysis. It covers the range of potential fuel loadings, resulting in the identification of three bounding sets of cooling requirements. The analysis is done considering the most pessimistic time available for manual restoration of cooling following loss of normal cooling.

309 The Spent Fuel Pool (SFP) PSA review has mainly been based on the information in (Ref. 29) and the CAFTA model for spent fuel pool fuel damage (Ref. 28). The review also made significant use of Westinghouse's draft response to RO-AP1000-54 on Shutdown and Spent Fuel Pool Faults (Refs 82 and 83), raised by ND's Fault Studies team and of the draft list of Design Basis Initiating Events for the AP1000 prepared by Westinghouse in response to RO-AP000-046 (Ref. 84) also raised by ND's Fault Studies team. The information required to assess the PSA was therefore found in several documents, some of which were only partially completed at the time of this review. These documents go some way in addressing some of the information requirements to support the PSA.

310 The review has been guided by the assessment expectations in Table A1-2.8 of T/AST/030 (Ref. 15). It should be noted that T/AST/030 does not include specific expectations for the assessment of a Fuel Pool PSA. However the review team found that table A1-2.8 (Low Power and Shutdown Modes) was adequate to support this review also.

311 A Risk Gap Analysis was performed to address the findings in this area and to understand their potential risk significance. The RGA quantitative evaluation was undertaken as follows:

- The SFP PSA model was modified to correct several errors and implement relevant review findings.

- Relevant human error probabilities were modified to account for human dependencies.
- The currently missing initiating events associated with criticality events are believed to be potentially important but could not be evaluated because the gap in knowledge about the potential evolution of the sequences was large enough to preclude a meaningful RGA.
- Internal and external hazards, currently missing from the study, were not evaluated in the RGA.

312 It should be noted that on 31st January 2011 Westinghouse submitted a revised response to RO-AP1000-054 (Refs 85 and 89). This includes a new PSA evaluation of spent fuel boiling frequency. Because of the late time of this submission, it was not possible for my team to revisit the assessment of the SFP PSA in light of the new documentation. However, it is understood that, when performing the new PSA analysis for the fuel pool, Westinghouse took into account some of the preliminary findings from the PSA review discussed in this and / or other sections of this report.

4.16.2 Strengths

313 The Spent Fuel Pool (SFP) PSA includes consideration of faults leading to potential fuel damage arising from loss of cooling from a wide range of events including failure of normal operating systems, pipe ruptures and leakage, and loss of electrical power.

314 Fault trees have been developed to evaluate the frequencies of the IEs “loss of normal cooling” and “loss of offsite power” and to model the mitigation systems. The complete model is integrated which results in the capability to handle the dependencies properly.

315 In most areas the bases for the assumptions and analysis are clear so that future updates and corrections are possible.

4.16.3 Findings

316 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Refs 34, 35 and 87.

317 A systematic description of all the configuration states of the SFP has not been provided. Westinghouse’s draft response to RO-AP1000-054 (Refs 82 and 83) provides relevant information for the draft PCSR and assesses the potential faults which can occur in the spent fuel pool. Although this is informative, and it facilitated the PSA review, it does not substitute the documentation requirements for a SFP PSA.

318 Limitations have been found in the PSA in relation to the definition of plant operational states and the identification of initiating events for the spent fuel pool. In fact, based on the final list of IEs included in the SFP PSA, the review team inferred that some sort of screening of POSs and initiating events had been done. However, no comprehensive screening analysis is presented in any of the documents reviewed. For example:

- Westinghouse’s draft response to RO-AP1000-054 (Refs 82 and 83) considers some faults in states not described in the SFP PSA, e.g. potential drain-down events through the Cask Loading Pit (CLP) or Fuel Transfer Canal (FTC). These faults, as well as potential drain-down events through RNS suction line breaks, have been screened out qualitatively without a justification that can be considered adequate for PSA purposes. In the PSA, no detailed information is provided on the various plant

configurations of the SFP with gate open to the CLP, and no assessment of potential specific faults that could occur in those plant operating states is included.

- There is extensive discussion in Westinghouse's draft response to RO-AP1000-054 (Refs 82 and 83) on the potential causes of criticality events, with varying conclusions on the frequency and boundary conditions under which they can occur. However, in the SFP PSA there is no evaluation of criticality faults or justification for screening out these events from the quantification of the FDF.
- Although some operator actions which could lead to initiating events (also called Type B HFEs) are considered, no information on any analyses carried out to support the identification of these HFEs has been included in the documentation reviewed.

319 The SFP PSA covers the range of potential fuel loadings, resulting in the identification of three bounding sets of cooling requirements. The analysis has been done using the most pessimistic time available for manual restoration of cooling following loss of normal cooling. Also, the timings for the recovery of cooling or water supply to the fuel pool are based on the time for the pool water to reach boiling point, however in the PSA the end state is damage to the fuel leading to release of fission products. A better representation of this condition would be the onset of fuel uncovery since the documentation provided shows that the differences between these two timeframes can be very large. In this regard, the success criteria used in the current SFP PSA are pessimistic and do not reflect the actual time available for restoration of cooling or supply of water to prevent fuel damage.

320 Fault trees have been developed to evaluate the frequencies of the IEs "loss of normal cooling" and "loss of offsite power" and to model the mitigation systems. A number of concerns have been identified in relation to these models; some examples are as follows:

- Fault tree models developed for evaluating the frequencies of the loss of cooling initiating events incorrectly include maintenance of the operating train as a contributor to the initiating event.
- Modelling of loss of cooling as the result of loss of offsite power is intended to include the station blackout scenario. The fault tree structure in the PSA does not model this correctly.
- Some failure modes appear to be missing, e.g. loss of inventory due to pipe rupture is included in the SFP fault tree; however rupture of common SFP cooling supply and delivery headers is not.
- In the fault tree for failure of the operating train of SFP normal cooling the failure of the operator to start the standby train is included in an incorrect place. Also the same HFE is used to represent both the operator error to start the standby train and the operator error to re-start the system following recovery of offsite power. However the human reliability analysis has not been conducted for the different scenarios.
- A single diesel generator run time (2.5 hours) has been used for all loss of power scenarios despite differences in recovery timing and continuing operation requirements.
- A mission time of 24 hours have been used to calculate failure probabilities on demand of some components (e.g. failure to close of manual valves following pipe rupture). This is incorrect.
- Initiating event fault trees models have not been provided and integrated in the SFP PSA for the IEs loss of component cooling water or loss of service water.

321 In case of loss of SFP cooling, six lines of defence are identified each of which requires operator intervention to restore cooling. The six operator errors modelled in the fault tree are treated as independent events. This is incorrect and is likely to lead to an underestimation of the Fuel Damage Frequency.

322 The RGA for this particular area of the PSA has shown that a significant numerical gap could be associated with the current lack of consideration of human dependencies, even taking into account the long times available for the operators to take actions.

> ***Assessment Finding AF-AP1000-PSA-052:*** *The Licensee shall provide a full scope, modern and well documented Spent Fuel Pool PSA for the AP1000, including evaluation of fuel damage, radioactive releases and consequences.*

4.16.4 Conclusions

323 Based on the outcome of this assessment, I have concluded that the current study is barely sufficient to help ND take a decision on whether a Design Acceptance Confirmation (DAC) should be granted. However GDA Issues raised from the criticality and fault studies assessments of the AP1000 Fuel Ponds (Refs 90 and 36) need to be addressed first and the responses will be key for my team to get a more complete understanding of the risk associated with this facility. For now, the limited Spent Fuel Pool PSA provided gives a degree of confidence that the risk will be low and any safety improvements that may be implemented as a result of the discussions with other technical assessment areas should reduce it further.

324 However this part of the AP1000 PSA needs significant enhancements to support further stages of the NPP development, i.e., a complete PSA for the AP1000 fuel pools should be developed as part of the next update of the PSA (see Section 5 below).

4.17 Level 1 PSA: Uncertainty Analyses, Quantification and Interpretation of the Level 1 PSA Results (A1-2.9)

4.17.1 Assessment

325 I started a review the AP1000 PSA task on “Uncertainty Analyses, Quantification and Interpretation of the Level 1 PSA Results” against the expectations in T/AST/030 during GDA Step 3.

326 My GDA Step 3 review identified that although Importance, Uncertainty and Sensitivity Analyses are presented in different Chapters of the PSA report (Ref. 21), the PSA documentation does not include a systematic description of all the sources of uncertainty. In response to several Technical Queries raised to address this area of analysis Westinghouse has committed to undertake relevant work during the next update of the PSA. However, without additional information it was not possible during GDA Step 4 to fully investigate whether the sensitivity and uncertainty analyses presented by Westinghouse had sufficient coverage of the uncertainties in the PSA, or whether any actions would be needed to reduce uncertainties that might have a significant (relative) impact on the overall risk.

327 However, a number of the findings presented in the various sub-sections in Section 4 of this report are implicitly associated with uncertainties in the PSA model and data. During GDA Step 4, some sensitivity studies were conducted by my team in the framework of the RGA to get a better understanding of the AP1000 risk associated with the identified uncertainties. This is discussed throughout Section 4 and it is not repeated here.

328 From a request I made Westinghouse did provide sensitivity analyses considering variations in the PSA reliability claims for the CCF of the software for the PMS and PLS platforms as well as for the failure of the DAS (Ref. 63). These showed that significant increases in these probabilities did have an impact on the risk but did not result in unacceptable risk levels.

329 The review of the quantification during GDA Step 3 raised concerns about the cut-off limit used for the PSA quantification. However this was based on the documentation provided in Ref. 21 which precedes the PSA model (version 3B) built in the CAFTA software submitted to ND for assessment in GDA Step 4. This model was attached to a calculation note (Ref. 25) which shows that the results of the PSA were quantified using a truncation limit of 10^{-14}. However, no justification for this cut-off value was provided. The adequacy of this has been considered during the review by conducting, in the framework of the RGA, a PSA (CDF and LRF) quantification using a lower truncation limit of 10^{-16}.

330 Apart from the above activities, no further assessment in this area was done during GDA Step 4 and the findings from GDA Step 3 therefore remain valid.

4.17.2 Strengths

331 Chapter 10 of the 2010 draft of the PCSR consolidated for GDA (Ref. 12) discusses some sources of uncertainty in the AP1000 PSA and their potential impact on the overall risk. Also a review of technical assumptions is presented. Finally a more comprehensive presentation of results is displayed and discussions are included. Without judging here the technical adequacy and completeness of this information, this was the first document seen in GDA that made an attempt to collate all this information in a more comprehensive manner for the version of the PSA reviewed (version 3B, Ref. 25).

4.17.3 Findings

332 My GDA Step 3 review raised concerns regarding the adequacy of the uncertainty analysis presented in Ref. 21 for the Level 1 PSA, including queries on the error factors assigned and the lack of consideration of the correlation between components using the same parameter. Having said that, during my GDA Step 4 review of the new version of the PSA (Ref. 25) it was seen that no uncertainty analysis had been undertaken on the new model, despite the fact that CAFTA has the capability to do this type of analyses.

> ***Assessment Finding AF-AP1000-PSA-053:*** *The Licensee shall provide justified probability distributions for all the basic events in the PSA and full propagation of parametric uncertainties thorough the model.*

333 As stated above all of the generic findings from GDA Step 3 remain valid. It should be noted that Westinghouse has provided, in responses to the relevant TQs, a commitment to address all the findings raised in this area.

> ***Assessment Finding AF-AP1000-PSA-054:*** *The Licensee shall provide a collated list of assumptions and sources of uncertainty in the PSA, a comprehensive set of sensitivity analyses and revised documentation of the AP1000 PSA results including discussions of the key areas of uncertainty and what is being done to reduce them (if necessary), and justification of the robustness of the PSA results.*

334 The RGA results in this area have proved that the truncation limit of 10^{-14} used for the quantification of the AP1000 PSA is sufficiently low. However, the PSA documentation should provide a formal justification for the cut-off value/s used in the PSA quantification.

Assessment Finding AF-AP1000-PSA-055: *The Licensee shall provide clarity on the cut-off/s used in the PSA quantification and justification of its / their adequacy.*

4.17.4 Conclusions

335 Based on the outcome of this assessment, I have concluded that the current model quantification together with the presentation of results in the draft Chapter 10 of the 2010 PCSR (Ref. 12) are sufficient for the PCSR PSA.

336 However, these aspects of the PSA need improvements for further stages of the NPP development. Thorough identification and documentation of assumptions, comprehensive sensitivity and uncertainty analyses and a proper presentation and discussion of the PSA results should be done as part of the next update of the PSA (see Section 5 below).

4.18 Level 2 PSA (A1-3)

4.18.1 Assessment

337 A high level review of the AP1000 Level 2 PSA against the expectations in T/AST/030 (Table A1-3) was conducted during GDA Step 3. This review raised general concerns in the following areas:

- Process to identify and select the attributes for the Plant Damage States (PDS), and transparency of the process to transfer Level 1 PSA information to the Level 2 PSA Containment Event Trees (CET).
- Traceability of the AP1000 Level 2 PSA model to the supporting MAAP4 analyses.
- Containment structural analyses: treatment of small penetrations and uncertainties and traceability of the analysis.
- Treatment of human dependencies between the Level 1 and Level 2 PSA.
- Transparency of the approach to CET nodal probability assignment.
- Source term grouping structure and quantification of release frequencies.
- Scope of the Level 2 study.

338 The objective of my GDA Step 4 assessment was to review, at a detailed level, the interface between the Level 1 PSA and the Level 2 (definition of PDS and allocation of Level 1 sequences to PDS), the Level 2 PSA containment event trees, the source term grouping structure, supporting MAAP4 analysis, containment structural analysis, detailed branch point quantification, model quantification, and scope issues.

339 My review was conducted in two phases. During the first phase the following tasks were undertaken:

- Development of a reassessment model of the AP1000 Level 2 PSA model with a separate computer tool (WinNUCAP, Ref. 91) that has an explicit graphical representation of the PDS grouping structure, as well as CET and source term modelling capabilities. This allowed a thorough examination of some of the concerns raised in GDA Step 3. It also facilitated rapid and systematic examination of model sensitivity to support prioritisation of later review tasks. Two sets of sensitivity analyses were carried out involving changes to the CET nodal probabilities and changes to PDS frequencies.

- Detailed review of PDS grouping structure and assignment of Level 1 sequences to groups. Identification of potential impact of alternative allocation of sequences to groups or an alternative grouping structure. For each PDS identified by Westinghouse, an identification of apparently misallocated sequences was carried out.
- Assessment of the CET structure, including identification of top events and treatment of dependencies within the CET. The results were then used to prioritise the later review of supporting analyses and branch probability evaluations.
- Assessment of the adequacy of the source term grouping structure.
- Review of CET / PDS quantification and impact of dependency modelling covering areas such as human dependencies and sequence timing dependencies.
- Model sensitivity: During this task my PSA review team looked at the scope of Westinghouse's sensitivity studies for the AP1000 Level 2 PSA and identified model sensitivities not addressed by Westinghouse. This also helped to define the scope of the detailed review during the next phase (MAAP4 calculations, phenomenological probabilities, containment structural capability, and source term analysis).

340 During the second phase an in depth assessment was conducted of specific aspects of the Level 2 analysis selected for thorough examination during phase 1 of the Level 2 PSA Step 4 review. In particular, the following work was done:

- Review of the Hydrogen Combustion Phenomena: this review covered two areas, i.e. Westinghouse's analysis of containment failure due to diffusion flame heating of the containment steel shell, and the analysis of detonation, both presented in Chapter 41 of the PSA (Ref. 21).
- Review of Westinghouse's analysis of the phenomenological failure of In-Vessel Retention (IVR) as reported in Chapter 39 of Ref. 21: In-vessel retention of molten core debris via water cooling of the external surface of the reactor vessel is a severe accident management feature of the AP1000. Retaining the debris in the reactor vessel protects the containment integrity by preventing ex-vessel severe accident phenomena, such as ex-vessel steam explosion and core-concrete interaction. The AP1000 design contains features that promote external cooling of the reactor vessel. The AP1000 Level 2 PSA model considers that IVR will be successful for low pressure sequences, provided the vessel has been externally flooded by the time of relocation of core materials to the lower head. Chapter 39 of Ref. 21 presents a description of the analysis performed by Westinghouse which consisted of a Monte Carlo simulation of the defined core melt scenario taking account of some uncertainties. My review team carried out a reassessment of the IVR probability of failure. For this, a Crystal Ball (Ref. 100) based reassessment tool was developed which modelled the relevant heat transfer processes, and had the capability to represent uncertainties using Monte Carlo simulation. The sensitivity of margin to failure to key parameters (decay heat, material masses, etc) and other uncertainties not considered in the Westinghouse study were also investigated.
- Independent calculations of containment pressure response were also conducted using a simple MELCOR model constructed for this purpose by my assessment team. The calculations were limited to so-called "dry containment" scenarios in the Level 2 PSA. The principal aims of these calculations were two-fold. The first aim was to assess the technical basis behind the conditional probability of late (after 24 hours) containment failure versus intermediate (before 24 hours) containment failure for

sequences involving failure of passive containment cooling. The second aim was to determine the extent to which peak containment pressure is sensitive to accident sequence characteristics and to modelling parameters affecting natural convection heat transfer to air in the baffle region outside the containment shell. The results of these calculations were compared to MAAP4 results described in Chapters 34 and 40 of the AP1000 PSA (Ref. 21).

- It is to be noted that the issue of containment pressurisation after failure of passive containment cooling is relevant to both the Level 1 and Level 2 PSA models due to the treatment of so-called “late containment failure” end-states in the Level 1 PSA. These end-states are labelled “LCF" in Level 1 and not treated further; their frequency is not added to the CDF or LRF nor are they transferred to the Level 2 PSA. It was convenient therefore to review this issue within a single task of the review, and it was decided to place that task within the Level 2 PSA review, although the conclusions also impact the Level 1 PSA.
- Review of the fault tree models for systems involved in the Level 2 PSA: this review task looked in detail at the Containment Hydrogen Control System (Hydrogen Igniters) and the Containment Isolation System.

341 In parallel to the above activities, the containment structural analysis for the Level 2 PSA was also reviewed in detail. This addressed the following:

- Identification of failure modes included in the overpressure analysis, also addressing assessment of the size of failure.
- Best estimate failure pressure presented for each failure mode, including any degree of optimism or conservatism in the supporting analysis
- Modelling of penetrations, including local stress intensity under pressurization close to ultimate strength, potential for failure of the penetration caused by large horizontal or vertical movements at pressures greatly in excess of design pressure (close to global ultimate strength) or other failure mechanisms. Adequacy of representation in ANSYS (for example, representation of smaller penetrations) and acceptability of any simplifications in the modelling.
- Temperature effects, especially around seals and penetrations, and the analysis and justifications presented by Westinghouse.
- Derivation of uncertainty parameters for the modelled failure modes.

342 It should be noted that in GDA Step 3 it was considered that it would be a useful input to the detailed Level 2 PSA assessment during GDA Step 4 if confirmatory analyses with a different code (MELCOR) of some selected AP1000 severe accident sequences were conducted. At that time 10 scenarios were selected and provided to ND’s Fault Studies team to be followed up with the appropriate TSC. The scenarios covered a variety of sequences to explore various aspects of particular interest for the Level 2 PSA review, for example:

- One of the cases requested was a core damage scenario starting from a spurious opening of 2 ADS Stage 2 valves (equivalent to a Medium LOCA in the pressuriser). In this case, the interest was to explore the evolution of the PDS 1D accident sequences. PDS 1D is composed of sequences with success of partial ADS without LOCA. In the PSA, PDS 1D has been grouped with PDS 3D which is composed of LOCA sequences with success of partial ADS, i.e., a larger total break size. The PSA review team wished to clarify the adequacy of this grouping.

- Another case selected was a 2” LOCA scenario with failure of PRHR and failure of full depressurisation via ADS Stage 4. Here the intention was to check whether IRWST could refill the vessel, and whether this would be before core damage, after core damage or after vessel failure.

During Phase 2 of the Level 2 PSA review a number of interactions were held to discuss the details of these analyses. Unfortunately, at the time in which the Level 2 PSA review team needed this input, results were not yet available. As a result, the review could not address certain aspects of the severe accident progression analysis, and the review of the source term analysis had to be undertaken with a different strategy. Nevertheless, the results of the confirmatory analyses for the scenarios originally selected have proved useful for the separate assessment of the AP1000 severe accident analysis. This is reported in Ref. 27.

343 The absence of detailed information in Ref. 21 about the source term calculations and the absence of independent confirmatory analyses with MELCOR for the AP1000 limited the scope of the review of the AP1000 PSA source term analysis. The scope was therefore as follows:

- Consistency of source term analysis information throughout the PSA documentation. All cases checked showed consistent results.
- Confirmation of consistency between the release fractions listed in relevant tables in Chapter 45 of Ref. 21 and data points on time-dependent plots from the MAAP4 calculations. All cases checked showed consistent results.
- The release fractions for a few selected sequences (for which such a comparison was considered meaningful) were compared against those calculated by MELCOR for the AP600 (Ref. 97). Good consistency was confirmed. However, the scenarios chosen were the only two scenarios that share similar features to permit a direct comparison. Therefore, this should not be taken as an overall confirmation of the robustness of the MAAP4 source term analyses for the AP1000.

344 Another piece of work done during my GDA Step 4 review of the Level 2 PSA was in support of ND’s Severe Accident and Chemistry assessment teams who raised concerns in relation to Westinghouse's analysis of In-Vessel Retention (IVR). In response to RO-AP1000-068 raised by the Severe Accident Assessment team, Westinghouse presented an updated containment event tree model considering different assumptions about the success criteria for IVR, and a re-evaluation of the frequency of “wet” and “dry” Reactor Coolant System (RCS) scenarios. Westinghouse’s response to RO-AP1000-068 was reviewed by my team. The results of this review were provided to ND’s Severe Accident and Chemistry assessment teams, and they are also discussed in Sections 4.18.2 and 4.18.3.2 below.

345 As for other PSA areas, the Risk Gap Analysis for Level 2 was carried out in two steps. First an initial identification and screening of issues to consider in the RGA was conducted. The screening was based on qualitative and quantitative factors. The items identified in the screening step were analysed to establish how they should be addressed in the RGA. This is discussed in the following examples:

- Level 2 PSA items explicitly modelled in the BC RGA Model were:
    - Explicit inclusion of IVR failure probability (a value of 3×10^{-4} was used).

- Changes to the containment isolation model by increasing the HEP for the HFE to manually isolate the containment following Large LOCA to account for shorter time window.
- Modifications to the models for systems required as part of the success criteria for IVR.
- Consideration of human dependency between the HFE to manually actuate Hydrogen Igniters and other HFEs prior to this.
- Consideration of dependency between the HFE to depressurise the RCS after the onset of core damage and the preceding human actions.
- Consideration of other human dependencies.
- Correction of PDS grouping errors.

- A number of findings from the review of the Level 2 PSA were evaluated in the RGA via sensitivity analyses:
  - Sensitivity of the LRF to the IVR failure probability (values of 4.4×10^{-3}, 2.1×10^{-2} were used)
  - Sensitivity of the LRF to the HEP to back up the containment isolation.
  - Sensitivity to variations in the hydrogen detonation probability; effects of elevated temperature challenge to containment integrity.
  - Contribution to LRF from un-isolated steam line break sequences.
- A number of findings from the review of the Level 2 PSA which had been screened-in for RGA were finally not included; they were either screened-out in re-evaluation or there was a gap in knowledge at the time of the assessment, and which would require efforts beyond the available resources for it to be addressed. One of these was related to the modelling of the configuration of the power supplies in the fault trees for the Hydrogen Igniters, which was excluded due to lack of information on the actual power supply configuration.

4.18.2 Strengths

346 In general, the Level 2 PSA is the soundest part of the AP1000 PSA.

347 Generally the PDSs were felt to be a good representation of the possible states of the plant arising, although there were some specific findings discussed in Section 4.18.3.1.

348 The CET developed by Westinghouse is a good representation of the accident progression and appears to capture the main severe accident issues relevant to the AP1000. However, the CET conservatively simplifies the treatment of high pressure sequences and failed In-vessel Retention scenarios (as discussed below in Section 4.18.3.4) which is an aspect for future improvement.

349 Issues related to hydrogen combustion following failure of the Hydrogen Igniters were well treated. A range of scenarios were analysed for Deflagration-to-Detonation Transition (DDT) and a number of scenarios were checked for a potential diffusion flame heating of the containment shell.

350 The Source Term Category (STC) grouping review did not identify any grouping errors. However, as identified earlier in GDA Step 3, the grouping does not provide a high level

of discrimination of issues impacting the source term other than release timing and bypass versus non-bypass status – this concern remains valid.

351 To the limited extent it was possible to check source term analyses; good internal consistency of the results presented was seen.

352 In the review of the AP1000 containment structural analysis for the Level 2 PSA the following strengths are highlighted:

- Various methods of varying degree of sophistication have been employed by Westinghouse to perform the analysis, but in terms of steel containment ultimate pressure capacity estimates, all meet industry standards.
- The loads and combinations of loads studied are clear. Temperature effects have been adequately addressed.
- The material properties assumed are realistic.
- Uncertainties associated with the capacity of the containment under extreme loads have been identified explicitly and have been appropriately treated.

353 In relation to Westinghouse's response to RO-AP1000-068 (Ref. 92), it was judged that:

- The overall structure of the CET model provided by Westinghouse was reasonable.
- The documentation provided was, in general, of good quality.
- Westinghouse's classification of the IVR end states into success and fail cases, noting the modelling assumptions regarding in-vessel debris bed configuration (and also noting that Westinghouse's opinion is that these are conservative), was considered to be sound. This conclusion is maintained notwithstanding findings discussed in Section 4.18.3.4 below.
- The conclusions drawn from the supporting MAAP4 analysis were believed to be reasonable.

4.18.3 Findings

354 The detailed technical reviews that support the findings discussed in the following sub-sections are documented in Refs 34, 35, 93, 94 and 95.

355 In addition to the specific findings for each technical area of the Level 2 PSA discussed in the sub-sections below, it should be noted that in response to TQs that I raised Westinghouse made some commitments to address identified shortcomings. Also, Westinghouse provided relevant technical information which should be formally included in the PSA documentation.

> ***Assessment Finding AF-AP1000-PSA-056:*** *The Licensee shall provide revised documentation of the Level 2 PSA taking into account commitments made and relevant technical information provided in responses to TQ-AP1000-334 to 348, 570, 757 to 759, 780 to 786, 1059, 1100, 1195, 1249 and 1250.*

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

356 The review raised some concerns regarding the identification, characterisation and grouping of PDS. Some examples are discussed in the following bullet points:

- A number of core damage sequences with failure of partial depressurisation have been assigned to the same PDS despite the status of the CMTs and / or the Accumulators. Westinghouse did not provide sufficient information to clarify whether success or failure of CMT and Accumulator injection are significant or otherwise for the accident progression in Level 2. For example, no discussion was provided about the time at which core damage occurs and corresponding decay heat levels with different combinations of CMT and Accumulator success or failure. This is not to say that some of these sequences have been assigned to the wrong PDS or that the PDS structure is not sufficiently discriminatory, however, it shows a shortcoming in the process, and in the documentation of the process, for the development of the PDS definitions.
- The review of the Level 2 CET and Level 1 - Level 2 interface showed that PDS 1D and PDS 3D had been lumped together and treated as a single, equivalent PDS. PDS 3D is characterised by successful partial ADS in conjunction with a Small or Medium LOCA. The CET model assumes that the corresponding core damage sequences are depressurised. PDS 1D is characterised by successful partial ADS with no other RCS opening (LOCA). The CET model also assumes that the corresponding core damage sequences are depressurised, since PDS 1D has been treated together with PDS 3D. The minimum requirement for success of partial ADS in the PSA models is the opening of 2 stage 2 or 3 valves, which corresponds to an opening equivalent to a Medium LOCA; in the Level 2 PSA Medium LOCAs without additional depressurisation are grouped as PDS 1AP, which is a high pressure PDS. Therefore it could be expected that PDS 1D would be a high pressure PDS (similar to PDS 1AP) and therefore its grouping under a low pressure PDS could be optimistic. Westinghouse did not offer a clear explanation about how the analyses support the classification of these sequences, or a justification for this apparent optimism.
- The review team felt that the AP1000 PSA model would benefit from specific separation into different PDSs of ADS Stage 4 spurious openings from LOCAs due to pipe breaks. This is because the current structure of the PDS makes it difficult to separate scenarios where re-flooding of the RCS can occur via a break in the loop from cases where the depressurisation was via stage 4 of ADS, implying that the RCS cannot be re-flooded via the break. Similarly, it may be beneficial to create specific PDS for Direct Vessel Injection (DVI) line break sequences, as there are some specific modelling differences for these cases also.

  Assessment Finding AF-AP1000-PSA-057: *The Licensee shall provide revised documentation of the interface between the Level 1 and Level 2 PSA including clear characterisation of the Plant Damage States (PDS), and description and justification of the final PDS groups and the process for their development.*

357 The review raised some concerns and identified some errors in the allocation of core damage sequences into relevant PDSs, i.e. in the transfer of the information from the Level 1 PSA event trees to the Level 2 PSA models. Examples of the identified findings are discussed in the following bullet points:

- The review considered that the assignment of one of the sequences in the event tree for Steam Line Break Upstream of the MSIVs (SLB-U) to PDS 1D was optimistic since there is no opening of the RCS in this sequence and PDS 1D is treated as a low pressure case. In addition queries were raised about the possible containment challenges in SLB-U sequences inside containment with return to power. Although the cumulative total frequency of the sequences of concern is low, this does not

change the requirement that the basis for their treatment should be well documented and appropriately justified.

- I requested Westinghouse to explain the modelling of containment isolation failure in the Level 2 PSA for sequences initiated by SLB-U with failure of main steam line isolation specifically considering the possibility of an isolation failure path via the steam lines. Westinghouse's response indicated that the modelling following PDS 5E (steam line break) was not important due to its low frequency. The conclusion is that, although numerically a small issue, the Level 2 PSA model should be complete and if a particular PDS is unimportant numerically it would be more appropriate to bound it by worst case modelling, as this gives a clear demonstration of low importance, and, importantly, means that the impact of the PDS will be picked up in future PSA revisions, if its frequency increases.
- My review queried the treatment of the PDSs arising from loss of offsite power and from steam line break core damage sequences. Westinghouse's response was not consistent with the treatment in the AP1000 Level 2 model. The response stated that sequences with steam line break and failure of steam line isolation are treated as early containment failure but this did not appear to be the case according to the end state classifications shown in Chapter 4 of the PSA (Ref. 21) or the CAFTA model (Ref. 25). Furthermore, Westinghouse did not offer a convincing justification for the current treatment of loss of offsite power sequences in the Level 2 PSA. The review therefore concluded that 1) there is a documentation gap in the AP1000 Level 2 PSA with regard to the treatment of loss of offsite power sequences and steam line break sequences, and 2) the treatment of these sequences may be inadequate and should be reviewed or updated. On further review my team eventually found that the specific PDSs for steam line break and loss of offsite power were not linked into the Level 2 PSA model at all, which is an additional concern.
- A question was raised in relation to the treatment in the Level 2 CET of the core damage sequences involving successful containment isolation and failure of sump recirculation (1 line closed) and core damage sequences with failure of containment isolation and failure of sump recirculation (both lines closed). The concern here was that all those sequences are grouped into a PDS 3BL despite the different configurations regarding status of containment isolation and recirculation lines (valves), and it was not clear how consistent treatment in the Level 2 model had been ensured. Westinghouse was not able to clarify this.
- In the opinion of my review team, SGTR sequences with failure of isolation of the damaged steam generator should be directly allocated to large release instead of being allocated to PDSs (as in the current model) where successful depressurisation is credited as a means to avoid large release. It should also be noted that depressurisation as a means to avoid large release would not be valid for any interfacing system LOCA sequences grouped into the same PDS as these SGTR sequences.
- It was noted that a number of ATWS core damage sequences were assigned to PDS 3D, which arises elsewhere when a small or medium LOCA initiator is combined with success of partial ADS. It was not clear that the equivalent opening in these sequences was sufficient to justify the classification as PDS 3D (low pressure) rather than 1AP (which would be a high pressure sequence). Westinghouse accepted that the ATWS sequences with failure of header "PRSOV" were wrongly allocated.

Assessment Finding AF-AP1000-PSA-058: *The Licensee shall provide a revised analysis of the interface between the Level 1 and Level 2 PSA addressing the specific shortfalls identified in the GDA review regarding allocation of Level 1 PSA sequences into Plant Damage States and transfer of PDSs into the Level 2 PSA models.*

358 As briefly mentioned in Section 4.6 above, a Technical Query (TQ) was raised regarding the sequences in the Level 1 PSA event trees with an associated consequence called Late Containment Failure (LCF) caused by failure of containment heat removal, which are not added to the CDF. The TQ concerned the capability of the containment to remove sufficient decay heat in the event of failure of the Passive Containment Cooling System (PCS), i.e. with a dry shell. Failure to remove sufficient decay heat via the containment shell could lead to the internal containment pressure raising above a value which could cause containment failure and consequent core damage. A brief discussion clarifying why this issue is relevant to Level 2 as well as Level 1 PSA is provided in Section 4.18.1. Westinghouse's response was supported by a White Paper addressing each question raised in ND's TQ. This response is discussed in some detail in the following bullet points:

- The Level 1 PSA currently assumes success (no containment failure or core damage) if PCS fails but core damage had otherwise been avoided.
- The containment pressure response for sequences with air cooling and failure of the PCS is discussed in Chapter 40 of Ref. 21, which presents containment failure probabilities for the dry shell situation at 24 and 72 hours. In this regard, the Level 1 PSA model and the Level 2 PSA documentation are inconsistent, since the Level 1 effectively assumes no impact of PCS failure on the CDF.
- The White Paper presented a first principles heat balance calculation assuming that the containment would not be challenged before 48 hours, using the decay heat at 48hr and equating this to the required heat flux at the shell that balances decay heat input. A relation between heat flux and containment internal pressure derived from test results was then used. The pressure derived from this procedure was less than the median containment failure pressure and Westinghouse took this to imply that the containment would not fail. It is not valid to argue in PSA space that if the pressure remains below the median failure pressure, then the probability of containment failure is zero. This evaluation does not therefore prove that the containment will not fail given failure of PCS cooling.
- The White Paper also presented a benchmarking of MAAP4 against the Large Scale Test Facility (LSTF) tests from which it was concluded that MAAP4 can be used to predict shell heat transfer and containment pressure. It was also indicated that two relevant changes have occurred since the MAAP4 analysis of Chapter 40 of Ref. 21 was performed. Some cases using updated MAAP4 models are described which indicate containment threatening pressures by 72 hours or before. Therefore MAAP4 appeared to predict that containment failure would eventually occur.
- Westinghouse also presented sensitivities to the opening area at PCS inlet to downcomer, to simulate blockages which showed a relatively small effect on containment pressure. Based on this Westinghouse concluded that the heat removal capability was only a relatively weak function of air velocity. My team looked at the parameter file and observed that the parameter varied to simulate blockages was not the limiting one and so the small sensitivity observed was not surprising. It was concluded that the lack of sensitivity of the containment pressure to blockages in the

air had not been demonstrated by Westinghouse. This conclusion (that lack of sensitivity has not been demonstrated) is supported by the results of a simplified MELCOR analysis of sequences with air cooling, described in Section 4.18.3.2 below, which suggest that sensitivity would be expected.

- Based on all the above, it was considered that Westinghouse had not shown that containment failure would not occur in sequences with a dry shell. Therefore, it is considered that, without additional recoveries, core damage would be expected in these scenarios, implying that the LCF sequences should be added to the CDF and transferred to the Level 2 by assigning an appropriate PDS. The treatment of LCF sequences in the PSA does not appear justified.

  Assessment Finding AF-AP1000-PSA-022 (same as par 137 above): *The Licensee shall provide revised PSA event trees where the Late Containment Failure sequences are treated as core damage sequences and are transferred to the Level 2 PSA.*

359 The evaluation of Westinghouse's responses to the Technical Queries raised from my GDA Step 3 review of the interface between the Level 1 and the Level 2 PSA concluded that the general concerns raised were valid, e.g.:

- Lack of visibility of the process to define PDSs and of the identification (inclusion / exclusion) of PDS parameters and the rationale for the final PDS groups. It is also to be noted that my review team found the dual naming of the PDSs confusing.
- Lack of treatment of human dependencies between the HFEs before and after core damage.

  Assessment Finding AF-AP1000-PSA-059: *The Licensee shall provide a revised PSA including treatment of dependencies between the human actions before and after core damage.*

360 Incompleteness of the model was already identified in GDA Step 3, i.e. sequences from the internal hazards and shutdown models are not linked to the Level 2 PSA model and neither are they added to the overall results. This is also discussed in Section 4.2 above.

4.18.3.2 Level 2 PSA: Deterministic Accident Progression Analysis (A1-3.2)

361 Three aspects of the phenomena involved in the severe accident progression were examined in detail during GDA Step 4, i.e. Hydrogen Combustion Phenomena, In-Vessel Retention and Dry Containment Pressure Response. These are discussed in turn in the following paragraphs.

362 The review of Westinghouse's analysis of containment failure due to diffusion flame heating of the steel shell documented in Chapter 41 of Ref. 21, and the conclusions from this review are discussed below:

- The implied mechanism for a diffusion flame is hydrogen release to a location in the containment where hydrogen would naturally accumulate to high concentrations (without combustion occurring, for example due to high steam concentrations and lack of oxygen within small compartments where hydrogen could be released) and subsequently vent to a region with flammable conditions. Westinghouse's analysis identifies and assesses scenarios where this can occur. Well-mixed regions of the containment were excluded from consideration, since, if flammable, deflagration is likely and this is treated elsewhere. My review team however considered that it would seem conceivable to generate a diffusion flame from a "well-mixed" region in which

steam is gradually removed. For example, migration of a well-mixed steam and hydrogen mixture to the containment wall might gradually create a locally-high concentration of hydrogen near the wall as steam condenses. This might create a sufficiently high concentration of hydrogen to drive a diffusion flame near the wall. A discussion of this phenomenon and why it was ruled out would be useful. It should be noted that Westinghouse has indicated that they can provide arguments to discount this scenario.

- In general it was noted that the traceability of the analysis to specific supporting analyses or references was weak. For example, in other parts of Chapter 41 of Ref. 21, the AP600 analysis is specifically identified as the source but that is not done specifically in the case of diffusion flames so it was not clear whether the AP600 analysis was the actual source. Westinghouse has subsequently clarified that the diffusion flame analysis is specific to the AP1000.
- Chapter 41 of Ref. 21 identifies a scenario following DVI line break where oxygen starvation in lower compartments leading to a standing flame rising through the stairway, could heat the shell. This scenario has not been followed through in the numerical quantification and an explanation for its omission was not found. Information offered by Westinghouse suggested that a modification had been made in the positioning of the hooded vents to design out this scenario. This was not apparent from the documentation reviewed.
- For the quantified diffusion flame scenarios where partial ADS discharges through the IRWST, the review found that 1) the success criteria used was unclear and not traceable to references; 2) there was a discrepancy between the success criteria used for calculation of the numerical probability of insufficient pipe vents opening and the originally stated success criteria, since the calculation assumed failure would occur if 2 pipe vents failed to open whereas the originally stated criteria assumed that failure would occur if only 1 pipe vent failed to open; and 3) Westinghouse used the same probability value for a pipe vent failure to open as for a hooded vent failure to reclose, which did not seem correct.

  Assessment Finding AF-AP1000-PSA-060: *The Licensee shall provide revised documentation of the diffusion flame phenomena in the Level 2 PSA. This should include clarification and justification of the scope of the scenarios considered and the analysis undertaken, and justification of the relevant success criteria and failure probabilities for venting mechanisms.*

363 The review of Westinghouse's analysis of Hydrogen Detonation documented in Chapter 41 of Ref. 21, and the conclusions from this review are discussed below:

- The basic method used to assess Deflagration-to-Detonation Transition (DDT) is generally reasonable, as are the various simplifying assumptions. However, the conditional probabilities of DDT used in the AP1000 model are taken directly from AP600 analysis. A separate supporting document performs some DDT calculations for the AP1000, but these results do not appear to have been used. They also show a strong dependence on the calculation method used. Having said that, a single specific case checked by my team showed reasonable consistency which provides confidence. Even if this may suggest that DDT probabilities are comparable for the AP1000 and AP600, it would be better to have an AP1000 specific analysis of DDT. One potential concern about using the AP600 analysis for AP1000 in this area is the technical basis for scaling deterministic analysis of hydrogen concentrations in the containment from AP600 to AP1000.

- For the DDT calculations Westinghouse used the Sherman-Berman methodology. This methodology has been well accepted but can be considered as somewhat dated, and has limitations. For future PSA revisions, the methodology should be reviewed against more recent references to show that it still gives acceptable results.

  Assessment Finding AF-AP1000-PSA-061: *The Licensee shall provide revised analysis of the hydrogen phenomena in the Level 2 PSA specific for the AP1000 and using an updated method.*

364 My review of Westinghouse's analysis that supports the probability assignment for the phenomenological failure of In-Vessel Retention (IVR) documented in Chapter 39 of Ref. 21 was mainly done by comparison with independent calculations performed by my review team. This is discussed in the following bullet points:

- The base case reassessment undertaken by my review team showed that when a more complete set of parametric uncertainties was considered, small probabilities of phenomenological failure of IVR were generated. This was the case even in the absence of specific assumptions about top metal layer thinning.
- A number of sensitivity cases were carried out to investigate the impact of various parameters, including a few cases which were proposed by ND's Chemistry Team. The sensitivity cases were chosen with the objective of providing insights into which parameters may most strongly impact the probability of failure, but no appraisal of the relative likelihood or credibility of the various scenarios themselves was carried out. The key results of the sensitivity cases were:
  - The probability of IVR failure remained below 1% in most of the sensitivity cases analysed.
  - Decreases in the probability of IVR failure were seen in some scenarios. In particular, it was noted that the margins to failure were considerably greater when variations of decay heat throughout the operating cycle were considered.
  - The results showed sensitivity to Critical Heat Flux (CHF) and decay heat (decay heat escaping as volatiles). Westinghouse's model for IVR does not contain an uncertainty distribution for CHF.
  - One case, the 30 cm metal layer, resulted in a 100% probability of failure. The importance of this result depends on the credibility of the postulated scenario, i.e. on the probability of the 30 cm metal layer occurring.
- From the results of the sensitivity cases, in particular the insights related to the metal layer thickness, it is considered important to note that the current Level 2 PSA does not include a probabilistic assessment of alternate debris configurations leading to thinner top metal layers. This is considered to be gap in the AP1000 Level 2 PSA. It should be noted that Westinghouse contends that thinned metal layer scenarios are highly improbable or impossible for the AP1000.
- Given the above points, I believe that, for the purposes of a Level 2 PSA, the analysis presented by Westinghouse is not sufficient to support the assignment to guaranteed success of all the sequences where there is adequate external reactor vessel flooding, as in the current AP1000 Level 2 PSA model. In a future PSA update Westinghouse should produce an improved assessment of the probability of failure of IVR for the Level 2 PSA. This should address the missing uncertainty distributions and include an assessment of the probability of metal layer thinning due to formation

of a three layer debris bed. The Level 2 PSA model should then be expanded, as appropriate, to account for the additional sequences.

- Finally, it should be noted that in response to RO-AP1000-068 Westinghouse has presented a modified CET to address concerns raised by ND's Severe Accident and Chemistry Assessment teams in relation to IVR. This has been assessed by my team. The results of this review are discussed in Section 4.18.3.4 below. Comments on the relevance of the modelling approach used in Westinghouse's modified CET to the future updating of the Level 2 PSA are included in Section 4.18.3.4 below.

  Assessment Finding AF-AP1000-PSA-062: *The Licensee shall provide a revised analysis of the probability of failure of IVR for the Level 2 PSA addressing the missing uncertainties and including an evaluation of the probability of metal layer thinning.*

  Assessment Finding AF-AP1000-PSA-063: *The Licensee shall provide a revised Level 2 PSA model expanded to account for additional IVR failure sequences.*

365 My team's evaluation of the dry containment pressure response included the performance of several calculations to examine the global containment pressure and temperature response to a postulated Medium LOCA. All calculations assumed failure of the PCS. Several sensitivity calculations were also conducted examining the effects of ambient temperature, IRWST drain to the RPV versus to the reactor cavity, and sensitivity to modelling parameters for air flow through the outer containment baffle. The findings from this study are as follows:

- Westinghouse's analysis of dry containment pressure response described in Chapter 40 of the PSA documentation (Ref. 21) appear to be based on a LOCA sequence without gravity drain of the IRWST to the RPV. Independent MELCOR calculations of containment pressure response for a Medium LOCA without gravity drain into the RPV confirmed Westinghouse's MAAP4 estimates of peak containment pressure after 24 hours, thereby providing confidence that the simple MELCOR model used could generate reasonable estimates of the AP1000 thermodynamic response, and some confidence in the estimated value for the load used to estimate late containment failure probability.
- The analysis basis for the assigned value of (dry) containment failure probability within 24 hours was not evident. My team's MELCOR calculations of a LOCA sequence with successful gravity injection into the RPV and a dry containment shell predicted pressures large enough to suggest containment failure probabilities before 24 hours (i.e. intermediate containment failure end-state) that are higher than the values used in the PSA. The absolute peak pressure over the whole transient was not higher than that predicted by Westinghouse's analysis, but the peak pressure occurred earlier, this being the reason why higher probabilities of intermediate containment failure are suggested.
- Flow resistance in the air baffle area of the shield building has a potentially large impact on containment heat transfer. Results of sensitivity calculations performed by my team with the (simple) MELCOR model suggested that peak containment pressure can vary considerably with small changes in flow resistance. Although this could be due, in part, to an under-estimation of heat transfer through the containment shell by the MELCOR model (using default dry surface correlations), it does suggest that Westinghouse may need to demonstrate a very high degree of confidence in the loss factors used in the MAAP4 model in order to justify the accuracy of the predicted peak pressures. It should be also noted that plastic strains created by beyond design

basis pressures in the containment vessel could affect the size of the air gap around the baffle plates.

- The key points of the above discussion are:

  1. Westinghouse's calculated containment pressure response could only be reproduced by assuming IRWST drain via a different path to that stated by Westinghouse in Chapter 40 of Ref. 21.
  2. A faster containment pressurisation was obtained when the IRWST drain modelling matched the Westinghouse's described drain path (to the RCS).
  3. The MELCOR analysis suggests that there may be substantial sensitivity of the calculated peak pressure to flow resistances in the air baffle.

  The three key points above are supplemented by the discussion of Westinghouse's White Paper on air cooling of the containment shell presented in Section 4.18.3.1 above. The conclusions of 4.18.3.1 are considered to be reinforced, i.e. that Westinghouse has not shown that containment failure will not occur in sequences with a dry shell, and without additional recoveries, and that in the Level 1 PSA the LCF sequences should be added to the CDF and transferred to the Level 2 by assigning an appropriate PDS. In addition, in the subsequent Level 2 treatment, the probability of intermediate containment failure (before 24 hours) may be underestimated. It is noted that this probability does not impact the Large Release Frequency, but the timing issue it implicitly relates to would impact a full offsite risk calculation, for comparison against the numerical targets of the SAPs (Ref. 4).

  Assessment Finding AF-AP1000-PSA-064: *The Licensee shall provide an improved analysis of the dry containment response to support the evaluation of failure probability of the containment in dry shell scenarios in the Level 2 PSA. This should address selection and justification of an appropriate bounding sequence for the analysis. It should also address the flow resistance in the air baffle area taking into account the gap allowed by the pressures in the relevant scenarios.*

4.18.3.3 Level 2 PSA: Containment Performance Analysis (A1-3.3)

366 The following specific concerns have been raised during my review of Westinghouse's evaluation of the AP1000 Containment Structural Analysis used as an input to the Level 2 PSA:

- No indications have been found that detailed localized analyses at discontinuities have been performed. It also appears that degradation effects (i.e., corrosion damage) of the steel containment vessel have not been considered.
- Failure sizes are not provided.
- The review team felt that primary failure modes had been addressed but to varying degrees of completeness. Documentation of assessments of "small" potential leakage paths is generally lacking and therefore it was not clear that a systematic review of the containment structure has been performed to identify all plausible and credible failure modes. In fact, the review team could not find evidence that detailed assessments of potential leakage paths through purge and vent valves had been done. Also, specific analyses of electrical and smaller process pipe penetrations have not been presented in the documentation.

- The assessment has not differentiated between leakage and rupture. What appears to be the most likely / dominant failure mode (i.e., leakage through main steam and feedwater bellows due to large radial movements following the onset of general tensile membrane hoop yielding of the containment vessel) is not separately identified from catastrophic rupture of the shell.
- In terms of the fragility presented representing failure of the main steam and feedwater pipework bellows, it is considered that the probability of failure (at any pressure point on the curve) has been considerably under-estimated. This is based on observations of numerous pre-test predictions of steel containment vessel scale models and subsequent test data. The fragility presented representing catastrophic rupture of the shell, which used the onset of a median yield stress, is considered to be reasonably realistic.

Assessment Finding AF-AP1000-PSA-065: *The Licensee shall provide a revised and documented AP1000 containment performance analysis for the Level 2 PSA addressing the shortcomings identified in the GDA review.*

4.18.3.4 Level 2 PSA: Probabilistic Modelling Framework – Accident Progression Event Trees (A1-3.4)

367 An important note to bring up first is that during GDA Step 4 Westinghouse's Severe Accident Management Guidelines (SAMG) were still in a preliminary (alpha) revision status. During the review it was observed that the communications and interactions between Westinghouse's Severe Accident and PSA teams were very good and therefore it is believed that there will be an adequate process to make sure that finalisation of the SAMGs will feed through into a future update of the PSA. However, from the point of view of a regulatory review of an updated version of the PSA, it would be expected that the link between the CETs and the SAMGs is transparent and explicitly documented. A future version of the PSA report should address this point.

Assessment Finding AF-AP1000-PSA-066: *The Licensee shall provide revised documentation of the Level 2 PSA showing clear links between the relevant parts of the Containment Event Trees and the Severe Accident Management Guidelines.*

368 The CET conservatively simplifies the treatment of failed In-vessel Retention scenarios (these being low pressure sequences), high pressure sequences and sequences with PCS failure, i.e.:

- Sequences with failure of IVR: Appendix B of Ref. 21 provides the results of a limited number of deterministic investigations of the consequences of ex-vessel severe accident phenomena for the AP1000. The results of this limited deterministic investigation suggested that the containment would not necessarily fail due to ex-vessel severe accident phenomena. However, the Level 2 PSA modelling does not treat these issues at all; rather it is simplified such that after IVR failure it conservatively assumes large release in all cases.
- Sequences with core damage at high pressure: for all sequences in which RCS depressurisation fails, induced SGTR due to creep-rupture is assumed (without any probability analysis) and they are directly considered as being large release sequences without any further evaluation of the challenges to the containment, potential release paths and potential mitigation of the releases.

- Furthermore, for sequences in which the CET node related to PCS fails, large release is directly assumed (albeit predominantly in the late timeframe, after 24 hours) based on a conservative estimation of the probability of containment overpressure failure. (By way of clarification, this statement about the conservatism of the treatment of late overpressure failures is not inconsistent with the discussion of 4.18.3.1 and 4.18.3.2 which referred to the failure probabilities assigned to different sequences in different timeframes).

It is felt that full development of the above sequences, which are conservatively treated in the current PSA, would be more informative, allow better understanding of impacts on risk, and facilitate a more robust ALARP justification.

> ***Assessment Finding AF-AP1000-PSA-067:*** *The Licensee shall provide revised and documented AP1000 Containment Event Trees expanded to more realistically reflect the evolution of sequences with IVR failure, core damage at high pressure, and failure of passive containment cooling.*

369 Detailed review of a number of phenomenological CET nodes was conducted during GDA Step 4. The conclusions of the assessment of Westinghouse's analysis of the phenomenology and probability evaluations for the CET nodes "Reactor vessel integrity", "No failure of over-pressurised containment before 24 hrs", "No containment failure due to elevated temperature of diffusion flame", "No containment failure due to DDT during hydrogen release", "No containment failure due to hydrogen deflagration", "No containment failure due to hydrogen detonation" are discussed in Section 4.18.3.2 above and no further detailed discussion is presented here. However, it should be mentioned that a general concern was raised regarding the lack of evidence that Westinghouse had obtained a consistent / uniform scale for the probabilities assigned to the individual nodes, since different methods had been used for the different nodes, and there was no visibility of any global consistency checks of the results obtained.

> ***Assessment Finding AF-AP1000-PSA-068:*** *The Licensee shall provide a justification that the probabilities assigned to the individual nodes in the Containment Event Tree are based on a consistent scale.*

370 The probabilities of a number of CET nodes associated with system failures were evaluated by Westinghouse using standard fault trees. A number of these ("containment isolation" and "hydrogen control") have been reviewed in GDA Step 4 and are discussed in the following paragraphs.

371 From the detailed review of the Containment Isolation fault trees, the following findings were raised:

- "Containment Isolation failure" is a heading in the Level 1 PSA event trees and in the Level 2 CET. It had already been mentioned in 4.6.3 above that the fault trees representing failure of containment isolation have been developed based on a screening criterion for penetrations that has been questioned in the review (i.e. based on a diameter of less than 2"). From the perspective of the Level 2 PSA, it should be added that Westinghouse did not provide specific analyses demonstrating negligible source term for a 2" containment failure as a justification. Statements such as general acceptability and acceptability by USNRC are not considered sufficient justification. A document referenced by Westinghouse, WCAP-15791 (Ref. 96) appears to use a justification that releases would not be large (i.e. not LRF) through a 2" opening. This is not considered a sufficient justification and it is certainly inadequate to calculate frequencies to compare against the numerical targets of the SAPs (Ref. 4). In addition, it was not clear to the reviewers that the same success

criteria would apply for the fault trees that represent failure of containment isolation in the Level 1 PSA (leading to different success criteria for the sump recirculation function) as for the fault trees that represent failure of containment isolation in the Level 2 PSA.

- CVS valves V045 and V047 are wrongly omitted from the fault tree models. Instead the failure of two different valves has been included in the model instead. While these errors may not have a significant numerical impact, they still need to be corrected.
- It appears that common cause failures of non-return valves with containment isolation function have not been included in the fault trees.
- Inconsistencies were found in gate descriptions.
- The use of "dummy events" in the fault tree (in this particular case under the DAS automatic and manual logic) with assigned probabilities of 10^{-20} created confusion in the review – the correct modelling of HFEs associated with isolation of the containment from DAS could not be confirmed.
- As indicated above, the containment isolation fault trees are used in both the Level 1 and Level 2 PSA models for different purposes. The use of the same time windows for operator action is not justified by specific analyses.

Assessment Finding AF-AP1000-PSA-069: *The Licensee shall provide revised criteria for screening of containment penetrations for the purpose of containment isolation. Separate justifications should be provided for the criteria used for the Level 1 and Level 2 PSA.*

Assessment Finding AF-AP1000-PSA-070: *The Licensee shall provide revised and documented PSA fault trees for the Containment Isolation taking into account the shortcomings identified by the GDA review.*

372 I conducted an assessment of the fault trees for the Containment Hydrogen Control System (Hydrogen Igniters). The concerns raised from my review were consistent with concerns raised during the review of other fault tree models for other systems discussed in Section 4.7 above. For example:

- There appeared to be inconsistencies within the text and between the text in Chapter 16 of the PSA (Ref. 21), the fault trees (Ref. 25), and Chapter 6 of the DCD (Ref. 51), with respect to the power supplies to the Hydrogen Igniters and sensors.
- It was not clear whether the CCF modelling was complete. CCF of all Hydrogen Igniters is included in the fault tree. Common cause failures affecting sub-groups of igniters are not modelled. Therefore it appears that there are CCF combinations missing from the results as well as combinations of CCFs and individual igniter failures. Furthermore, the precise success criteria for the igniters is not clear.
- The hydrogen sensors are not modelled explicitly within the fault trees. Instead a generic event with an assigned probability of 10^{-6} /d is modelled, which appears to be too optimistic considering the information about the limited number of hydrogen sensors provided in Chapter 6 of the DCD (Ref. 51). On the other hand, there is also a lack of clarity regarding the cues for actuation of the Hydrogen Igniters. It is believed that Hydrogen Igniter actuation would be required in symptom-based procedure FR-C.1 before entering the SAMGs, in which case hydrogen concentration would not be the principal cue, implying that the logical representation of the hydrogen sensors in the fault tree model might not be correct anyway. This reinforces a finding raised from my GDA Step 3 review regarding the simplistic modelling

throughout the PSA of instrumentation failures that contribute to the human errors (e.g. failure of the alarms or indications), which is unrelated to the actual instrumentation available.

- Modular events have been used in the modelling of power supplies to the Hydrogen Igniters and there was not clarity about what they represented and why probabilities of apparently similar modules in different trains were inconsistent.

Assessment Finding AF-AP1000-PSA-071: *The Licensee shall provide revised and documented PSA fault trees for the Containment Hydrogen Control System taking into account the shortcomings identified by the GDA review.*

373 The evaluation of Westinghouse's responses to the Technical Queries raised from my GDA Step 3 review of the AP1000 Containment Event Trees has confirmed the validity of the concern I originally raised about the lack of treatment of human dependencies between the HFEs before and after core damage (also discussed in Section 4.18.3.1 above).

374 Finally, and consistently with what was already identified during the review of the Level 1 PSA, the timings for operator actions post core damage are not well justified by analysis. An example is the estimation of time windows for RCS depressurisation in different core damage sequence types.

Assessment Finding AF-AP1000-PSA-072: *The Licensee shall provide specific analysis to justify the time windows for all the human actions credited in the Level 2 PSA model.*

375 Westinghouse's response to RO-AP1000-068 (Ref. 92) describes a modified CET in which the success criteria for IVR have changed from that considered in the original PSA (Ref. 21). The new model, presented as a sensitivity analysis, reflects IVR success if water cooling is achieved from outside the RPV (as before) but only if water is injected inside the RPV. The findings from my review of Ref. 92 are discussed below:

- Reassessment of two sequences assigned to "success of IVR" in the model provided resulted in a small probability of IVR failure in one of the cases (consistently with the conclusions reported in Section 4.18.3.4 above) but this would not have a significant effect on the results obtained.
- There was a concern that, given the short time windows, the probabilities obtained in the human reliability analysis appeared to be optimistic. The method applied by Westinghouse did not explicitly consider the impact of time available to carry out the actions in relation to the typical time that would be required to perform the action. In addition, similarly to the concern that was raised during the review of the Level 2 PSA (see above) for this study dependencies with human errors present in the Level 1 core damage sequences were not modelled either.
- According to drawings provided by Westinghouse representing the diagram for IRWST cavity injection via RNS, valves linking train A and train B of the RNS suction lines are shown normally open, but it is indicated that they "FC" which was understood to mean that they fail closed on loss of power supply. If that is the case there may be an error in the fault tree model.
- As was the case in the baseline Level 2 PSA (Ref. 21), PDSs which are at high pressure at the time of core damage and which are subsequently depressurised by operator action (by opening ADS Stage 4 valves) do not use a fault tree to model

failure of IRWST injection, i.e. the model implicitly assumes success of IRWST injection. This is considered optimistic.

- Westinghouse did not perform a fully linked fault tree analysis to generate the results presented in Ref. 92. This may lead to certain degree of underestimation in the results.
- The results from the new model presented by Westinghouse indicate a potential increase of LRF when the modified assumptions about IVR success are included. It was noted that the modified CET model assumes the use of an accident management strategy (IRWST injection via the RNS suction line) which is not currently proceduralised (although it should be noted that Westinghouse indicated that this had been embedded into their change control process to be formally implemented).
- Finally, Westinghouse should update the (baseline) AP1000 Level 2 PSA to reflect the modified IVR success criteria as per Ref. 92.

Assessment Finding AF-AP1000-PSA-073: *The Licensee shall provide an updated AP1000 Level 2 PSA reflecting the modified IVR success criteria as per Ref. 92. For the development of the modified model the Licensee shall address the shortcomings identified during the GDA review of Ref. 92.*

4.18.3.5 Level 2 PSA: Source Term Analysis (A1-3.5)

376 A quantitative description of the fission product source terms to the environment for each Release Category (RC) in the AP1000 PSA is provided in Chapter 45 of Ref. 21. The description of radionuclide release is limited to plots of the time-dependent release fraction for several radioactive species and a tabular summary of the cumulative release fractions at two times in the accident sequence (24 and 72 hrs). No discussion is offered to connect the fission product release signatures in Chapter 45 to corresponding information on the chronology of events and severe accident phenomena in Chapter 34 of Ref. 21. This is considered a gap in the PSA documentation.

377 The evaluation conducted in GDA Step 4 of Westinghouse's responses to the TQs raised from the Step 3 review of the AP1000 PSA source term analysis confirmed that the concerns initially raised were valid. This evaluation raised important insights in the context of compliance against the numerical targets of the SAPs (Ref. 4). Therefore, they are discussed in some detail in the following paragraphs.

378 My GDA Step 3 review of the AP1000 source term analysis raised concerns about the adequacy of the level of discrimination among Release Categories (RC). A common source term 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. Some examples of potential influences on releases that are not considered in the RC definitions (or even discussed as potential release category attributes) are: timing of core damage onset, sequence type (LOCA or transient), use of sprays for release mitigation, IRWST status, cause of containment failure, etc. Some examples of concerns arising due to the lack of granularity of the RCs are:

- The wide range of radiological release scenarios enveloped within each RC may limit any evaluation or understanding of the relative contribution of systems, sequences or phenomenological issues to overall (risk and release frequency) results.
- Potentially, the ALARP discussion could be impacted.

- A clear mapping of the AP1000 RCs to the dose bands in Target 8 and to the societal risk in Target 9 from NT.1 of the SAPs (Ref.4) cannot be established.

Therefore, it is concluded that there is a gap related to the level of detail and (insufficient) number of source term categories defined in the AP1000 Level 2 PSA and more work will be needed to fulfil the UK specific requirements.

379 The wide range of radiological release scenarios enveloped by each release category make it more difficult to select representative sequences for each RC for quantitative source term evaluation. Westinghouse was requested to explain and justify the process used to select a representative sequence for each RC and to provide a technical basis for the use of a single sequence to represent the RC bearing in mind the potential variability of releases between sequences assigned to each RC. From Westinghouse's response the following is concluded:

- Westinghouse referred to US targets (large release < 10^{-6} /yr) and presented the argument that the analysis performed was sufficient given compliance with this target and, generally, the low risk results from the AP1000. This may be sufficient in the US regulatory context but it is not relevant in the context of compliance with the numerical targets of the SAPs (Ref. 4) in the UK.
- The Level 2 PSA documentation (Ref. 21) does not refer to the sensitivity studies in Ref. 99 (AP1000 Source Term Analysis), which was presented to support Westinghouse's response to a TQ. Nor does the Level 2 PSA documentation lay out the process for selection and justification of the presented source term analyses. It is therefore considered that there is a documentation gap in the PSA submission.

380 The above points were explored further during my GDA Step 4 review of the Level 2 PSA for two specific examples. In these particular cases my review noted that a sequence initiated by SGTR, rather than an induced SGTR, had been chosen to represent release category "BP" (containment bypass) for source term analysis, when in fact induced SGTR sequences are higher contributors to this RC. Also, a sequence corresponding to PDS "3D" followed by a containment failure due to elevated temperature had been chosen to represent release category "CFE" (early containment failure) when in fact the largest contribution to this RC comes from sequences that involve failure of cavity flooding belonging to a different PDS. Westinghouse was requested to justify the choice of sequences for source term evaluation for those two specific RCs. Westinghouse's response was considered insufficient since, although it referred to Ref. 99 which provided some sensitivity studies for alternative sequences, the specific case of sequences with vessel failure had not been performed, and Westinghouse's response on that part of the question was simply to state this.

381 My GDA Step 3 review queried various aspects of the source term characterisation presented in Chapter 45 of Ref. 21. From Westinghouse's response the following is concluded:

- Westinghouse explained why the continuous release fractions from MAAP4 calculations are reduced to four consecutive plumes, each with a unique start time, duration and (constant) release rate – the four plume assumption appeared to be caused by a limitation in the version of the Level 3 PSA code MACCS. However, it should be noted that the limit of 4 plume segments was removed in the version of MACCS2 released in late 2008.
- In the AP1000 PSA the releases are assumed to have no internal energy (i.e. no plume rise is reflected in the offsite dispersion calculations).

- The chemical forms of released radionuclides are stated (based on the MAAP4 framework) in Ref. 21, however, the assumed isotopic inventory of radionuclides used to translate the fractional releases from MAAP4 to offsite dose is not described.

The above points highlight an aspect of the AP1000 Level 2 / 3 PSA that is incomplete for applications in the U.K. Although internal energy (heat content) and elevation of the release are listed as attributes of fission product source terms in the Level 2 PSA, numerical results for these parameters (from MAAP4 calculations) are ignored in the assessment of ex-plant radiological dose. The plume is treated as a "cold" release (zero energy) at ground elevation to minimize atmospheric dispersion, and to maximize the calculated dose at the site boundary. A limitation of this approach is that it precludes a realistic calculation of offsite dose for comparison against Targets 7, 8 and 9 from NT.1 of the SAPs (Ref. 4). See also Section 4.19 below for a specific discussion of my team's review of the AP1000 Level 3 PSA results.

Assessment Finding AF-AP1000-PSA-074: *The Licensee shall provide revised Source Term analysis for the AP1000 Level 2 PSA addressing the shortcomings identified during the GDA review. The analysis should be of sufficient scope and level of detail to allow a meaningful comparison against the numerical targets of the SAPs.*

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

382 During my review of the Level 2 PSA in GDA Step 3, I identified that the quantification process described in Chapter 43 of the PSA (Ref. 21) did not match the AP1000 PSA model developed in CAFTA. In fact, none of the references provided by Westinghouse accompanying the CAFTA model (Refs 24 and 25) provide a complete documentation of the current CAFTA Level 2 PSA model.

383 Ref. 25 includes a comparison of CAFTA model LRF cutsets against the cutsets corresponding to the older model documented in Chapter 43 the PSA (Ref. 21). It is indicated there that many of the discrepancies are the direct result of the C&I model revision and the change in the frequency of the initiating event "Spurious ADS". Apparently, some other discrepancies in the LRF cutsets were due to the change in methodology of the LRF quantification between both models. Ref. 25 also presents a summary of the Plant Damage State frequencies in both versions of the PSA. It is indicated there that while these may differ in value due to modelling changes, they are similar in percent contribution. Ref. 25 however fails to explain the differences in the frequencies of the Release Categories, in particular why the CAFTA model gives a much higher (although in absolute terms still small) frequency for the release category "CFL" (Late Containment Failure).

384 Ref. 24 presents a list of the "Component Importances for LRF At-Power". However, it does not include a complete summary of the Level 2 PSA results together with accompanying discussions providing a clear understanding of the risk of the defined categories of radioactive releases, where this risk comes from and which are the most significant uncertainties.

385 From the discussion above it is concluded that the documentation of the AP1000 Level 2 PSA results needs significant improvements to meet the expectations of ND's PSA guide (Ref. 15).

Assessment Finding AF-AP1000-PSA-075: *The Licensee shall provide revised documentation of the AP1000 Level 2 PSA including a thorough and complete description of the results and the conclusions obtained.*

386 It was already identified in GDA Step 3 that in the current PSA there is no propagation of uncertainties to the results of the Level 2 PSA, i.e. uncertainty distributions on the frequencies of the release (source term) categories have not been generated by Westinghouse. Westinghouse has committed to undertake this work in a future update of the PSA.

Assessment Finding AF-AP1000-PSA-076: *The Licensee shall provide AP1000 Level 2 PSA results including presentation of the propagation of uncertainties throughout the complete PSA model.*

387 During GDA Step 4, Westinghouse also provided a commitment to address, in a future update of the PSA, the following aspects currently missing from the study:

- Incorporation of the hazards in the Level 2 PSA.
- Incorporation of other sources of radioactivity (spent fuel pool) in the Level 2 PSA.
- Performance of an AP1000 Shutdown Level 2 PSA.
- Evaluation of the frequency of, and radiological releases from, accident sequences without core damage and integration of the results with the overall results of the Level 2 PSA.
- Provision of a demonstration that the risk of radioactive release for the AP1000 is ALARP taking into account all the aspects currently missing from the PSA.

Assessment Finding AF-AP1000-PSA-005 (repeated from Sub-section 4.2.3 above): *The Licensee shall provide a full scope PSA for the AP1000.*

Assessment Finding AF-AP1000-PSA-006 (repeated from Sub-section 4.2.3 above): *The Licensee shall provide an evaluation of the frequency of, and radiological releases and consequences from, AP1000 accident sequences without core damage.*

Assessment Finding AF-AP1000-PSA-077: *The Licensee shall provide a demonstration that the risk of radioactive release for the AP1000 is ALARP taking into account the overall results from the PSA.*

4.18.3.7 Results of the Risk Gap Analysis

388 The Base-case (BC) RGA Model, including the Level 1 and Level 2 PSA changes, generated a higher CDF and a significantly higher LRF. This model therefore presented a conditional Large Release Probability (LRP) higher than that in the current PSA. The reasons driving the overall increase in LRP could be understood by comparing the profile of the CDF in terms of PDS frequencies and contribution for the PSA version 3B model (Ref. 25) and the BC RGA Model. This comparison showed that the RGA implementation (for Level 1 issues) led to a larger increase in the frequency of PDSs with bypass or core damage at high pressure, than in the frequency of sequences with core damage at low pressure. As a result, the profile of the core damage sequences suggested by the RGA was different to that in the current PSA.

389 The above result is of critical importance for the results of the Level 2 model in the RGA and is a key conclusion from the overall PSA review. Sequences with core damage at

high pressure have a high probability of leading to large release, according to Westinghouse's Level 2 PSA. An increase in the frequency of PDSs with core damage at high pressure therefore has a disproportionate impact on large release. This is supported by the numerical results which show that most of the increase in LRF is associated with release category "BP" (bypass) which arises from PDSs with bypass or high pressure PDSs which are not depressurised and which are subsequently assumed to lead to an induced steam generator tube rupture.

390 The other important highlight from the RGA in relation to the Level 2 PSA is that some degree of sensitivity is seen to the IVR failure probabilities. This is not inconsistent with Westinghouse's response to RO-AP1000-68, which also showed that there is sensitivity of LRF to the modelling of IVR.

391 The other studies undertaken did not identify any other significant areas of sensitivity.

392 The impact of the findings identified during the review of the containment performance analysis for the Level 2 PSA has not been addressed quantitatively in the RGA. However, the impact may not be negligible when the shortcomings in the analysis are corrected, in particular the optimism in the main steam and feedwater bellows failure and associated containment vessel leakage fragility.

4.18.4 Conclusions

393 On the basis of the assessment of the Level 2 PSA described above I conclude the following:

- Westinghouse's Level 2 PSA is considered sufficient for the "generic" PCSR PSA but will require improvements to support further stages of the NPP development. An updated and fully documented Level 2 PSA, covering all the initiating events and sources of radioactivity for operations at power, low power and shutdown, should be developed as part of the next update of the PSA (see Section 5 below). In particular, the traceability of the models to the supporting analyses needs to be improved. Also, development of those sequences currently (potentially conservatively) assigned to large release will better support a more complete understanding of the risk and an adequate ALARP evaluation. Improvements in the PSA source term analysis are required to better support a comparison against Targets 7, 8 and 9 from NT.1 of the SAPs.
- Westinghouse's containment structural analysis for the Level 2 PSA is plausible and generally reasonable although it lacks thorough and clear documentation of all potential failure modes, and lacks separate identification of a fragility from leakage and a fragility from catastrophic shell rupture. This will require improvements to support future stages of the NPP development. More detailed containment structural analysis specifically addressing small penetrations will also be required. Therefore, a revised containment structural analysis should be ready to be inputted to the next update of the Level 2 PSA (see Section 5 below).

4.19 Level 3 PSA (A1-4)

4.19.1 Assessment

394 No assessment of Level 3 PSA was carried out at Step 3 of GDA. My primary focus of assessment in GDA Step 4 has been on the adequacy of Westinghouse's derivation, from the release frequencies and source terms identified in the Level 2 PSA, of risks to

the public for comparison with Targets 7 to 9 from NT.1 of the SAPs (Ref. 4). It is recognised that, as many parameters needed in Level 3 PSA are site specific (for example weather and population distribution), the risks derived for GDA are only indicative.

395 As Westinghouse's case claims risks below the BSOs, in accordance with SAPs requirements under that circumstance, my assessment has been principally concerned with confirming the validity of the claimed risk figures. As suggested in T/AST/30 and T/AST/45, independent calculations were carried out. These were performed using the computer code PC COSYMA by the UK Health Protection Agency as a Technical Support Contractor to HSE. PC COSYMA is the principal modern Level 3 PSA code in use in the UK. The MAACS2 code used by Westinghouse is discussed below. The results are discussed in detail in the next section, but broadly they confirmed Westinghouse's analysis to the degree of accuracy that can be expected for Level 3 PSA.

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

396 The analysis carried out by Westinghouse is biased towards US methodology and regulatory requirements. Consequently, inferences have to be made when comparing the assessment results with SAP targets as direct comparisons are not possible.

397 For the release categories the source terms are clearly defined including quantities of radionuclides, frequencies and timings. Conservatively releases are assumed to be at ground level (see also discussion in 4.18.3.5 above). The methods used to model dispersion in the environment and calculate doses are discussed, but the description is incomplete. For example, details of the calculation of doses from inhalation and immersion in the radioactive plume are given, but not from external irradiation due to deposited material, or inhalation of resuspended material. (Note: this has subsequently been addressed in a revision of the PCSR, but has not been assessed). The data used in the dose calculations is also not clearly defined in the PCSR and referenced data sources are sometimes not readily available.

398 The Level 3 PSA code used by Westinghouse is MACCS2 (MELCOR Accident Consequence Code System,). MACCS2 was developed under the sponsorship of the US Nuclear Regulatory Commission. Whilst there is no issue with the robustness of this code, the parameters it uses, such as weather and dose coefficients are not those used in the UK.

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

399 Westinghouse summarises the outcome of the Level 3 PSA in Chapter 5 of Ref.11. Direct comparison of these results with the SAP targets is not possible because they represent different quantities. Westinghouse recognises this and provides arguments to conclude that the BSOs for Targets 7 to 9 from NT.1 of the SAPs (Ref. 4) are met. The independent calculations by the Health Protection Agency for HSE also confirm that they have been met, although not by as large a margin.

400 There are a number of shortcomings in the analysis. No estimation of deterministic health effects is included. In considering Target 7 from NT.1 of the SAPs (Ref. 4) no contribution to risk from accident sequences other than those described by the reference release categories is considered. In considering Target 8 from NT.1 of the SAPs the dose calculated for each release category has been used, however only one of these release categories gives a dose that is not in the highest dose band of each target.

Based on these few release categories the conclusion is drawn that the targets are met because the total release frequency does not exceed the BSO. Justification for not considering other release categories which result in lower doses but which may occur more frequently is needed. In addition, the dose is a mean dose and the implications of using this rather than the maximum or a high percentile should be addressed.

401 For the assessment of societal risk it is argued that, in meeting the US regulatory target, the Target 9 from NT.1 of the SAPs (Ref. 4) is also met because the latter is less restrictive. However, this conclusion is not robust because although the risk corresponding to the SAP target is higher, it includes all on-site accidents which may result in 100 or more fatalities in the UK population, and this may include events that do not meet the site boundary dose criterion in the US target.

402 Probabilistic assessments of dose presented in Ref. 21 do not appear to be the same as those presented in Ref. 11.

4.19.2 Strengths

403 The independent modelling and calculations done for HSE by the Health Protection Agency are in broad agreement with Westinghouse's submission.

404 The PSA process is described in detail.

405 The release categories used in the analysis are clearly defined.

406 A recognised accident consequence assessment code MACCS2 has been used.

407 Results of the Level 3 PSA are clearly presented.

4.19.3 Findings

408 The detailed technical reviews that support the findings discussed in the following paragraphs are documented in Ref. 103.

409 Sufficient evidence on dispersion and consequence modelling has been provided to show that the AP1000 will meet the BSLs for Targets 7, 8 and 9 from NT.1 of the SAPs (Ref. 4), and that the BSOs are likely to be met, based on the input source terms and frequencies. However there are shortcomings in the evidence presented. For UK site-specific Level 3 PSA, site specific analyses of frequency for relevant fault sequences will need to be incorporated, together with site specific dispersion and consequence modelling parameters (such as weather data and distribution of population and agriculture) for all releases. Evidence will need to be presented to permit direct comparison with the UK framework rather than by inference from comparison against US standards.

> ***Assessment Finding AF-AP1000-PSA-078:*** *The Licensee shall provide a Level 3 PSA that addresses site specific analyses of frequency for relevant fault sequences, using site specific dispersion and consequence modelling parameters, with assessed outcomes commensurate with the UK framework.*

4.19.4 Conclusions

410 On the basis of the assessment of the Level 3 PSA described above I conclude that Westinghouse's submission in respect of Level 3 PSA provides sufficient evidence that

the AP1000 is capable of being constructed and operated in compliance with UK requirements and hence is adequate for GDA.

4.20 Overall Conclusions from the PSA (A1-5)

4.20.1 Assessment

411 This section presents my conclusions of the GDA review of the AP1000 PSA when compared against relevant expectations in Table A1-5 of ND's PSA TAG (Ref. 15)

412 My assessment team has looked at the PSA, together with the results of the review conducted and the results of the Risk Gap Analysis, in order to judge:

- The adequacy of the PSA documentation.
- Whether it is believed that all aspects of the PSA have been subject to sufficient level of independent review by the duty-holder.
- Whether the PSA has a credible and defensible basis.
- Whether the PSA reflects the design of the AP1000 submitted for GDA.
- The adequacy of the process in place to ensure that the PSA assumptions regarding design and operation of the AP1000 are captured in the development of future procedures, policies and strategies, design, design modifications and back-fits, etc.
- The adequacy of the process in place to keep the PSA living.
- Whether the PSA has enabled a judgement to be made as to the acceptability of the overall risk of the facility against the SAPs numerical targets.
- Whether the PSA has been effectively used to demonstrate that a balanced design has been achieved and that the risk associated with the design and operation of the AP1000 is ALARP.

4.20.2 Strengths

413 The strengths found during the review of the AP1000 PSA have been described in all the individual technical sections above as / when appropriate.

4.20.3 Findings

414 I already stated in my GDA Step 3 report (Ref. 6) that the AP1000 PSA documentation was not consolidated. Some chapters of the UK AP1000 PSA report (Ref. 21) had been superseded by Calculation Notes (including the PSA model itself). Also there was heavy reliance on, and reference to, the AP600 PSA documentation and supporting analyses. My detailed reviews of all aspects of the PSA support analyses, models and data conducted in GDA Step 4 have provided additional evidence that not all aspects of the PSA are fully traceable to the design documentation, drawings, analyses, operating procedures, or any other supporting information. In addition, the significant number of errors found when reviewing the models has led me to judge that the AP1000 PSA has not been subject to a sufficient level of internal independent review by Westinghouse. It should be noted that Westinghouse has indicated that the reason for this is that the AP1000 PSA has evolved through incremental changes without a review of the totality of the PSA or a global update of the PSA to current standards.

Assessment Finding AF-AP1000-PSA-079: *The Licensee shall provide evidence that independent detailed reviews of all aspects of the AP1000 PSA have been undertaken.*

415 My team enquired about Westinghouse's system to capture assumptions made in the PSA which could be affected by siting, design and construction, or operational matters (such as procedures, maintenance and testing strategies, training programmes, control room staffing and organisation, etc), and which would need to be reviewed when / as detailed information becomes available. During GDA Step 4 Westinghouse's system to capture PSA assumptions was discussed and the following can be highlighted:

- Westinghouse has a procedure that controls the interactions between the PSA and the Design Change Process, called Design Change Package 341 (form 341-3).
- In addition Westinghouse has provided a review of the Design Change Proposals (Ref. 98) for PSA.
- There is also a Corrective Action Plan (CAP) with an associated database which captures and controls inconsistencies (errors) between the PSA, DCD, etc, and the design or analyses.

Based on the succinct review conducted, and the current status of the PSA, it was not totally clear to me whether the system/s in place will be able to effectively enable the PSA assumptions to be captured in future design, construction and procedure development. Also, it was not clear whether the system would enable an effective transfer of the latest available design and operational information to the PSA so that assumptions (and models) can be reviewed accordingly. Because of this, further checks should be conducted while following-up Westinghouse's completion of the two PSA GDA Issues, in particular the one on Fire PSA **(GI-AP1000-PSA-02)**. It should be noted that this has been captured in one of the Fire PSA GDA Issue Actions **(GI-AP1000-PSA.02.15)** which requests Westinghouse to develop and provide a Living PSA procedure to allow the Fire PSA to be updated as further design information becomes available and when the Internal Events PSA evolves in a way that may impact the Fire PSA.

Assessment Finding AF-AP1000-PSA-080: *The Licensee shall implement and provide the procedure to maintain the PSA and keep it Living.*

Assessment Finding AF-AP1000-PSA-081: *The Licensee shall implement and provide the procedure for the use of the PSA to support all aspects of design and operation of the NPP.*

Assessment Finding AF-AP1000-PSA-082: *The Licensee shall provide an updated version of the Fuel Pool PSA including as-built and as-(to be)-operated information before fuel is brought into the site.*

Assessment Finding AF-AP1000-PSA-083: *The Licensee shall provide an updated version of the Reactor at Low Power and Shutdown PSA including as-built and as-(to be)-operated information before fuel is loaded into the reactor.*

Assessment Finding AF-AP1000-PSA-084: *The Licensee shall provide an updated version of the Reactor at Power PSA including as-built and as-(to be)-operated information before first criticality.*

416 The results of my review and of the Risk Gap Analysis, discussed in the above sub-sections, have helped me to judge whether the PSA has a credible and defensible basis and whether in its current state enables a meaningful comparison against the SAPs numerical targets. The conclusion is that the PSA needs substantial improvements to

meet these expectations. This judgement is based on the numerous findings identified during the review, on the potentially significant risk gaps and those potential gaps which could not be quantified in the RGA. The review findings are discussed extensively in the sections above for each technical area of the PSA. The results of the RGA are summarised in the following paragraphs.

417 The following are the most significant (potential) risk gaps found:

- Missing internal IEs from the current version of the PSA.
- Changes in IE frequencies (in particular IS LOCA frequency)
- Omission of sequences involving failure of the pressuriser Safety Relief Valves (SRV) to open when challenged, and omission of sequences involving failure of containment heat removal.
- Current omission of pre-accident human errors (Type A HFEs).
- Missing common cause failures.
- Missing scenarios in the Internal Flooding PSA.
- Seismic risk.
- Consideration of maintenance unavailabilities allowed during Low Power and Shutdown states.
- Consideration of dependencies between HFEs in the Spent Fuel Pool PSA.
- In addition, Westinghouse's response to RO-AP1000-099 shows another risk gap in relation to the current SGTR model.

418 As described in Section 2.3.2 above, as part of the Risk Gap Analysis I developed a Base-case (BC) RGA Model from the original PSA by implementing modifications to the model and data based on the review findings. The quantification of the modified model showed a CDF increase. The LRF increased by a larger factor. Since the intention of the RGA was not to produce alternative PSA results, the precise numbers are not presented here. The results obtained lead to qualitatively interesting insights on how the deficiencies and limitations found in the PSA, when corrected, could potentially change the AP1000 risk profile. In particular, it appears that the impact is larger on the frequency of sequences with core melt at high pressure – these sequences are currently assumed in the AP1000 PSA to lead to large release without any further analysis. Whether this is a conservative assumption, i.e. whether an induced SGTR could be avoided or whether the AP1000 steel containment shell is capable of withstanding such challenges has not been assessed by Westinghouse in any of the documents provided.

419 Gaps not addressed quantitatively during the RGA are as follows:

- Risk associated with internal fires and other currently un-evaluated internal and external hazards.
- Risk associated with potentially correlated external hazards.
- Cross-cutting findings related to the PSA success criteria.
- Findings related to the PSA models which could not be quantified because the amount of modelling effort required was beyond the available resources.
- Potential deficiencies in areas of the PSA not reviewed.

- Scenarios for which there is no analysis available to conduct a reasonable RGA.
- Multiple errors have been found in the models although it is difficult to estimate the overall numerical impact when all of these are corrected simultaneously.
- On the other hand, it is acknowledged that conservatisms have been built in some aspects of the model and data. These have not been addressed in the RGA.

4.20.4 Conclusions

420 Based on the above, I have concluded that the AP1000 PSA needs considerable improvements to meet the expectations of ND's PSA TAG (Ref. 15) (this TAG is a compilation of good practice guidance from the international community put in the context of the UK's regulatory framework). It should be noted that the need for extensive upgrade of the PSA was already acknowledged by Westinghouse in Chapter 5.4 of the 2009 version of the PCSR (Ref. 11) and specific commitments for a future PSA update are made in Chapter 10 of the 2010 draft version of the PCSR (Ref. 12). It is understood that work is already ongoing.

421 Furthermore, the AP1000 PSA in its current state neither enables a complete and reliable comparison against the SAPs numerical targets and nor provides an effective demonstration that the AP1000 risk is ALARP. In this regard, the following should be noted:

- The estimated risk gap addressing those findings which could be evaluated quantitatively, concluded that the CDF and LRF for the AP1000 could be higher than the current figures estimated by Westinghouse, but are still lower than those figures of merit for currently operating PWRs.
- Two GDA Issues have been raised in the areas of larger uncertainty, i.e. success criteria **(GI-AP1000-PSA-01)** and Fire PSA **(GI-AP1000-PSA-02)**. In order to address these GDA Issues Westinghouse needs to consider also the IEs and consequential IEs identified as currently missing from the PSA (including the missing high energy line break scenarios).
- The AP1000 PSA is built on assumptions based on design documentation available at the time when the PSA was developed. Much of the documentation has changed since then but the PSA has not been kept in step with these changes. Also, GDA Issues have been raised in other technical areas the outcome of which may further affect the ability of the PSA in its current form to reliably predict the risk of the AP1000.
- The RGA showed a change in the AP1000 risk profile in that the frequencies of sequences with core melt at high pressure are more affected when some of the limitations and deficiencies found during the review are corrected in the model. This is an important insight from the review because a change of this nature in the risk profile may impact the decisions on whether improvements to reduce the risk are reasonably practicable.
- A number of the perceived risk gaps will depend on final detailed design, on-site specific characteristics, and / or on operational matters (procedures, maintenance schedule, refuelling outage strategy, etc).

4.21 Overseas Regulatory Interface

422 The AP1000 Multinational Design Evaluation Programme (MDEP) does not have a PSA subgroup. Therefore no formal interactions have been held with Overseas Regulators during GDA in this assessment area. Interactions of informal nature have however been held with the US-NRC PRA staff. In particular, ND's PSA team's strategy to address some concerns raised in the C&I and Fault Studies areas of GDA in relation to spurious PMS actuations was discussed with US-NRC PRA and I&C staff.

4.22 Interface with Other Regulators

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

4.23 Other Health and Safety Legislation

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

5 CONCLUSIONS

425 This report presents the findings of the Step 4 Probabilistic Safety Analysis (PSA) assessment of the Westinghouse AP1000 reactor.

426 Based on the extensive assessment, albeit on a sampling basis, of all the technical areas of the PSA, I conclude that the AP1000 PSA needs substantial improvements to be suitable to adequately support the AP1000 "generic" PCSR.

427 Furthermore, based on the results of the Risk Gap Analysis (RGA) conducted in Step 4 of GDA, the AP1000 PSA in its current state does not enable a complete and reliable comparison against the numerical targets of the SAPs (Ref. 4).

428 Two GDA Issues have been raised in two areas considered to have larger uncertainty, i.e. PSA Success Criteria **(GI-AP1000-PSA-01)** and Fire PSA **(GI-AP1000-PSA-02)**. In order to address these GDA Issues Westinghouse needs to consider also the Initiating Events (IE) and consequential IEs identified as currently missing from the PSA. Both GDA Issues include Actions requiring Westinghouse to evaluate the implications of the new analysis on the AP1000 Core Damage Frequency (CDF) and Large Release Frequency (LRF).

429 The estimated risk gap addressing the review findings which could be evaluated quantitatively in GDA, concluded that the CDF and LRF for the AP1000 could be higher than the current figures estimated by Westinghouse, but are still lower than those figures of merit for currently operating PWRs. Also, it is acknowledged that there are conservatisms in some aspects of the AP1000 PSA model and data. All this suggests that the risk associated to the AP1000 design is potentially able to meet the Basic Safety Objectives (BSO) for the Targets 7 and 9 from NT.1 of HSE's SAPs (Ref. 4). However, this conclusion is subject to the following:

- Satisfactory outcome from both GDA Issues on "PSA Success Criteria" and "Fire PSA".
- The AP1000 PSA is built on assumptions based on design documentation available at the time when the PSA was developed. The documentation has changed since then but the PSA has not been updated accordingly. Also, GDA Issues have been raised in other technical areas the outcome of which may further affect the ability of the PSA in its current form to reliably predict the risk of the AP1000.

430 In addition, the RGA showed a potential change in the AP1000 risk profile in that the frequencies of sequences with core melt at high pressure are more affected when some of the limitations and deficiencies found during the review are corrected in the model. This is an important insight from the review because a change of this nature in the risk profile may impact the decisions on whether improvements to reduce the risk are reasonably practicable.

431 It should be noted that a number of the perceived risk gaps will depend on final detailed design, on-site specific characteristics, and / or on operational matters (procedures, maintenance schedule, refuelling outage strategy, etc). So, ultimately, a "site-specific" PCSR should be in place before the start of construction of the nuclear island and this should be supported by an adequate PSA.

432 Therefore, a more complete and updated Level 1, 2 and 3 PSA (Fuel Pool, Reactor at Power, Low Power and Shutdown, Internal Events and Internal and External Hazards) should be available to support further stages of the NPP development. This should be

accompanied by ALARP evaluations to demonstrate that no further improvements to reduce the risk are reasonably practicable (or otherwise). In this regard, the milestones for a future Licensee to address the GDA Assessment Findings on PSA have been chosen to ensure that future updates of the PSA capture design, construction and operational developments and that the PSA is used to inform these as appropriate (see Appendix 1).

433 Finally:

- An updated version of the Fuel Pool PSA including as-built and as-(to be)-operated information should be available before fuel is brought into the site.
- An updated version of the Reactor at Low Power and Shutdown PSA including as-built and as-(to be)-operated information should be available before fuel is loaded into the reactor.
- An updated version of the Reactor at Power PSA including as-built and as-(to be)-operated information should be available before first criticality.

5.1 Key Findings from the Step 4 Assessment

5.1.1 Assessment Findings

434 I conclude that the Assessment Findings extensively discussed in Section 4 above and explicitly listed in Annex 1 should be programmed during the forward programme of this reactor as normal regulatory business. As indicated above, the milestones assigned to the Assessment Findings on PSA have been chosen to ensure that future updates of the PSA capture design, construction and operational developments and that the PSA is used to inform these as appropriate.

5.1.2 GDA Issues

435 I conclude that the GDA Issues discussed in Section 4 above and listed in Annex 2 must be satisfactorily addressed before a Design Acceptance Confirmation (DAC) will be granted. A DAC will be necessary for the commencement of nuclear island safety related construction.

6 REFERENCES

1 *GDA Step 4 Probabilistic Safety Analysis Assessment Plan for the Westinghouse AP1000.* HSE-ND Assessment Plan AR 09/059, Revision 1. April 2010, TRIM Ref. 2009/466174.

2 *ND BMS. Assessment Process.* AST/001 Issue 4. HSE, April 2010. http://www.hse.gov.uk/nuclear/operational/assessment/ast001.htm.

3 *ND BMS. Technical Reports.* AST/003 Issue 3, HSE. November 2009. http://www.hse.gov.uk/nuclear/operational/assessment/ast003.htm.

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

5 *Nuclear power station generic design assessment – guidance to requesting parties.* Version 3, HSE, August 2008. http://www.hse.gov.uk/newreactors/guidance.htm.

6 *Step 3 Probabilistic Safety Analysis Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/017/ November 2009. TRIM Ref. 2010/0609908.

7 *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels.* WENRA. January 2008. http://www.sujb.cz/doc/ListofreferencelevelsJanuary2008/pdf.

8 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600721.

9 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600724.

10 *Westinghouse AP1000 - Schedule of Regulatory Issues Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600725.

11 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732 Revision 2. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/23759.

12 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-793 Revision A. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/23783.

13 AP1000 Master Submission List – UKP-GW-GLX-001 Revision 0 – TRIM Ref 2011/246930.

14 *Safety Assessment and Verification for Nuclear Power Plants. Safety Guide.* International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.2. IAEA, Vienna, 2001, TRIM 2007/29995.

15 *ND BMS. Technical Assessment Guide. Probabilistic Safety Analysis.* T/AST/030 Issue 3. HSE. February 2009. http://www.hse.gov.uk/nuclear/operational/tech_asst_guides/tast030.pdf.

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

17 *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants.* IAEA Safety Standards Series, Specific Safety Guide SSG-3, International Atomic Energy Agency (IAEA). Vienna. 2010.

18 *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants.* IAEA Safety Standards Series, Specific Safety Guide SSG-4, International Atomic Energy Agency (IAEA). Vienna. 2010.

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

20 *UK AP1000 PRA Configuration Control Model.* UN REG WEC 000131. Westinghouse Electric Company LLC. February 2010. TRIM 2011/93711.

21 *UK AP1000 Probabilistic Risk Assessment.* UKP-GW-GL-022 Revision 0. Westinghouse Electric Company LLC. May 2007. TRIM Ref. 2011/81984.

22 *AP1000 PRA Protection and Safety Monitoring System (PMS).* APP-PRA-GSC-222 Revision 1. Westinghouse Electric Company LLC. September 2008. TRIM Ref. 2011/81567.

23 *AP1000 PRA Plant Control System Model.* APP-PRA-GSC-228 Revision 0. Westinghouse Electric Company LLC. May 2007. TRIM Ref 2011/466336.

24 *UK AP1000 Probabilistic Risk Assessment Update Report.* UKP-GW-GLR-102 Revision 0. Westinghouse Electric Company LLC. January 2010. TRIM Ref. 2011/93198.

25 *AP1000 PRA Quantification (includes PSA CAFTA Model Version 3B).* APP-PRA-GSC-236 Revision 1. Westinghouse Electric Company LLC. TRIM Ref. 2011/76409.

26 *Step 4 Human Factors Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-012 Revision 0. TRIM Ref. 2010/581519.

27 *Step 4 - Fault Studies – Containment and Severe Accident Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-004 Revision 0, TRIM Ref. 2010/581405.

28 *AP1000 Spent Fuel Pool Probabilistic Risk Assessment (PRA) (includes PSA CAFTA Model).* APP-PRA-GSC-400 Revision C. Westinghouse Electric Company LLC. 2009. TRIM Ref. 2011/81572.

29 *AP1000 PRA Spent Fuel Pool Evaluation.* UKP-GW-GL-743 Revision 1. Westinghouse Electric Company LLC. January 2010. TRIM Ref. 2011/93194.

30 *Regulatory Observation Action RO-AP1000-47.A1.3 – Diversity for Frequent Faults; Safety System Classification.* Letter from AP1000 Joint Programme Office to ND. WEC000258. 6 July 2010. TRIM Ref. 2010/299287.

31 *AP1000 Plant PRA Systems Analysis Guidebook.* APP-PRA-GM-004 Revision B. Westinghouse Electric Company LLC. 1 July 2010. TRIM Ref. 2011/81559.

32 *AP1000 Plant Fire PRA Model Development Guidebook*. APP-PRA-GM-010 Revision A. Westinghouse Electric Company LLC. 2010. TRIM Ref. 2011/81560.

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

34 *Review of the AP1000 PSA for Step 4 of GDA (Part 1: Level 1 PSA, Part 2: Level 2 PSA).* JEL2-HSE-1002 (Part 1 of 2) Revision 1 & JEL2-HSE-1002 (Part 2 of 2) Revision 0. Jacobsen Engineering Ltd, May & April 2011. TRIM Refs 2011/302651 & 2011/302653.

35 *Risk Gap Analysis of AP1000 PSA for Step 4 of GDA.* JEL5-HSE-1002, Revision 1, Jacobsen Engineering Ltd, May 2011. TRIM Ref. 2011/314124.

36 *Step 4 Fault Studies – Design Basis Fault Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-004a Revision 0. TRIM Ref. 2010/581406.

37 *AP1000™ Plant Probabilistic Risk Assessment, Steam Generator Tube Rupture Analysis*. APP-PRA-GSC-101 Revision 0. Westinghouse Electric Company LLC. 2010. TRIM Ref. 2011/81563.

38 *Spent Fuel Pool Boiling Frequency for the UK AP1000 Plant.* UKP-PRA-GSC-002 Revision A. Westinghouse Electric Company LLC. January 2011. TRIM Ref. 2011/91026.

39 *MAAP/NOTRUMP Benchmarking to Support the Use of MAAP4 for AP600 PRA Success Criteria Analyses.* WCAP-14869. Westinghouse Electric Company LLC. April 1997. TRIM Ref. 2011/82153.

40 *AP1000 PRA Thermal/Hydraulic Uncertainty Evaluation for Passive System reliability.* WCAP14800. Westinghouse Electric Company LLC. June 1997, TRIM 2011/82149.

41 *Success Criteria for PSA for AP1000*, GRS-V-HSE-WP11-14-14a-01. Gesellschaft fur Anlagen-und Reaktorsicherheit (GRS) mbH. January 2011. TRIM Ref. 2011/109368.

42 *Review of the UK AP1000 PRA – Internal Initiating Events during Full Power Operation*. JEL2-HSE-0309 Revision 2. Jacobsen Engineering Ltd. Stetkar J. April 2010. TRIM Ref. 2011/284471.

43 *Response to TQ-AP1000-517 – AP1000 PRA Success Criteria Documentation related to Six Initiating Event Sequences*. Westinghouse Electric Company LLC. April 2010. TRIM Ref. 2011/134233.

44 *Review of AP1000 PSA for Step 4 of GDA - Accident Sequence Development: Event Sequence Modelling (Event Trees).* Letter WEC70322N. HSE-ONR. June 2011. TRIM Ref. 2011/326417.

45 *Not used.*

46 *Review of AP1000 PSA Spurious PMS Events for Step 4 of GDA.* JEL1-HSE-1005 Revision 0. Jacobsen Engineering Ltd. February 2011. TRIM Ref. 2011/194298.

47 *AP1000 Human Factors Program and Assessment for the United Kingdom.* UKP-GW-GL-042 Revision 1. Westinghouse Electric Company LLC. TRIM Ref 2011/81992.

48 *Detailed Review of Systems Analysis for AP1000 PSA for Step 4 of GDA.* JEL2-HSE-1001 Revision 0. Jacobsen Engineering Ltd. January 2011. TRIM Ref. 2011/144423.

49 *Detailed Review of I&C Systems Analysis for AP1000 PSA for Step 4 of GDA.* JEL3-HSE-0803 Revision 0. Jacobsen Engineering Ltd. May 2011. TRIM Ref. 2011/302713.

50 *Piping and Instrumentation Diagram of the Component Cooling Water System.* APP-CCS-M6-001 Revision 4. Westinghouse Electric Company LLC. July 2009. TRIM Ref. 2011/76267.

51 *AP1000 European Design Control Document.* EPS-GW-GL-700 Revision 1. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/81804.

52 *ND BMS. Technical Assessment Guide. Human Reliability Analysis.* T/AST/063 Issue 1. HSE. March 2010. http://www.hse.gov.uk/nuclear/operational/tech_asst_guides/tast063.htm.

53 *Handbook of human reliability analysis with emphasis on nuclear power plant applications (THERP).* Swain & Guttmann. NUREG/CR-1278. 1983.

54 *Human Cognitive Reliability Model for PRA Analysis (HCR).* Hannaman & Spurgin. EPRI Project RP2170-3 draft NUS-4531. 1984a.

55 *Williams J C. A data-based method for assessing and reducing human error to improve operational performance (HEART).* Proceedings of IEEE Fourth Conference on Human Factors in Power Plants. Monterey, California. June 5-9. pp.436-450. 1988.

56 *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.* NUREG/CR-6928. INL/EXT-06-11119. February 2007.

57 *CCF Parameter Estimations. 2007 Update.* U.S. Nuclear Regulatory Commission. April 2010. http://nrcoe.inel.gov/results/index.cfm?fuseaction=ParamEstSpar.showMenu.

58 *Review of AP1000 PSA Data Analysis for Step 4 of GDA*. JEL4-HSE-1002 Revision 0. Jacobsen Engineering Ltd. January 2011. TRIM Ref. 2011/144407.

59 *McDermid J and Kelly T. Software in Safety Critical Systems*. Nuclear Future, Volume 02, No.03. http://www.cs.york.ac.uk/ftpdir/pub/hise/Software_in_Safety_Critical_Systems:Achievement_and_Prediction.pdf.

60 *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems.* IEC-61508. International Electrotechnical Commission (IEC). 2004.

61 *Step 4 Control & Instrumentation Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-006 Revision 0. TRIM Ref. 2010/581525.

62 *NRC Integrated Program for the Resolution of Unresolved Safety Issues A-3, A-4 and A-5 Regarding Steam Generator Tube Integrity: Final Report.* NUREG-0844. United States Nuclear Regulatory Commission. September 1988.

63 *AP1000 PRA Control and Instrumentation Sensitivity Cases Quantification*. APP-PRA-GSC-254 R1 Revision 1. Westinghouse Electric Company LLC. December 2009, TRIM 2011/76414.

64 *ATWS: A Reappraisal – Part 3: Frequency of Anticipated Transients.* EPRI NP-2230. Electric Power Research Institute. January 1982.

65 *Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 – 1995*. NUREG/CR-5750. 1999.

66 *Not used.*

67 *Step 4 Internal Hazards Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-001 Revision 0. TRIM Ref. 2010/579786.

68 *Internal Hazards Topic Report.* UKP-GW-GLR-001 Revision 2. Westinghouse Electric Company LLC. 30 September 2010. TRIM Ref. 2011/82084.

69 *Guidelines for the performance of Internal Flooding Probabilistic Risk Assessment.* EPRI-TR-101314. EPRI, Palo Alto, CA: 2009:1019194.

70 *AP1000 Plant Internal Flooding PSA.* White Paper Submitted in Response to TQ-AP1000-825. Westinghouse Electric Company LLC. August 2010. TRIM Ref. 2011/94339.

71 *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME RA-Sa-2009 Addenda to ASME RA-S-2008. The American Society of Mechanical Engineers. February 2009.

72 *AP1000 External Hazards Topic Report*. UKP-GW-GL-043 Revision 0. Westinghouse Electric Company LLC, December 2009. TRIM Ref. 2009/503652.

73 *Review of Selection and Screening Methodology Applied to External Hazards within the AP1000 Probabilistic Risk Assessment*. ABS Report Number 2342643-R-02 Issue 1. March 2011. TRIM Ref. 2011/19441.

74 *AP1000 European Design Control Document.* EPS-GW-GL-700 Revision 0. Westinghouse Electric Company LLC. February 2009. TRIM Ref 201/384093.

75 *ND BMS. Technical Assessment Guide. External Hazards.* T/AST/013 Issue 3. HSE. April 2010. http://www.hse.gov.uk/nuclear/operational/tech_asst_guides/tast013.htm.

76 *AP1000 Seismic Margin HCLPF Calculations.* APP-PRA-GSR-002 Revision 2, 3 and 4. Westinghouse Electric Company LLC. TRIM Ref. 2011/94124, 2011/81574, 2011/94125.

77 *AP1000 PRA-Based Seismic Margins Assessment Update*. APP-PRA-GSC-027, Revision 1. Westinghouse Electric Company LLC. October 2010. TRIM Ref 2011/467145.

78 *AP1000 Seismic Margins Assessment: GDA Review of Seismic Fragility Derivation.* ABS Report No 2342643-R-03 Issue 1. July 2011. TRIM Ref. 2011/19449.

79 *Detailed Review of Seismic Analysis for AP1000 PSA for Step 4 of GDA.* JEL1-HSE-1001 Revision 0. Jacobsen Engineering Ltd. May 2011. TRIM Ref. 2011/302727.

80 *Advanced Light Water Reactor Utility Requirements Document*. Volume III. ALWR Passive Plant. Chapter 1 Appendix A. PRA Key Assumptions and Ground-rules. EPRI Palo Alto. Revisions 5 & 6. Issued December 1993.

81 *Low Power and Shutdown Assessment for Revision 4 of the AP600 PSA Levels 1 and 2*. PRA-GSC-249 Revision 1. Westinghouse Electric Company LLC. 1995. TRIM Ref 2011/466586.

82 *Re-submittal of Response to RO-AP1000-54 – Shutdown & Spent Fuel Pool Faults and Regulatory Observation Actions RO-AP1000-54.A1.1 and A2.1*. UN REG WEC 000310. Westinghouse Electric Company LLC. 2010, TRIM 2010/385305.

83 *AP1000 Shutdown & Spent Fuel Pool Faults (Response to RO-AP1000-54)*. UKP-GW-GL-077 Revision A. Westinghouse Electric Company LLC. October 2010. TRIM Ref. 2011/82079.

84 *Response to RO-AP1000-46 and RO-AP1000-46.A1.1 – List of Design Basis Initiating Events Following ND Comments on the Westinghouse Response of 28 May 2010*. UN REG WEC000290, TRIM 2010/351527.

85 *Revised Full Response to RO-AP1000-54 Shutdown and Spent Fuel Pool Design Basis Analysis*. Letter from AP1000 Joint Programme Office to ND. 000496. January 2011. TRIM Ref. 2011/71266.

86 *Probabilistic safety assessments of nuclear power plants for low power and shutdown modes*. IAEA-TECDOC-1144. International Atomic Energy Agency (IAEA). Vienna, 2000.

87 *Review of the AP1000 Shutdown and Fuel Pool PSA for Step 4 of GDA,* JEL3-HSE-1002 Revision 0. Jacobsen Engineering Ltd. November 2010. TRIM Ref. 2010/627006.

88 *White Paper. AP1000 Plant High Point Risk Estimates for Shutdown Plant Operating States. (Supports response to TQ-AP1000-950)*. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/94676.

89 *AP1000 Shutdown & Spent Fuel Pool Faults.* UKP-GW-GL-077 Revision 0. Westinghouse Electric Company LLC. January 2011. TRIM Ref. 2011/91027.

90 *Step 4 Radiological Protection Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-009 Revision 0. TRIM Ref. 2010/581522.

91 *WinNUCAP Version 1.0 Users' Manual*. Scientech Inc. May 2000. http://winnupra.scientech.us/winnucap.htm.

92 *AP1000 In-Vessel Retention of Molten Core Debris (IVR): The Impact of Lower Plenum Debris Bed Chemistry and Mixing Uncertainties on Reactor Vessel Integrity during a Core Melt*. EPS-PRA-GSC-306 Revision 0. Westinghouse Electric Company LLC. 2010. TRIM Ref. 2011/81844.

93 *GDA Step 4 Phase 1 Review of the AP1000 Level 2 PSA.* JEL1-HSE-0803-2 Revision 0. Jacobsen Engineering Ltd. June 2010. TRIM Ref. 2011/284459.

94 *GDA Step 4 Review of AP1000 Level 2 PSA Analyses Related to In-Vessel Retention.* JEL1-HSE-1002 Revision 1. Jacobsen Engineering Ltd. June 2011. TRIM Ref. 2011/326062.

95 *AP1000 Generic Design Assessment (GDA) - Level 2 Probabilistic Safety Assessment (PSA) Support - Containment Fragility Review.* ABS Report 2342643-R-06 Issue 1. June 2011. TRIM Ref. 2011/302742.

96 *Risk Informed Evaluation of Extensions to Containment Isolation Valve Completion Time*. WCAP15791-P-A Revision 2. Westinghouse Electric Company LLC. 2008. TRIM 2011/133476

97 *MELCOR Calculations Supporting the NRC/NRR AP600 Design Certification Review.* ITS/SNL-95-006. Sandia National Laboratories. August 1995.

98 *UK AP1000 Design Change Proposal Review for PRA and Severe Accident Impact.* UKP-PRA-GER-001. Revision 0. Westinghouse Electric Company LLC. January 2010. TRIM Ref. 2011/93201.

99 *AP1000 Severe Accident Source Term to the Environment Calculation with MAAP4.04*. APP-PRA-GSC-206. Revision 0. Westinghouse Electric Company LLC. 2007. TRIM Ref. 2011/81565.

100 *Oracle Crystal Ball Fusion Edition.* http://download.oracle.com/docs/cd/E17236_01/epm.1112/cb_user/frameset.htm?index.html.

101 *GDA Issue GI-UKEPR-PSA-01 Revision 0. Background and explanatory information.* TRIM Ref. 2011/81141.

102 *GDA Issue GI-UKEPR-PSA-02 Revision 0. Background and explanatory information.* TRIM Ref. 2011/81148.

103 *Review of Level 3 PSA for Generic Design Assessment Step 4 Westinghouse AP1000 Reactor Design,* CRCE-EA-5-2011. Health Protection Agency Centre for Radiation, Chemical and Environmental Hazards. TRIM Ref. 2011/414220.

Table 1

GDA Supporting Documentation for Probabilistic Safety Analysis Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
See paragraphs 14 and 15 in Section 2.3 of the main body of this Assessment Report and Westinghouse's documents included in the list of references.	

Table 2

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

SAP No. and Title	Description	Interpretation	Comment
FA.10 **Fault analysis: PSA** **Need for a PSA**	"Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis"	This principle sets the framework and requirements for a PSA study. The overriding aim of the PSA assessment is to assist ND judgements on the safety of the facility and whether the risks of its operation are being made as low as reasonably practicable.	Addressed in Section 3 of this report. The need for PSA has been recognised from the outset. However this assessment report concludes that the PSA is not yet suitable or sufficient to support the AP1000 PCSR. Hence the SAP is not fully met.
FA.11 **Fault analysis: PSA Validity**	"PSA should reflect the current design and operation of the facility or site"	This principle establishes the need for each aspect of the PSA to be directly related to existing facility information, facility documentation or the analysts' assumptions in the absence of such information. The PSA should be documented in such a way as to allow this principle to be met.	Addressed in the various sub-sections in Section 4 of this report. The PSA provided has not yet been updated to reflect the current stage of the design, so the SAP is not fully met.
FA.12 **Fault analysis: PSA** **Scope and extent**	"PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site"	In order to meet this principle the scope of the PSA should cover all sources of radioactivity at the facility (e.g. fuel ponds, fuel handling facilities, waste storage tanks, radioactive sources, reactor core, etc), all types of initiating faults (e.g. internal faults, internal hazards, external hazards) and all operational modes (e.g. nominal full power, low power, shutdown, start-up, refuelling, maintenance outages).	Addressed in Section 4.2 of this report. The scope of the PSA needs some extensions for this SAP to be fully met.

Table 2

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

SAP No. and Title	Description	Interpretation	Comment
FA.13 **Fault analysis: PSA Adequate representation**	"The PSA model should provide an adequate representation of the site and its facilities"	The aim of this principle is to ensure the technical adequacy of the PSA. Inspectors should review PSA models, data and results to be satisfied that the PSA has a robust technical basis and thus provides a credible picture of the contributors to the risk from the facility.	Section 4 of this report is almost entirely devoted to this SAP. Since two GDA Issues have been raised, it can be concluded that the PSA needs improvements to be totally adequate for GDA. Hence the SAP is not fully met.
FA.14 **Fault analysis: PSA** **Use of PSA – FA.14**	"PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities"	The aim of this principle is to establish the expectations on what uses the duty-holders should make of the PSA to support decision-making and on how the supporting analyses should be undertaken.	There is evidence that the PSA has been used in the design process and in this respect the SAP is met. Many of the assessment findings are aimed at ensuring the PSA is developed sufficiently to aid operational safety decisions in the future.
Numerical Targets NT.1	**Target 7:** Individual risk to people off the site from accidents	BSL 10^{-4}/yr BSO 10^{-6}/yr	Addressed in Sections 2.3.6, 4.18, 4.19, 4.20

Table 2

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

<table>
<tr><th>SAP No. and Title</th><th>Description</th><th>Interpretation</th><th>Comment</th></tr>
<tr><td rowspan="2"></td><td>Target 8: Frequency dose targets for accidents on an individual facility – any person off the site</td><td><table>
<tr><td></td><td>BSL</td><td>BSO</td></tr>
<tr><td>Offsite dose 0.1-1 mSv</td><td>1</td><td>10^{-2}</td></tr>
<tr><td>Offsite dose 1-10 mSv</td><td>10^{-1}</td><td>10^{-3}</td></tr>
<tr><td>Offsite dose 10-100 mSv</td><td>10^{-2}</td><td>10^{-4}</td></tr>
<tr><td>Offsite dose 100-1000 mSv</td><td>10^{-3}</td><td>10^{-5}</td></tr>
<tr><td>Offsite dose >1000 mSv</td><td>10^{-4}</td><td>10^{-6}</td></tr>
</table></td><td rowspan="2">and 5 of this report.

The PSA has not been designed to allow a realistic and complete comparison against Targets 7, 8 and 9. Further improvements to the PSA will be required to facilitate this comparison.

However, the RGA has provided certain confidence that the AP1000 design might be able to meet the BSOs for Targets 7 and 9.</td></tr>
<tr><td>Target 9: Total risk of 100 or more fatalities</td><td>BSL 10^{-5}/yr BSO 10^{-7}/yr</td></tr>
</table>

Table 2

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

SAP No. and Title	Description	Interpretation	Comment
Numerical Target NT.2	Sufficient control of radiological hazards at all times	Sufficient protection based on engineering and operational features. Avoidance of High point in time risks that would exceed BSLs if evaluated as continuous risks	Addressed in Sections 2.3.6 and 4.15 of this report. Within GDA this was explored for shutdown states, when the point-in-time risk could approach or slightly surpass the BSLs figures when maximum allowed systems unavailabilities are assumed. This has not raised concerns within GDA space because, given the estimated risk for this reactor, the future licensee/s will be able to manage the operational risk and keep it ALARP at all times.

DEFINITIONS	
Type A HFE	Human action before the accident that causes equipment or systems to be unavailable when required post fault
Type B HFE	Human action that either by itself or in combination with equipment failures leads to an initiating event
Type C HFE	Human action occurring post-fault. This can be an error that occurs while performing safety actions or it can be an action that aggravates the fault sequence

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-1. General Expectations		
Table A1-1.1 Approaches and Methodologies		
AF-AP1000-PSA-001	The Licensee shall provide an enhanced PRA System Analysis Guidebook to provide wider and more detailed guidance and to remove instructions potentially leading to models which are optimistic or limited to support operational decisions.	Nuclear island safety related concrete
AF-AP1000-PSA-002	The Licensee shall implement and provide task procedures for all the technical areas of the PSA.	Nuclear island safety related concrete
Table A1-1.2 PSA Scope		
AF-AP1000-PSA-004	Before pouring nuclear island safety related concrete the Licensee shall provide evidence that a full scope site-specific PSA is in place or a demonstration that the scope of the PSA at the start of nuclear safety related construction is representative of the installation being constructed, is bounding and provides sufficient insights into the relative vulnerabilities and strengths of the plant design in the specific site.	Nuclear island safety related concrete
AF-AP1000-PSA-005	The Licensee shall provide a full scope PSA for the AP1000.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-006	The Licensee shall provide an evaluation of the frequency of, and radiological releases and consequences from, AP1000 accident sequences without core damage.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-1.3 Freeze Date		
AF-AP1000-PSA-003	The Licensee shall provide a “site-specific” PCSR PSA whose freeze date is consistent with the design freeze date.	Nuclear island safety related concrete

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-1.4 Computer Codes and Inputs		
AF-AP1000-PSA-007	The Licensee shall provide an electronic model of the complete AP1000 PSA making the best possible use of the PSA software capabilities regarding the integration between event trees and fault trees and including clear descriptions for all the basic events and gates.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-008	The Licensee shall provide a revised demonstration that the limitations of the codes selected to undertake the thermal-hydraulic and neutronics analyses for the PSA do not impact the AP1000 PSA success criteria.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-009	The Licensee shall provide revised ATWS success criteria analyses using a best estimate code.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-010	The Licensee shall provide revised PSA documentation including information on: 1) validation and verification for all the codes used; 2) plant nodalization and plant parameter files for all the codes used; and 3) showing full traceability between the PSA models and the supporting analyses.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2. Level 1 PSA		
Table A1-2.1 Identification and Grouping of Initiating Faults		
AF-AP1000-PSA-011	The Licensee shall put in place a robust process for identification and grouping of Initiating Events and shall provide revised PSA documentation describing in detail such process.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-012	The Licensee shall provide a revised PSA taking into consideration all the Initiating Events and consequential Initiating Events which have been identified as missing (both by the GDA review and by themselves using the enhanced process for identification and grouping of IEs as per previous finding).	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-013	The Licensee shall provide a revised list of Initiating Events for the PSA correctly grouped.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-014	The Licensee shall provide revised documentation of the PSA task on Identification and Grouping of Initiating Events taking into account commitments made and relevant technical information provided in responses to TQ-AP1000-094 to 127.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.2 Accident Sequence Development: Determination of Success Criteria		
N/A	GDA Issue.	
Table A1-2.3 Accident Sequence Development: Event Sequence Modelling		
AF-AP1000-PSA-015	The Licensee shall provide revised documentation of the PSA Event Sequence Modelling presenting justification and full traceability between all aspects of the event sequence models and the supporting analyses.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-016	The Licensee shall provide revised documentation of the PSA Event Sequence Modelling including a collated and clear description of general assumptions used.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-017	The Licensee shall provide revised documentation of the PSA Event Sequence Modelling including a complete and clear description of the treatment of dependencies. The Licensee shall provide revised AP1000 PSA event sequence models, as appropriate, with correct treatment of dependencies.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-018	The Licensee shall provide revised documentation of the PSA Event Sequence Modelling showing clear links between all aspects of the event sequence models and relevant operating and emergency procedures.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-019	The Licensee shall provide revised and documented PSA event sequence models including adequate treatment of consequential events.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-020	The Licensee shall provide revised and documented PSA event sequence heading models (functional fault trees) addressing all the errors and inconsistencies identified in the GDA review and ensuring that all the PSA heading models that could be affected (as well as those reviewed during GDA) are also revised.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-021	The Licensee shall provide revised and documented PSA event trees addressing all the errors and inconsistencies identified in the GDA review and ensuring that all the PSA event trees that could be affected (as well as those reviewed during GDA) are also revised.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-022	The Licensee shall provide revised PSA event trees where the Late Containment Failure sequences are treated as core damage sequences and are transferred to the Level 2 PSA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-023	The Licensee shall provide revised and documented PSA event trees taking into account 1) specific shortcomings identified in TQs raised in this area; 2) shortcomings relevant to the sequence modelling identified in TQs related to PSA success criteria, 3) commitments made by Westinghouse in the TQ responses; and 4) relevant technical information provided in response to the TQs and ROs. Relevant TQs and ROs in this area are: TQ-AP1000-348, 351, 352, 433, 517, 572 to 582, 584 to 589, 863 to 876, 880 to 898, 914 to 924, 1006 to 1008, 1012 to 1015, 1020, 1025 to 1027, RO-AP1000-072 and RO-AP1000-099.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-024	The Licensee shall provide revised and documented PSA event trees for ATWS Initiating Events taking into account specific shortcomings identified by the TSCs during the reviews of the AP1000 PSA Event Sequence Modelling and Success Criteria. These are documented in Ref. 34, PTQ-AP1000-AS-38 to 49, and in Ref. 41, Part-2-PTQs 73 to 95.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.4 System Analysis		
AF-AP1000-PSA-025	The Licensee shall provide revised PSA Systems Analysis documentation including the following: system boundaries and interfaces, component boundaries, FMEAs, complete dependency matrices, details of system testing and maintenance.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-026	The Licensee shall provide revised systems fault trees consistent with the UK-AP1000 design and including complete modelling of failures (pre-accident human errors, structural failures, passive failures, indication failures, unavailabilities due to testing and maintenance, common cause failures), and removal of modular events, unnecessary simplifications and asymmetries.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-027	The Licensee shall provide revised and documented PSA fault trees for the Passive Cooling Systems taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-028	The Licensee shall provide revised documented PSA Fault Trees for the Start-up Feedwater System taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-029	The Licensee shall provide revised documented PSA Fault Trees for the AC Power System and Diesel Generators taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-030	The Licensee shall provide revised documented PSA Fault Trees for the Component Cooling Water (CCS) and Service Water (SWS) Systems taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-031	The Licensee shall provide revised documented PSA Fault Trees for the Protection and Safety Monitoring System (PMS), Plant Control System (PLS) and Diverse Actuation System (DAS) taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-032	The Licensee shall provide revised documented PSA Fault Trees taking into account 1) specific shortcomings identified in TQs raised in this area; 2) commitments made by Westinghouse in the TQ and RO responses; and 3) relevant technical information provided in response to the TQs. Relevant TQs and ROs in this area are: TQ-AP1000-359 to 365, TQ-AP1000-854 to 861, and RO-AP1000-045.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.5 Human Reliability Analysis		
AF-AP1000-PSA-033	The Licensee shall provide revised values for the Human Error Probabilities in the PSA with correct conversion of medians into means.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-034	The Licensee shall provide a revised method for the evaluation of probabilities for pre-accident HFEs using an HRA method consistent with the one used in the rest of the HRA in the PSA. The method should be applied to all the Type A HFEs in the PSA and should realistically take into account the frequency and ability of the credited tests and surveillances to identify and correct latent human errors.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-035	The Licensee shall provide PSA documentation with a clear mapping between the specific aspects of the PSA model and any supporting Human Factors analyses.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.6 Data Analysis		
Table A1-2.6.1 Initiating Fault Frequencies		
AF-AP1000-PSA-036	The Licensee shall provide revised frequencies, properly justified and documented, for all the Initiating Events in the PSA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-037	The Licensee shall provide revised probabilities, properly justified and documented, for all the consequential Initiating Events in the PSA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.6.2 Random Component Failures		
AF-AP1000-PSA-038	The Licensee shall provide revised mission times consistent with the evolution of the accident sequences.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-039	The Licensee shall provide revised reliability data, properly justified and documented, for all the random component failures in the PSA. The Licensee shall justify the reliability model used on a case by case basis.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.6.3 Unavailabilities Due to Testing and Maintenance		
AF-AP1000-PSA-040	The Licensee shall provide revised unavailabilities due to testing and maintenance properly justified and documented.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.6.4 Common Cause Failures		
AF-AP1000-PSA-041	The Licensee shall provide revised and documented Common Cause Failure modelling taking into account all component types, and considering, on a case by case basis, all coupling mechanisms and defences in place against these.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-042	The Licensee shall provide revised CCF probabilities properly justified and documented.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-2.7 Analysis of Hazards		
Table A1-2.7.1 General (Screening of Internal Hazards)		
AF-AP1000-PSA-043	The Licensee shall provide a systematic screening of all internal hazards, representative of the design and layout of the AP1000 and a demonstration that the risk associated with all the screened out internal hazards would be insignificant compared to the AP1000 total risk.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-044	The Licensee shall provide a PSA for the internal hazards that have been screened in according to the stated criteria.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.7.2 Analysis of Internal Fires		
GDA ISSUE	GDA Issue.	
Table A1-2.7.3 Analysis of Internal Flooding		
AF-AP1000-PSA-045	The Licensee shall provide a modern complete and well documented Internal Flooding PSA representative of the design and layout of the AP1000.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.7.1 General (Screening of External Hazards)		
AF-AP1000-PSA-046	The Licensee shall provide a systematic screening of external hazards considering the specific characteristics of the site. The analysis should also address external hazards that could be correlated. The Licensee shall provide a demonstration that the risk associated with all the external hazards screened out would be insignificant compared to the AP1000 total risk.	Nuclear island safety related concrete
AF-AP1000-PSA-047	The Licensee shall provide a PSA for the external hazards and combination of external hazards that have been screened in according to the stated criteria. The analysis should address the potential for consequential internal hazards.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
Table A1-2.7.4 Seismic Analysis		
AF-AP1000-PSA-048	The Licensee shall provide a consolidated report collating all the seismic fragility analyses and a process to update it in the future as required to address the concern raised by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-049	The Licensee shall provide a Seismic PSA for the site. The study should address other external hazards that could occur in correlation with the seismic events, and also induced internal hazards.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.8 Low Power and Shutdown Modes		
AF-AP1000-PSA-050	The Licensee shall provide a full scope, modern and well documented Low Power and Shutdown PSA specific for the AP1000.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.8 Spent Fuel Pool PSA		
AF-AP1000-PSA-052	The Licensee shall provide a full scope, modern and well documented Spent Fuel Pool PSA for the AP1000, including evaluation of fuel damage, radioactive releases and consequences.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-2.9 Uncertainty Analyses, Quantification and Interpretation of the PSA Results		
AF-AP1000-PSA-053	The Licensee shall provide justified probability distributions for all the basic events in the PSA and full propagation of parametric uncertainties thorough the model.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-054	The Licensee shall provide a collated list of assumptions and sources of uncertainty in the PSA, a comprehensive set of sensitivity analyses and revised documentation of the AP1000 PSA results including discussions of the key areas of uncertainty and what is being done to reduce them (if necessary), and justification of the robustness of the PSA results.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-055	The Licensee shall provide clarity on the cut-off/s used in the PSA quantification and justification of its / their adequacy.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-3. Level 2 PSA		
AF-AP1000-PSA-056	The Licensee shall provide revised documentation of the Level 2 PSA taking into account commitments made and relevant technical information provided in responses to TQ-AP1000-334 to 348, 570, 757 to 759, 780 to 786, 1059, 1100, 1195, 1249 and 1250.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-3.1 Interface Between Level 1 and Level 2 PSA		
AF-AP1000-PSA-057	The Licensee shall provide revised documentation of the interface between the Level 1 and Level 2 PSA including clear characterisation of the Plant Damage States (PDS), and description and justification of the final PDS groups and the process for their development.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-058	The Licensee shall provide a revised analysis of the interface between the Level 1 and Level 2 PSA addressing the specific shortfalls identified in the GDA review regarding allocation of Level 1 PSA sequences into Plant Damage States and transfer of PDSs into the Level 2 PSA models.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-059	The Licensee shall provide a revised PSA including treatment of dependencies between the human actions before and after core damage.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-3.2 Deterministic Accident Progression Analysis		
AF-AP1000-PSA-060	The Licensee shall provide revised documentation of the diffusion flame phenomena in the Level 2 PSA. This should include clarification and justification of the scope of the scenarios considered and the analysis undertaken, and justification of the relevant success criteria and failure probabilities for venting mechanisms.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-061	The Licensee shall provide revised analysis of the hydrogen phenomena in the Level 2 PSA specific for the AP1000 and using an updated method.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-062	The Licensee shall provide a revised analysis of the probability of failure of IVR for the Level 2 PSA addressing the missing uncertainties and including an evaluation of the probability of metal layer thinning.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-064	The Licensee shall provide an improved analysis of the dry containment response to support the evaluation of failure probability of the containment in dry shell scenarios in the Level 2 PSA. This should address selection and justification of an appropriate bounding sequence for the analysis. It should also address the flow resistance in the air baffle area taking into account the gap allowed by the pressures in the relevant scenarios.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-3.3 Containment Performance Analysis		
AF-AP1000-PSA-065	The Licensee shall provide a revised and documented AP1000 containment performance analysis for the Level 2 PSA addressing the shortcomings identified in the GDA review.	Containment pressure test
Table A1-3.4 Probabilistic Modelling Framework – Accident Progression Event Trees		
AF-AP1000-PSA-066	The Licensee shall provide revised documentation of the Level 2 PSA showing clear links between the relevant parts of the Containment Event Trees and the Severe Accident Management Guidelines.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-067	The Licensee shall provide revised and documented AP1000 Containment Event Trees expanded to more realistically reflect the evolution of sequences with IVR failure, core damage at high pressure, and failure of passive containment cooling.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-068	The Licensee shall provide a justification that the probabilities assigned to the individual nodes in the Containment Event Tree are based on a consistent scale.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-069	The Licensee shall provide revised criteria for screening of containment penetrations for the purpose of containment isolation. Separate justifications should be provided for the criteria used for the Level 1 and Level 2 PSA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-070	The Licensee shall provide revised and documented PSA fault trees for the Containment Isolation taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-071	The Licensee shall provide revised and documented PSA fault trees for the Containment Hydrogen Control System taking into account the shortcomings identified by the GDA review.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-072	The Licensee shall provide specific analysis to justify the time windows for all the human actions credited in the Level 2 PSA model.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-073	The Licensee shall provide an updated AP1000 Level 2 PSA reflecting the modified IVR success criteria as per Ref. 92. For the development of the modified model the Licensee shall address the shortcomings identified during the GDA review of Ref. 92.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-063	The Licensee shall provide a revised Level 2 PSA model expanded to account for additional IVR failure sequences.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-3.5 Source Term Analysis		

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-074	The Licensee shall provide revised Source Term analysis for the AP1000 Level 2 PSA addressing the shortcomings identified during the GDA review. The analysis should be of sufficient scope and level of detail to allow a meaningful comparison against the numerical targets of the SAPs.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-3.6 Presentation and Interpretation of the Level 2 PSA Results		
AF-AP1000-PSA-075	The Licensee shall provide revised documentation of the AP1000 Level 2 PSA including a thorough and complete description of the results and the conclusions obtained.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-076	The Licensee shall provide AP1000 Level 2 PSA results including presentation of the propagation of uncertainties throughout the complete PSA model.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-077	The Licensee shall provide a demonstration that the risk of radioactive release for the AP1000 is ALARP taking into account the overall results from the PSA.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-4. Level 3 PSA		
AF-AP1000-PSA-078	The Licensee shall provide a Level 3 PSA that addresses site specific analyses of frequency for relevant fault sequences, using site specific dispersion and consequence modelling parameters, with assessed outcomes commensurate with the UK framework.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
Table A1-5 Overall Conclusions from the PSA		
AF-AP1000-PSA-079	The Licensee shall provide evidence that independent detailed reviews of all aspects of the AP1000 PSA have been undertaken.	Mechanical, Electrical and C&I Safety Systems, Structures and Components –delivery to Site
AF-AP1000-PSA-080	The Licensee shall implement and provide the procedure to maintain the PSA and keep it Living.	Nuclear island safety related concrete
AF-AP1000-PSA-081	The Licensee shall implement and provide the procedure for the use of the PSA to support all aspects of design and operation of the NPP.	Nuclear island safety related concrete

Annex 1

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

Probabilistic Safety Analysis – AP1000

Finding No	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-PSA-082	The Licensee shall provide an updated version of the Fuel Pool PSA including as-built and as-(to be)-operated information before fuel is brought into the site.	Fuel on-site
AF-AP1000-PSA-083	The Licensee shall provide an updated version of the Reactor at Low Power and Shutdown PSA including as-built and as-(to be)-operated information before fuel is loaded into the reactor.	Fuel load
AF-AP1000-PSA-084	The Licensee shall provide an updated version of the Reactor at Power PSA including as-built and as-(to be)-operated information before first criticality.	Initial criticality
Table A1-6 Use of PSA to Support Decision-Making		
AF-AP1000-PSA-051	The Licensee shall implement a risk monitor (covering full power, low power, shutdown, reactor and spent fuel pool) and the necessary procedure/s to manage the risk at all times.	Power raise

Notes

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

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

2 Table numbers refer to tables in T/AST/030 (Ref. 15).

Annex 2

GDA Issues – Probabilistic Safety Analysis – AP1000

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A1**
GDA Issue	The AP1000 PSA should be supported by design specific analysis of sufficient detail and scope and fully traceable. During our assessment we have compiled evidence that the Success Criteria for the AP1000 PSA does not meet our expectations. Deficiencies have been found in the following areas: • Demonstration of overall success of sequences. • Use of AP600 analysis without visible justifcation or sufficient evidence of applicability. • Coverage of faults. • Justification of time windows for operator actions. • Traceability of the analysis.		
GDA Issue Action	Westinghouse should provide the procedure (Guidebook) established to guide the development of success criteria for the AP1000 PSA. The guidebook should provide clear information on: • The methods to be used for the derivation of the success criteria. • The code/s to be used for derivation of the success criteria including how the analysis should deal with the limitations of the code/s. • Clear definition of the meaning of “success”. • How the operator time windows will be evaluated. • How the success criteria analyses will be documented. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A2**
GDA Issue Action	Westinghouse should provide the AP1000 Input deck/s (parameter file/s) for the code/s to be used. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A3**
GDA Issue Action	Westinghouse should provide a complete list of Initiating Events (IEs) correctly grouped, details of the success sequences & event tree headings to be evaluated including a demonstration that the analysis (both thermal-hydraulic and neutronics) is sufficient to support the success criteria for all the accident sequences in the AP1000 PSA. The review of the AP1000 PSA conducted in GDA identified a number of Initiating Events missing from the PSA and a number of IEs incorrectly grouped. In addition, the Risk Gap Analysis undertaken by ONR's PSA team in the framework of GDA has concluded that the missing IEs could have an important contribution to the AP1000 risk. In order to properly address the success criteria GDA Issue and to ensure completeness, Westinghouse should include in the success criteria evaluations the missing initiating events as appropriate and should also show that the IE grouping is correct for the purpose of success criteria evaluation. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A4**
GDA Issue Action	Westinghouse should provide the success criteria analyses and results for Loss of Coolant Accidents (LOCA). • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • A demonstration should be included that sufficient analysis has been performed to cover all the variety of LOCAs in the PSA (ie, LOCAs of different sizes and in different locations). • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A5**
GDA Issue Action	Westinghouse should provide the success criteria analyses and results for Transients. • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • A demonstration should be included that sufficient analysis has been performed to cover all the variety of (intact primary and secondary circuit) transients in the PSA including the transients currently missing from the PSA which were identified during ONR's GDA review. • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A6**
GDA Issue Action	Westinghouse should provide the success criteria analyses and results for Steam Line Breaks. • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • A demonstration should be included that sufficient analysis (both thermal-hydraulic and neutronics) has been performed to cover all the variety of steam line breaks in the PSA (eg, steam line breaks dowsntream of the MSIVs, upstream of the MSIVs both inside and outside containment, spurious opening of valves in the secondary circuit, double steam line breaks in the containment, feed water line breaks grouped together with steam line breaks in the PSA, feed water line breaks occurring as a consequence of steam line breaks, etc). • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A7**
GDA Issue Action	Westinghouse should provide the success criteria analyses and results for Steam Generator Tube Ruptures (SGTR). • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • A demonstration should be included that sufficient analysis (both thermal-hydraulic and neutronics) has been performed to cover all the variety of SGTRs in the PSA (including consequential SGTRs). • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A8**
GDA Issue Action	Westinghouse should provide the success criteria analyses and results for Anticipated Transients Without SCRAM (ATWS). • The sequence assumptions should be justified and clearly documented. • Time-lines should be provided with clear link to relevant procedures, clues for operator actuation etc. • A demonstration should be included that sufficient analysis (both thermal-hydraulic and neutronics) has been performed to cover all the variety of ATWS in the PSA. • The delineation of time windows for operator actuation has to be clearly documented. • The minimum equipment requirement and performance for success should be clearly documented. • Any conservatisms in the analysis should be described together with a justification that they are not important enough to bias the results of the analysis. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A9**
GDA Issue Action	Westinghouse should develop a Gap Analysis to evaluate the implications of the new analysis on the AP1000 Core Damage Frequency (CDF) and Large Release Frequency (LRF) (including development and quantification of new and modified event trees as necessary). With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SUCCESS CRITERIA FOR THE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-01 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-PSA-01**	**GDA Issue Action Reference**	**GI-AP1000-PSA-01.A10**
GDA Issue Action	Westinghouse should complete the documentation and provide a stand alone document compiling all the PSA Success Criteria Analysis and Gap Analysis performed accompanied by the supporting references. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A1**
GDA Issue	From the GDA assessment of the AP1000 PSA it cannot be concluded that the current prediction of internal fire risk is representative for the AP1000. This leaves ONR with a lack of understanding of the potential gap between the current estimated AP1000 risk associated with internal fires, and the AP1000 fire risk based on an up-to-date, realistic and complete evaluation. Since the current prediction of the fire Core Damage Frequency (CDF) is 5E-08/yr (approx 25% of the overall CDF) the uncertainty in the fire risk translates directly into uncertainty in the overall plant risk. Therefore a modern standards Fire PSA should be developed for the AP1000 to close this gap.		
GDA Issue Action	Westinghouse should provide the final approved procedure (Guidebook) established to guide the development of Fire PSA for the AP1000 PSA. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A2**
GDA Issue Action	Westinghouse should provide detailed information on the Database/s established / selected to be used to support the Fire PSA. The database/s should be populated with up-to-date design information. Example of information expected to be found in the database/s selected or developed to support the Fire PSA include: • List of fire PSA components and failure modes. • Circuit analysis, cable selection and routing process (with identification of uncertainties). • Physical characteristics of the fire compartments and their inventories, barriers and penetrations, ignition sources, transient combustibles, etc. • Equipment & power supplies location. Data on relevant fire events in other NPPs. A database of assumptions should also be developed. This should provide clarity on: • General assumptions of the fire PSA analysis. • The type of assumptions (related to design, operation, fire impact, etc). • Specific information on those assumptions that are not yet substantiated in specific design documentation. • Pointers to the area of the Fire PSA where the specific assumptions are used. It is expected that the assumptions database (updated as appropriate) should feature in most of the deliverables for relevant GDA Issue Actions. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A3**
GDA Issue Action	Westinghouse should provide information (including a programme of work) of the modifications to the internal events PSA model required to support the development of the Fire PSA. This should address the following: • Updates to the internal events PSA model and data to comply with Westinghouse's PSA Guidebooks which are required to support the development of the Fire PSA. • Updates to the internal events PSA model and data to address relevant findings from ONR's review of the AP1000 PSA during GDA, which are required to support the development of the Fire PSA. This should include completion of the list of Initiating Events and associated models as required. • Specific changes to the internal events PSA required by the Fire PSA itself. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A4**
GDA Issue Action	Westinghouse should provide detailed documentation of any qualitative screening of fire compartments including the screening criteria used and assumptions made. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A5**
GDA Issue Action	Westinghouse should undertake and document thoroughly an evaluation of Hot Shorts that could impact the risk associated to internal fires. ONR would expect Westinghouse to convene an expert panel to address single and multiple spurious actuation issues which may impact one or more safety functions (Note this would also be a requirement to support a modern deterministic safe shutdown analysis; albeit extended to address additional systems considered within the fire PSA). With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A6**
GDA Issue Action	Westinghouse should provide detailed documentation on the Evaluation of Fire frequencies. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A7**
GDA Issue Action	Westinghouse should provide detailed documentation of any quantitative screening of fire compartments including the screening criteria used. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area	**PROBABILISTIC SAFETY ASSESSMENT**		
Related Technical Areas	Internal Hazards		
GDA Issue Reference	**GI-AP1000-PSA-02**	GDA Issue Action Reference	**GI-AP1000-PSA-02.A8**
GDA Issue Action	Westinghouse should provide fire progression event trees (or equivalent) for all compartments screened in accompanied by detailed documentation of fire impact in each compartment and details of all the fire scenarios identified. • Details of any fire modelling undertaken to support this task should also be included. • The identification of the most onerous Initiating Event for each fire scenario should be clearly documented. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A9**
GDA Issue Action	Westinghouse should provide documented evaluation of the reliability of the fire protection measures claimed (eg, PSA models for fire protection systems claimed and human reliability analyses as appropriate). With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A10**
GDA Issue Action	Westinghouse should provide documented evaluation of the inter-compartment fire propagation. Fire progression event trees for all relevant multi-compartment fires and details of any fire modelling undertaken to support this task should also be included as per Action 08. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A11**
GDA Issue Action	Westinghouse should provide documented re-evaluation of the Human Reliability Analysis for all the fire scenarios identified. The effects of the fire, both direct (e.g. the need to evacuate the control room) and indirect (e.g. confusing information resulting from spurious indications, impact of smoke), on operator actions have to be considered. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A12**
GDA Issue Action	Westinghouse should provide a documented Fire PSA model in CAFTA together with the results of the CDF quantification and evaluation of the results. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A13**
GDA Issue Action	Westinghouse should provide an estimation of the Large Release Frequency associated with internal fires. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A14**
GDA Issue Action	Westinghouse should provide the complete fire PSA documentation and ALARP assessment. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
FIRE PROBABILISTIC SAFETY ANALYSIS (PSA)
GI-AP1000-PSA-02 REVISION 0

Technical Area		**PROBABILISTIC SAFETY ASSESSMENT**	
Related Technical Areas		Internal Hazards	
GDA Issue Reference	**GI-AP1000-PSA-02**	**GDA Issue Action Reference**	**GI-AP1000-PSA-02.A15**
GDA Issue Action	Westinghouse should develop and provide a Living PSA procedure to allow the Fire PSA to be updated as further design information becomes available and when the Internal Events PSA evolves in a way that may impact the Fire PSA. With agreement from the Regulator this action may be completed by alternative means.		

Further explanatory / background information on the GDA Issues for this topic area can be found at:	
GI-AP1000-PSA-01 Revision 0	Ref. 101.
GI-AP1000-PSA-02 Revision 0	Ref. 102.