Health and Safety Executive

HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Reactor Build

Westinghouse AP 1000 Step 2 PSA Assessment

HM Nuclear Installations Inspectorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

1. Introduction

This report deals with the Generic Design Assessment (GDA) Step 2 assessment of the PSA approach detailed in the PSR provided by Westinghouse for the AP1000. The main conclusion is that Westinghouse has provided sufficient information to demonstrate that its PSA techniques are consistent with NII's Safety Assessment Principles (SAPs). This provides us with a sufficient degree of confidence to recommend that GDA Step 2 requirements have been met for the AP1000.

2. ND Assessment

2.1 Requesting Party's Case

Westinghouse's case is outlined in their UK Compliance document (Ref 1) and the major supporting document is the Design Control Document (DCD) (Ref 2) compiled to meet USNRC requirements. The DCD contains a large amount of information relevant to the UK, but there is not a one to one correspondence with ND requirements noted in the GDA guide (Ref 3) and our Technical Assessment Guide (TAG) on safety reports (Ref 4). The UK Compliance document is intended to bridge these gaps.

Westinghouse addresses PSA in sections A 3.4 and C of the UK Compliance document and claims to have carried out a comprehensive study and to systematically analyse the complete range of anticipated initiating faults, internal and external initiators, and includes all modes of operation. Section A 3.4 discusses the various elements of the PSA covering PSA methodology and gives an overview of the results. The methodology section covers initiating faults, accident sequence analysis, systems analysis, human reliability analysis, data analysis (initiating fault frequency, component reliability and common cause failure), quantification, containment performance (level 2) and consequence analysis (level 3).

Section C of the UK Compliance document contains specific sections against each of our SAPs and Numerical Targets. For the PSA ones (see ref 7) the relevant claims are shown in the table below:

SAP/NT	WESTINGHOUSE Claim:
FA.10 Need for PSA	The AP1000 design has addressed FA.10. NRC 10 CFR 52.47 requires that a design-specific PRA be performed to support Design Certification. The AP1000 PRA was done by considering risks due to all initiators and all modes of operations. The AP1000 PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. DCD Chapter 19 discusses the interaction between the design and the PRA
FA.11 Validity	The AP1000 design has addressed FA.11. The AP1000 PRA was used in the Design Certification process to identify important safety insights and assumptions to support certification requirements, such as the reliability assurance program (RAP). The AP1000 PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. DCD Chapter 19 discusses the interaction between the design and the PRA. Duty Holder items identified in DCD Chapter 19 are designed to ensure that site-specific factors are addressed in the PRA once a site is chosen
FA.12 Scope and extent	The AP1000 design has addressed FA.12. The AP1000 PRA considers the reactor core as the largest source of radioactivity in the AP1000. Thus, the PRA quantifies risk due to initiating events that may challenge the core integrity. The AP1000 initiating event analysis is described in PRA Chapter 2. Additional sources of radioactivity – that is, spent fuel – are discussed in DCD Chapter 19 and the PRA
FA.13 Adequate representation	The AP1000 design has addressed FA.13. NRC 10 CFR 52.47 requires that a design-specific PRA be performed to support Design

	Certification. The AP1000 PRA was performed by considering risks due to all initiators and all modes of operations. The PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. DCD Chapter 19 discusses the interaction between the design and the PRA. Duty Holder items identified in DCD Chapter 19 are designed to ensure that site-specific factors are addressed in the PRA once a site is chosen. The scope of the PRA accounts for contributions to the risk due to the following random individual component failures, components which are failed as a result of the initiating fault, common cause failures (and as necessary, other dependent and consequential failures), unavailabilities due to testing and maintenance & human errors. Discussion of the scope of the PRA is throughout the PRA report, but specifically in the system notebooks, PRAs Chapters 8 through 28. Generic data sources have been used because plant-specific operational experience does not exist. However, a consistent approach to the use of generic data is discussed in PRA Chapter 32. The methodology for the human reliability analysis is documented in PRA Chapter 30.
FA.14 Use of PSA	The AP1000 design has addressed FA.14. NRC 10 CFR 52.47 requires that a design-specific PRA be performed to support Design Certification. The AP1000 PRA was done by considering risks due to all initiators and all modes of operations. The AP1000 PRA iterated with the AP1000 plant design to ensure risk insights were considered during the design phase. AP1000 DCD Chapter 19 discusses the interaction between the design and the PRA. Duty Holder items identified in DCD Chapter 19 are designed to ensure that site-specific factors are addressed in the PRA once a site is chosen. The AP1000 Design Reliability Assurance Program (D-RAP) is implemented as an integral part of the AP1000 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP1000 PRA will remain valid throughout plant life.
Target 7	The AP1000 meets this limit and this objective. As discussed under Target 5, a detailed PRA has been done for the AP1000. This assessment is summarized in DCD Chapter 19, but is documented in detail in a separate PRA report. Per detailed calculations, the AP1000 core damage frequency is approximately 5.0 x 10-07 per annum. Thus, even if it is conservatively assumed that a core damage event will lead to fatalities (which obviously is not true, significant mitigation is provided in the plant design); this core damage frequency is lower than the objective of 1 x 10-06 pa. The risk of death to people on the site is not significantly different from that to people off the site for AP1000
Target 8	The AP1000 complies with these limits and meets these objectives. The AP1000 PRA was done for level 1, 2 and 3. For the theoretical site specified by the URD, the AP1000 Level 3 PRA calculates a 24-hour site boundary whole body dose of less than the URD limit of 0.25 Sv with a frequency less than 1 x 10-06 per annum. Since this is a theoretical limit, site-specific re-evaluation may be required, but the fact that this URD limit is much lower than UK objectives provides confidence that the UK objectives will be met. Using the theoretical site from the URD, the specific AP1000 PRA Level 3 performance breakdown is claimed to better the UK targets by 3 or 4 orders of magnitude in each of the dose bands.
Target 9	The AP1000 meets this limit and this objective. While accidents causing the risk of 100 or more fatalities have not been specifically identified in the AP1000 evaluations, a metric with comparable intent would be the large release frequency. The large release frequency is defined as the calculated frequency of a core damage event where in addition to the core damage, a containment event tree sequences where the containment is bypassed or failed occurs. The calculated large release frequency for the AP1000 is approximately 6 x 10-8 per annum. Since this compares favourably with the BSO coupled with Target 9, there is high confidence that the AP1000 meets this objective.

Westinghouse's Preliminary AP1000 Core Damage Frequency Estimates are:

Category	**CDF /year**
At-Power Internal Events	2.41×10^{-7}
At-Power Fire	5.61×10^{-8}
At-Power Flood	8.82×10^{-10}
Shutdown Internal Events	1.23×10^{-7}
Shutdown Fire	8.52×10^{-8}
Shutdown Flood	3.22×10^{-9}
TOTAL	5.09×10^{-7}

2.2 Standards and Criteria

In respect of PSA, Step 2 of the GDA guidance (Ref 3) requires the Requesting Party (RP), in section 2.6, to provide "An overview statement of the approach, scope, criteria and output of the probabilistic safety analysis". The GDA guide goes on to say that HSE will undertake "an assessment directed at reviewing the design concepts and claims" and specifically in point 2.22 "the PSA approach".

Hence the PSA itself is not being assessed in Step 2; rather we are looking at high level claims on how the PSA SAPs will be met by the RP's submission. The Fault Analysis strategy Project Assessment Report (PAR) (Ref 7) identified SAPs FA.10 to FA.14 and NT. 7 to 9 as the relevant sections. The equivalent section of the IAEA standards (Ref 8) and WENRA reference levels (Ref 9) have also been listed. The aim of the assessment at Step 2 is to see that appropriate claims have been made. The arguments and evidence supporting these claims will be assessed in Step 3 and beyond.

2.3 ND Assessment

The UK compliance document describes a full scope Level 3 PSA which is claimed to address ND requirements for completeness in terms of the lists of faults and hazards and the claimed coverage of all operating modes. In terms of the SAPs, FA10 and FA 11 appear to be sufficiently well developed at this stage requiring no additional information in Step 3. For FA.12 Westinghouse considers that the reactor core is the largest source of radioactivity and appear to imply other sources can be ignored. This is not accepted, for example, the spent fuel pool will contain a significant amount of irradiated fuel and may represent significant risks to workers and the public. We do accept that the core is the most significant source. Westinghouse has undertaken to cover non-core sources and worker risks in its submission for Step 3.

The claim against FA 13 appears to be reasonable. For FA14, use of the PSA during design is reported in many parts of the UK compliance document and the DCD, so seems satisfactory.

Westinghouse's analysis does not specifically address SAPs numerical targets 7, 8 and 9. It does however provide reasonable argument that its current analysis can be interpreted to show that the targets can be met.

Other points for ND follow up in Step 3 and beyond:

- Linked event and fault tree approach is acceptable in principle but detailed modelling not assessed at this Step.
- External events – we will want to review the evidence for screening out of external flood, snow loading etc.
- Intersystem CCF is considered – good point, but we will need to see the detail in later steps.
- All modes of operation are claimed but not clear to us yet how transition between modes is dealt with.
- Multiple Greek Letter method for CCF – acceptable in principle, uses generic data. Nothing wrong with generic data for new design but the data sources will need further assessment.
- Evidence of the use of importance values – good point, and again we will want to explore this in Step 3.
- Component failure data – as with CCF, the data sources seem old, and will need detailed assessment in Step 3 and beyond.

3. Conclusions

Westinghouse has provided an adequate overview of the approach, scope criteria and output of the PSA.

Westinghouse accepts that it needs to provide analysis of non-core sources of radioactivity and that it will need to re-analyse the PSA consequences for proper comparison with SAPs numerical targets. Reasonable arguments have been advanced, which give a strong indication that targets will be met or bettered.

A high level ND assessment of the claims for adequacy of the PSA and its output does not indicate any fundamental cause for concern.

A number of points for future consideration (by ND) have arisen during this high level assessment and it has not been possible, or indeed appropriate, to address them in Step 2. These will be picked up during our assessment in Step 3 and beyond.

4. Recommendations

HSE should accept that Westinghouse has provided sufficient information on the approach, scope criteria and output of the PSA for Step 2 of GDA.

5. References

1. AP1000 – UK Compliance document. UKP-GW-GL-720 Rev 0

2. AP1000 Design Control Document.

3. HSE Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties, Version 2, 16 July 2007

4. T/AST/051 Guidance on the purpose scope and content of Nuclear Safety Cases. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/index.htm

5. ASME Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications. ASME-RA-Sb-2005. 2005

6. not used.

7. Step 2 Fault Analysis & PSA Strategy. AR07015.

8. IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design – Requirements – No.NS-R-1.

9. Western European Nuclear Regulators Association (WENRA) Reactor Safety Reference Levels, January 2007.