New Reactors Programme

GDA close-out for the AP1000® reactor

GDA Issue GI-AP1000-PSA-01

Success Criteria for the Probabilistic Safety Analysis for the Westinghouse AP1000® Reactor (Internal Events At-Power)

Assessment Report: ONR-NR-AR-16-017
Revision 0
March 2016

Published 03/17

EXECUTIVE SUMMARY

Westinghouse Electric Company LLC (Westinghouse) is the reactor design company for the AP1000 reactor. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues require resolution prior to award of a Design Acceptance Confirmation (DAC) and before any nuclear safety related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse AP1000 reactor design in the area of Probabilistic Safety Analysis (PSA). Specifically this report addresses GDA Issue, GI-AP1000-PSA-01 - Success Criteria for the Probabilistic Safety Analysis (Ref. 1).

This GDA issue arose in Step 4 because AP600 reactor plant success criteria had been used instead of AP1000 reactor plant specific success criteria. Additional confidence was also needed in the coverage of initiating events and the traceability and documentation of the PSA.

The Westinghouse GDA Issue resolution plan states that its approach to closing the issue is:

- To perform success criteria analysis specifically for the AP1000 plant based on current operating procedures. This would ensure proper representation of the AP1000 plant fault sequence mitigation and operator response.
- To systematically review the AP1000 plant design to properly represent the initiating events.
- To fully document the PSA.

My assessment conclusion is:

- Westinghouse has submitted a new internal events at-power PSA to address GDA Issue GI-AP1000-PSA-01. I am largely satisfied that the internal events at-power PSA meets the guidance in the ASME PSA standard and the ONR technical assessment guide on PSA. However, I have identified a number of shortfalls which need to be resolved during licensing.
- Westinghouse claims that the core damage frequency and large release frequency from internal events at-power is below the ONR BSO for numerical targets 8 and 9 respectively.
- My judgement is that the ONR SAP numerical target 8 and 9 BSOs may be met, but confirmation of this needs completion of the work to resolve the shortfalls.
- An understanding of the overall risks from the AP1000 plant needs consideration of the internal events at-power risks, together with the impact of shortfalls, and the full range of additional plant and site hazards. This will be developed fully during the licensing phase. My judgement of the overall risk from the AP1000 reactor plant at GDA is that the ONR SAP target 8 and 9 BSOs are likely to be exceeded, but I consider the risk should be within the respective BSLs with a significant margin.
- My assessment of the internal events at-power PSA has not found any major areas of the plant design for which ALARP analysis is needed to consider alternative features. However, my assessment does support findings which have ALARP implications for the detailed design phase.
- I consider that suitable and sufficient work has been presented by Westinghouse to enable GDA issue GI-AP1000-PSA-01 to be closed.

My judgement is based upon the following factors:

- I consider the ASME PSA standard to be suitable for the development of the internal events at-power PSA.

- AP1000 plant specific success criteria has been used and the comprehensiveness of the initiating events is adequate for GDA.
- I undertook this assessment by sampling from each technical area of the PSA using the ONR SAPs and the ONR technical assessment guide on PSA as my benchmark. My assessment was assisted by technical support contractors with specialist PSA knowledge and I conducted many discussions with Westinghouse.
- I understand the risks from internal events at-power, the dominant contributors to risk and the risk impact of the shortfalls I have identified.
- I have identified assessment findings to be resolved during licensing to ensure the PSA continues to develop into a useful living PSA.
- My assessment supports the view that the risks from internal hazards at-power are being managed ALARP as the AP1000 reactor plant design process continues through GDA and into the licensing phase.

The following matters remain, which are for a future licensee to consider and take forward in its site-specific safety submissions. These matters do not undermine the generic safety submission and require licensee input/decision.

I have raised 12 assessment findings and 4 minor shortfalls. The assessment findings cover the following high level topics:

- The validation and completeness of operator error data used in the PSA.
- Undertaking additional MAAP analysis to confirm plant performance and operator timelines.
- Review of the methodology and data used to include additional consideration of dependency and common cause failure in the PSA.
- Ensuring that the treatment of containment bypass fault sequences is comprehensive.
- Providing a comprehensive analysis of the reliability of the safety systems during the detailed design phase.
- Reviewing the treatment of plant damage states where relevant fault sequence information may be lost for the Level 2 PSA.

In summary I am satisfied that GDA Issue GI-AP1000-PSA-01 (Success Criteria) can be closed.

LIST OF ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
ADS	Automatic Depressurisation System (Stages 1, 2, 3 and 4)
AF	Assessment Finding
ALARP	As Low As Reasonably Practicable
ASME/ANS	American Society of Mechanical Engineers/American Nuclear Society
ATWS	Anticipated Transient Without Scram
BL	Large Bypass
BS	Small Bypass
BSL	Basic Safety level
BSO	Basic Safety Objective
CAFTA	Computer Aided Fault Tree Analysis
CCS	Component Cooling Water System
CDF	Core Damage Frequency
CET	Containment Event Tree
CIM	Component Interface Module
CMT	Core Make-Up Tank
CP	Close-Out Programme
CVS	Chemical and Volume Control System
C&I	Control and Instrumentation
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DCP	Design Change Proposal
DVI	Direct Vessel Injection
EPR	European Pressurised (Water) Reactor
EPRI	Electric Power Research Institute
FMEA	Failure Modes and Effects Analysis
HOW2	ONR Business Management System
HVAC	Heating, Ventilation and Air Conditioning
IEC	International Electrotechnical Commission
IEF	Initiating Event Frequency
ISGTR	Induced Steam Generator Tube Rupture
ISV	Integrated System Validation
GDA	Generic Design Assessment
IAEA	The International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IE	Initiating Event
IRWST	In-Containment Water Storage Tank

LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPSD	Low Power and Shutdown
LRF	Large Release Frequency
LTC	Long Term Cooling
MAAP	Modular Accident Analysis Programme
MCR	Main Control Room
MCS	Minimal Cut Set
MDEP	Multi-national Design Evaluation Programme
MRI	Metal Reflective Insulation
MS	Minor Shortfall
MSIV	Main Steam Isolating Valve
MTTR	Mean Time To Repair
MW	Mega-Watt
NUREG	NUclear REGulatory Document (USNRC)
OECD-NEA	Organisation for Economic Co-operation and Development –Nuclear Energy Agency
ONR	Office for Nuclear Regulation
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PDS	Plant Damage State
PORV	Power Operated Relief Valve
POS	Plant Operating State
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PRA	Probabilistic Risk Assessment – US term for PSA
PRHR	Passive Residual Heat Removal
PSA	Probabilistic Safety Assessment
PSR	Preliminary Safety Report
PWR	Pressurised Water Reactor
PWROG	PWR Owners Group
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RGP	Relevant Good Practice
RNS	Normal Residual Heat Removal System
RP	Requesting Party
RPV	Reactor Pressure Vessel
RQ	Regulatory Question
SAPs	Safety Assessment Principles

SFAIRP	So Far As Is Reasonably Practicable
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SIL	Safety Integrity Level
SLB	Steam Line Break
SRV	Safety Relief Valve
SSC	System, Structure (and) Component
SSER	Safety, Security and Environmental Report
SWS	Service Water System
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
US NRC	United States (of America) Nuclear Regulatory Commission
WENRA	The Western European Nuclear Regulators' Association
Westinghouse	Westinghouse Electric Company LLC

TABLE OF CONTENTS

Table(s)

Annex(es)

1 INTRODUCTION

1.1 Background

1. Westinghouse Electric Company LLC (Westinghouse) completed GDA Step 4 in 2011 and paused the regulatory process. It achieved an IDAC which had 51 GDA issues attached to it. These issues require resolution prior to award of a DAC and before any nuclear safety related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

2. This report is the ONR's assessment of the Westinghouse AP1000 reactor design in the area of Probabilistic Safety Analysis (PSA). Specifically this report addresses GDA Issue GI-AP1000-PSA-01 Rev 0 – Success criteria for the PSA (Ref. 1).

3. The related GDA Step 4 report is published on our website (http://www.onr.org.uk/new-reactors/ap1000/reports.htm), and this provides the assessment underpinning the GDA issue. Further information on the GDA process in general is also available on our website (http://www.onr.org.uk/new-reactors/index.htm).

1.2 Scope

4. The scope of work required by Westinghouse to address GDA Issue GI-AP1000-PSA-01 Rev 0 is described in the resolution plan agreed between ONR and Westinghouse following Step 4 of GDA (Ref. 1). I reviewed the scope of work at the start of the close-out phase. The final version of the resolution plan is presented in (Ref. 2). The scope of work is summarised below.

5. The resolution plan scope of work is based on the expectations that the AP1000 plant PSA will be based upon success criteria analysis performed specifically for the AP1000 plant and based on AP1000 plant operating procedures to assure proper representation of AP1000 plant accident mitigation. This work needs to be properly documented along with the justification of the time windows for operation actions to provide traceability. PSA initiating events need to be identified and properly represented in a systematic fashion to represent all plant faults. The following high level and specific tasks have been identified in the resolution plan as necessary to 1) gain an appropriate level of confidence that the internal events at-power PSA is based on AP1000 plant specific performance analysis, 2) is an adequate representation of the generic AP1000 plant design, 3) confirms and/or adds to the insights into the plant risks highlighted at Step 4, and 4) supports ALARP assessment.

5.1 High level tasks:

- Task 1: Define event tree initiators
- Task 2; Develop event trees from initiating event responses
- Task 3: Determination of success criteria
- Task 4: Determination of Plant Damage States (PDS) and quantification of the risk model.
- Task 5: Documentation of PSA success criteria analysis and gap analysis.

5.2 Specific Tasks:

- Provide a methodology to guide the development of success criteria for the AP1000 plant PSA.

- Provide the AP1000 plant input deck(s) (and parameter file(s)) for the computer code(s) to be used.
- Provide a complete list of Initiating Events (IEs) correctly grouped, and details of the success sequences including a demonstration that the analysis (both thermal hydraulic and neutronics) is sufficient to support the success criteria
- Provide the success criteria analyses and results for Loss of Coolant Accidents (LOCA).
- Westinghouse should provide the success criteria analyses and results for intact circuit faults.
- Provide the success criteria analyses and results for Steam Line Breaks (SLB).
- Provide the success criteria analyses and results for Steam Generator Tube Ruptures (SGTR).
- Provide the success criteria analyses and results for Anticipated Transients Without Scram (ATWS).
- Develop a gap analysis to evaluate the implications of the new analysis on the AP1000 plant core damage frequency (CDF) and large release frequency (LRF).
- Complete the documentation and provide a standalone document compiling all the PSA success criteria analysis and gap analysis performed accompanied by the supporting references.

6. When compared with the PSA assessed by ONR at GDA Step 4 the internal events at-power PSA is essentially a new risk model with additional initiating events, extensive new supporting performance analysis and a selection of new logical models.

7. For low power and shutdown internal events I agreed additional limited scope success path analysis with Westinghouse. This was requested because the success criteria for the shutdown plant operating states at GDA Step 4 was based on AP600 plant analysis. The scope of work was agreed between ONR and Westinghouse outside the resolution plan to determine whether AP1000 plant specific MAAP analysis would significantly alter the success criteria for the shutdown plant operating states (Ref. 4). The scope of work addressed a review of shutdown plant state initiating event frequencies and new AP1000 plant MAAP analysis for four shutdown initiating events:

   - A LOCA through valve RNS-PL-V024 during non-drained condition sequences.
   - Loss of Normal Residual Heat Removal (RNS) operation during drained condition sequences.
   - Loss of Component Cooling Water System (CCS)/Service Water System (SWS) during drained condition sequences.
   - Loss of Offsite Power (LOOP) during drained condition sequences.

8. Two reports were produced by Westinghouse for ONR: 1) a review of low power and shutdown (LPSD) initiating events (Ref. 30) and 2) an accident sequence/success criteria report (Ref. 29).

1.3 Method

9. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 5).

1.3.1 Sampling strategy

10. It is rarely possible or necessary to assess a safety submission in its entirety, and therefore ONR adopts an assessment strategy of sampling. I considered that a proportionate sampling strategy for this assessment would be achieved providing it included review for each of the main technical areas needed to produce an internal events at-power PSA. A good understanding of each main technical area of the PSA would then enable an overall view to be assembled and an overall judgement on adequacy to be made. The technical areas I sampled were chosen from the PSA standards against which the PSA was constructed, ASME/ANS RA-Sa-2009 (Ref. 6) and Regulatory Guide 1.200 Revision 2 (Ref. 10).

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

11. ONR's GDA Guidance to Requesting Parties (http://www.onr.org.uk/new-reactors/ngn03.pdf) states that the information required for GDA may be in the form of a PCSR, and Technical Assessment Guide (TAG) 051 (Ref 8) sets out regulatory expectations for a PCSR (http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf).

12. At the end of Step 4, ONR and the Environment Agency raised GDA Issue CC-02 (Ref. 9) (http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the AP1000 design reference point.

13. A separate regulatory assessment report is provided to consider the adequacy of the PCSR and closure of GDA Issue CC-02, and therefore this report does not discuss the PSA aspects of the PCSR. This assessment focused on the supporting documents and evidence specific to GDA issue PSA-01 (Ref. 1).

2.2 Standards and Criteria

14. The standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs) 2014 edition, Rev 0 (Ref. 3), internal Technical Assessment Guides (TAGs) for PSA (NS-TAST-GD-030 Revision 5: Ref. 7). Other standards that represent relevant good practice for nuclear reactor PSA are those from the IAEA, WENRA and ASME/ANS RA-Sa-2009 (Ref. 6) and US Regulatory Guide 1.200 Revision 2 (Ref. 10).

2.2.1 Safety Assessment Principles

2.2.2 The key PSA related safety assessment principle SAPs applied within the assessment are FA.10 to FA.14 (Ref. 3).

2.3 Use of Technical Support Contractors (TSCs)

15. It is usual in GDA for ONR to use technical support, for example to provide additional capacity to optimise the assessment process, enable access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision making.

16. I used TSCs to support my assessment of GDA issue PSA-01. This support was required to share the detailed technical review workload, provide high quality expertise for the broad range of specialised and diverse technical subjects needed for an internal events at-power PSA, assist in the production of questions to Westinghouse and review of the responses, and to provide support at technical meetings with Westinghouse. The UK based technical support consultants Jacobsen-Analytics was chosen based on a competitive tendering process. Jacobsen-Analytics was supported by the US based consultants Scientech (Curtiss-Wright) for very specialised tasks concerning the use of the MAAP computer code to model the plant response to fault sequences.

2.4 Integration with Other Assessment Topics

17. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore be carried out in isolation as there are often safety issues of a multi-topic or cross-cutting nature. The following cross-cutting issues have been considered within this assessment:

- The performance of the plant operators as modelled in the PSA. This involved coordination with ONR's human factors inspector to understand the implications of the main control room simulator trials, and the quality of the human factors assessment of operator responses.

- The performance and modelling of the plant C&I control and protection systems. This involved coordination with the ONR control and instrumentation inspectors. This investigated the sensitivity to risk of the claims made for the reliability of the Protection and Safety Monitoring System (PMS), Diverse Actuation System (DAS) and Plant Control System (PLS), and the risk sensitivity of the claims made following spurious actuation of the squib valves by the PMS.

- The mechanical and structural integrity of the squib valves and pipework following a spurious actuation. This involved coordination with the mechanical engineering and structural engineering inspectors. This work investigated the potential for consequential damage to plant components nearby the squib valves.

- The potential for pipe whip following a Passive Residual Heat Removal (PRHR) line fracture to compromise the integrity of the In-Containment Refuelling Water Storage Tank (IRWST) to retain its water. This water is needed to protect the initiating event. This work was coordinated with the ONR structural integrity inspector.

- The risk sensitivity of using non-nuclear codes for the UK class 2 and class 3 Structures, Systems and Components (SSC). This work was coordinated with the ONR structural integrity inspector.

2.5 Out of scope items

18. The Step 4 GDA Assessment report (Ref 11) programmed the resolution of the assessment findings from Step 4 GDA (listed in Annex 1 of the assessment report) to the forward programme for the reactor as part of normal regulatory business. The resolution of these assessment findings was not included in the resolution plan for this GDA Issue and are therefore are out of scope of this assessment.

3 REQUESTING PARTY'S SAFETY CASE

3.1 GDA Issue AP1000-PSA-01 (Success Criteria for the PSA)

19. Westinghouse has undertaken new deterministic accident analysis based on the Modular Accident Analysis Programme (MAAP) computer code to derive AP1000 plant specific success criteria. Westinghouse has also taken the opportunity to substantially revise its internal events at-power risk model which incorporates these new success criteria. The submission is essentially a new PSA for internal events at-power (Refs 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22).

20. The scope of the internal events at-power PSA includes a comprehensive consideration of the initiating events that can arise due to failures of the primary and secondary systems or operators. The scope is limited to initiating events which occur when operating at full power. The PSA includes both a Level 1 and Level 2 analysis.

21. The Level 1 PSA analysis examines the performance of the engineered safety systems provided, and any operator actions needed, to prevent loss of critical safety functions; in particular the control of reactivity and the provision of decay heat removal following a plant fault. Failure of these safety functions may lead to core damage. The Level 2 PSA assesses the performance of the containment and its associated systems to contain any radioactive material arising from core damage. Failure of the containment can give rise to a release of fission products to the environment. The output from the PSA is the core damage frequency, the large release frequency, and various importance measures. Extensive analysis of the results has been performed using importance analysis and also sensitivity studies, so that the effectiveness of the safety systems and operator responses can be understood, and the dominant contributors to risk presented.

22. The PSA is modelled and quantified using the Electric Power Research Institute (EPRI) R&R workstation software suite for both the Level 1 and Level 2 PSA with the identified versions or higher:

- CAFTA 6.0 – logic model development program
- PRAQuant 5.1a – sequence level quantification control program
- FTREX 1.6 – cutset generation program
- QRecover 3.1 – cutset recovery and modification program
- UNCERT 3.0 – computes probability density distributions.

23. This suite of software has been developed by EPRI and is a widely used method for the construction and evaluation of PSAs. The PSA has been developed by Westinghouse to meet the requirements of ASME/ANS-RA-Sa-2009 (Ref. 6) and Regulatory Guide 1.200 Revision 2 (Ref. 10).

24. The design basis claim for the AP1000 plant is for passive safety systems to put the plant into a safe state without the need for operator action. The internal events at-power PSA explores the defence-in-depth provided should the design basis claims fail to be met. It also includes a comprehensive range of beyond design basis initiating events to present a comprehensive fault sequence analysis for internal events at-power.

25. The PSA claims five modes of decay heat removal for the reactor plant, both passive and active depending upon the initiating event and the availability, or not, of off-site and on-site power supplies. The PSA models decay heat removal using the active

safety systems if possible, with the passive safety systems in reserve. This represents the operating philosophy of the plant which is to prevent significant steaming to and flooding of the containment unless necessary. The number of decay heat removal methods available including the passive safety systems supports the very small core damage frequency and very small large release frequencies presented in the PSA in documents APP-PRA-GSC-322 Rev B (Ref 18) and APP-PRA-GSC-376, Rev B (Ref. 20) respectively.

26. The PSA is discussed further by Westinghouse in the PCSR Chapter 10 (Ref. 32) in which the main use of the PSA results is stated to be the demonstration of compliance with ONR numerical targets and the demonstration that the overall risks from planned operation of the reactor are as low as reasonably practicable (ALARP). The discussion in the PCSR applies to the broader scope PSA and not just to the internal events at-power PSA. However, the internal events at-power PSA makes a contribution to the overall position stated by Westinghouse in the PCSR.

27. Westinghouse states that the core damage frequency and large release frequency is generally comparable with industry data for plants of similar design. However, the AP1000 plant is the only generation III+ reactor with passive features so a direct comparison is not possible. Westinghouse notes that the core damage frequency for the AP1000 plant is approximately two orders of magnitude lower than a typical PWR plant and this is due to the unique passive safety systems and the defence in depth capabilities of the design.

28. In the PCSR (Chapter 10) (Ref. 32) Westinghouse compares the results of the PSA with ONR SAP numerical target 8. This is the target for the total predicted frequencies of accidents on an individual facility per annum which would give doses to a person off the site. Westinghouse compares this target to the core damage frequency and large release frequency. This comparison is given in the table below.[*]

Table 1: AP1000 Plant Risks for Internal Events At-Power

ONR Numerical Target 8 Dose > 1000 mSv	PSA Claims	
	Core Damage Frequency	Large Release Frequency
BSL 10^{-4}/year	1.7×10^{-7}/year	1.2×10^{-8}/year
BSL 10^{-6}/year		

29. The PCSR (Appendix 10A) describes how the basic design of the AP1000 plant, and its predecessor the AP600 plant, were reviewed by Westinghouse using insights from successive versions of the PSA to identify reasonably practicable design changes that would significantly reduce the risk from the plant. As a result of these reviews, Westinghouse states that a number of design improvements have been implemented to produce risks that are ALARP.

30. Westinghouse also states in the PCSR that as the AP1000 plant design develops the PSA will continue to demonstrate that the ONR SAP numerical target BSOs are met. Therefore Westinghouse considers there is little need to further reduce the AP1000 plant at-power PSA risk.

[*] *Westinghouse has not undertaken a PSA radiological dose assessment using its updated PSA model to enable a direct comparison with ONR SAP numerical target 8 to be undertaken. The frequency with which a dose would be received may be lower than the core damage frequency or large release frequency.*

3.2 Success Criteria for the Shutdown PSA

31. Westinghouse has presented a limited review of the shutdown PSA to incorporate new AP1000 plant specific success criteria within the fault sequence analysis (Ref. 30 and Ref. 29). This work presents a review of the frequencies for the following initiating events:

- loss of the normal residual heat removal system;
- loss of the component cooling water system, and
- loss of the service water system.

32. Westinghouse has also submitted new MAAP analysis to support the success criteria for the following four initiating events:

- LOCA through valve RNS-PL-V024 during non-drained conditions;
- Loss of the normal residual heat removal system operation during drained conditions;
- Loss of the component cooling water system/service water system during drained conditions, and
- Loss of off-site power during drained conditions.

33. Westinghouse states that this new MAAP analysis for the shutdown initiating events shows one particular difference when compared to the previous analysis. It shows that passive containment cooling is required for the long term success of all fault sequences that do not end with the restoration of RNS. Westinghouse does not consider that this difference is significant as the change is consistent with the at-power analysis to ensure long term stability and cooling.

34. Westinghouse also notes that in the MAAP runs for the loss of RNS cases that the core would briefly begin to uncover until either IRWST injection or RNS gravity injection would begin. This uncovery was due to the timing associated with opening the ADS Stage 4 valves to depressurise the plant and the actuation of gravity fed IRWST injection. Westinghouse considers that the timings should be further investigated to determine if earlier actuation of the ADS Stage 4 valves should be permitted to enable earlier IRWST gravity injection to prevent partial core uncovery. In addition Westinghouse states that investigation into the potential to reduce the timing for restoration of RNS gravity injection given the inability of passive core cooling IRWST injection should also be performed.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-PSA-01

35. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 31).

4.1 Scope of Assessment Undertaken

36. To determine the scope of assessment required I undertook a preliminary high level review of the PSA documentation and Westinghouse’s conclusions. I then put together the following high level technical assessment strategy and scope:

- Gain confidence in the overall construction, completeness and logical modelling used in the PSA, and whether these conform to modern standards.
- Review of the success criteria and supporting MAAP analysis. Review of the changes to the risk models will be undertaken for a sample of initiating events to cover LOCAs, general transients, steam line break, steam generator tube rupture and anticipated transient without scram). This will include review of accident timelines, time windows, relevant procedures and cues for operator action. Coordination with ONR’s fault studies and human factors technical areas is needed here.
- Gain confidence in the dominant contributors to risk.
- Gain confidence in the derivation of a selection of important initiating events. In particular those which put the fault outside the design basis. An overview assessment of the initiating events will be undertaken to consider their comprehensiveness.
- Review the sensitivity and uncertainty analysis presented, the insights and conclusions presented by Westinghouse, the impact of Design Change Proposals (DCPs) on the PSA and the use of the PSA to support ALARP assessment.

4.2 Assessment Strategy

37. The following topic areas where identified for assessment to address the overall construction, completeness and logical modelling used in the PSA:

- The methodology used to determine the success criteria and the overall construction of the PSA.
- The comprehensiveness of the initiating events, development of fault sequences, and the development of functional fault trees and their integration into the PSA.
- The manner in which dependencies have been addressed between the initiating events and the risk model, and between safety systems/support systems within fault sequences.
- The method used to model dependent failure between components and its application to selected system fault trees.
- The adequacy of the human reliability data and other reliability data used in the PSA.
- The interface between the Level 1 and Level 2 PSA and the implications of the new Level 1 accident sequences on the Level 2 PSA.

- The manner in which the electronic risk model has been constructed and quantified.

- Review the adequacy of the success criteria analysis and the supporting MAAP analysis (and MAAP parameter file), and the resulting accident timelines, time windows, relevant procedures and cues for operator action in coordination with ONR's human factors inspector.

- The accident sequence analysis for a sample of initiating events to cover LOCAs, transients, steam line break, steam generator tube rupture and anticipated transient without scram.

- Review of the dominant contributors to risk and any areas where a single point failure in a safety system could result in core damage.

- The modelling of common cause failure of the PMS and selective mechanical equipment.

- Modelling of operator errors which are contained in the dominant minimal cut sets (MCS).

- The comprehensiveness of the initiating events and the bounding approach used, taking into consideration the list of initiating faults ONR identified as not included at GDA Step 4.

- LOCA Initiating Event Frequencies (IEF), by assessing the approach used by Westinghouse in NUREG-1829, which uses generic US PWR operating experience, for its application to the AP1000 design.

- Review of the sensitivity and uncertainty analysis, the insights and conclusions presented by Westinghouse, the impact of DCPs on the PSA and the use of the PSA to support ALARP assessment.

4.3 Review of the Completeness and Grouping of Initiating Events

38. The resolution plan (Ref. 2) requested that Westinghouse includes in the success criteria evaluations an updated listing and grouping of AP1000 plant specific initiating events. Westinghouse was also requested to show that the initiating event grouping is correct for the purpose of success criteria evaluation. Westinghouse submitted an updated assessment to ONR to resolve these items in the initiating event and interfacing systems LOCA notebooks (Ref. 13 and Ref. 39).

39. My assessment was carried out in some detail for this aspect of the PSA. This is because completeness of the initiating events is an important aspect of PSA (SAP FA.12), and ONR considered there to be missing initiating events as recorded in the GDA Step 4 PSA report (Ref.11). I presented my assessment in RQ-AP1000-1384, RQ-AP1000-1441 and RQ-AP1000-1442 (Refs 44, 43 and 48 respectively). Westinghouse provided responses to these RQs in a series of documents reflecting multiple discussions with Westinghouse (Ref. 45, 46, 47, 49 and 50).

40. Westinghouse has updated its list of initiating events to include isolable interfacing systems LOCAs, PRHR cooling, CMT injection, IRWST injection and containment recirculation systems. Westinghouse has used both generic PWR operating experience and AP1000 plant specific analysis to identify the initiating events and explain how the initiating faults have been grouped together to make initiating events (Refs 13 and 39).

41. I consider that Westinghouse has included an adequately comprehensive range of generic PWR initiating events and also now includes those which are unique to the AP1000 passive safety system design. This meets the expectations of the resolution plan and is adequate for GDA. My assessment identified a number of areas where the detailed analysis of initiating events gave rise to residual matters which are discussed below.

4.3.1 Loss of HVAC Cooling

42. Loss of Heating Ventilation and Air Conditioning (HVAC) can result in excessive temperatures of equipment resulting in their failure or shutdown. There are thirteen HVAC systems on the AP1000 plant and Westinghouse has analysed the impact of loss of these on the reactor (Ref. 13). Westinghouse has identified that loss of the turbine building HVAC will result in loss of the component cooling water system. Loss of this system requires a reactor trip because it removes heat from reactor coolant system equipment. Westinghouse has included loss of the turbine building HVAC as an initiating event in the PSA. Westinghouse has also identified loss of the annex/auxiliary building non-radioactive ventilation system as an initiating event. This is because it provides cooling for the reactor trip switchgear room and various electrical switchgear rooms and the battery charger room. Loss of this equipment due to overheating would require a reactor trip and represents an additional initiating event.

43. However, Westinghouse has not presented sufficient justification that excluding loss of HVAC to other plant areas will not result in an initiating event. For example, the nuclear island non-radioactive ventilation system provides cooling for PMS equipment, main AC power equipment and the class 1 electrical rooms. Overheating of this equipment may require a reactor trip and represents an additional initiating event.

44. Westinghouse in its response to RQ-AP1000-1441 (Ref. 50) states that an expert panel analysis has been used to address this but room heat up calculations were not available following loss of HVAC. The two loss of HVAC initiating events currently included in the PSA contribute about 4% to the total core damage frequency. I consider that the potential absence of additional loss of HVAC initiating events is unlikely to be risk significant. However, for completeness of the PSA I consider that a loss of HVAC analysis for each area of the plant containing PSA equipment is needed. This is to justify that loss of the HVAC systems do not result in additional initiating events.

45. The response provided by Westinghouse to RQ-AP1000-1441 (Ref. 50) acknowledged that loss of HVAC to the Main Control Room (MCR) is not currently addressed in the AP1000 plant PSA. I consider this to be an omission that can be resolved during the site licensing phase. This is because the operating conditions in the main control room will take time to reach the point where evacuated is needed, the design of the display screens to minimise their heat loading is under review, there may be adequate time available to repair the HVAC, the reactor can be tripped and the main control room evacuated to the remote shutdown room from which a controlled shutdown of the reactor can be carried out. The ONR GDA Step 4 PSA report raised an assessment finding to address the completeness and grouping of initiating events (AF-AP1000-PSA-012[†]). I consider that the need for additional HVAC analysis can be resolved together with this Step 4 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).*

Technical item 12-1 for resolution with Step 4 AF-AP1000-PSA-012: The licensee shall carry out a loss of HVAC analysis, with heat-up calculations used, to establish whether there are any additional initiating events, and to inform MCR habitability considerations.

4.3.2 Consequential Initiating Events

46. My assessment of the initiating event notebook noted that the methodology for accounting for consequential initiating events is not adequately described (Ref. 13). A very brief discussion is presented that states Safety Relief Valve (SRV) opening and failure to close is addressed within the initiating events, but no further information is given.

47. The response from Westinghouse helped to clarify the treatment of consequential initiating events (Ref. 40). I have interrogated the risk model and it is apparent that it includes the SRV failure to close fault sequences as input to the initiating event for medium LOCA. Although not described in the initiating event notebook it is appropriately modelled.

48. I consider that improved documentation to describe the methodology and treatment in the PSA should be included in a future update of the initiating event notebook. This should include for example, a list of event trees and the associated transfers to assist the understanding of the initiating event modelling.

Minor Shortfall (CP-MS-AP1000-PSA01-01): The documentation should be improved to describe the methodology used to analyse consequential events in the PSA. A list of event trees and associated transfers to assist understanding the initiating event analysis is requested.

4.3.3 Consequential Loss of Offsite Power (LOOP)

49. Following an initiating event the plant will experience demands on its electrical power systems, and potentially faults as well. This may feed back into the grid connection resulting in a loss of offsite power. Westinghouse has used a probability of 9.8×10^{-5} for a consequential loss of offsite power during the 24 hours after an initiating event. I consider this small considering that NUREG CR-6890 (Ref. 51) provides a probability of 5×10^{-3} for a consequential loss of offsite power for US plant.

50. I consider that the modelling of consequential loss of offsite power may be optimistic especially considering the characteristics of the UK high voltage grid which is smaller than the US high voltage grid. In addition, no consideration has been given within the PSA to the potential for a higher consequential LOOP probability following a LOCA event when higher than normal demands are made on the internal plant electrical systems. Also no recovery of short term loss of offsite power loop events has been considered in the PSA. I note that the probability of a consequential loss of offsite power can be influenced by the site specific switchyard design which is yet to be determined.

51. In the Step 4 GDA PSA report AF-AP1000-PSA-019[‡] has captured the requirement to include the adequate treatment of consequential events. My assessment highlights the need for the site specific PSA to use UK specific design information and data. In this case for the switchyard and the characteristics of the UK grid. I am raising this modelling improvement for resolution together with the Step 4 GDA assessment finding.

[‡] *AF-AP1000-PSA-019 The Licensee shall provide revised and documented PSA event sequence models including adequate treatment of consequential events.*

Technical item 19-1 for resolution with Step 4 AF-AP1000-PSA-019: The licensee shall update the probability of consequential loss of offsite power to take into account the characteristics of the UK high voltage grid and the site specific switchyard design. The potential for a higher probability of loss of offsite power following a LOCA events shall be included. Recovery for short term loss of offsite power events shall be credited in order to remove conservatism from the model.

4.3.4 Support System Initiating Events

52. The methodology for treating dependencies between the mitigating systems and the various support system initiating events is described in the initiating event notebook (Ref. 13). I consider this to be very high level and discussed it with Westinghouse (Ref. 40).

53. My assessment of this topic sampled seven initiating events and is presented in RQ-AP1000-1540 (Ref. 74) and RQ-AP1000-1655 (Ref. 75). I found that the modelling of dependencies between the initiating events and the support systems is largely adequate although a number of items were raised for discussion with Westinghouse. These particular cases are discussed further in Sections 4.3.6 and 4.6.1 and have been clarified as not risk significant with Westinghouse (Refs 47 and 75). Having identified a small number of dependencies to be considered further from assessing seven initiating events, I consider that a further review of this topic should be undertaken for the other initiating events. This is to provide additional confidence in the completeness of the manner in which dependency modelling has been addressed.

54. Westinghouse has undertaken a systematic review of the AP1000 plant systems to identify support system contributions to initiating events. This has been presented as a Failure Modes and Effects Analysis (FMEA) (Ref. 13: Table A-1). I consider this is more consistent with a screening analysis in which the AP1000 plant systems are reviewed to identify whether potential failure modes are possible, and which initiating event would be affected. The analysis is not detailed enough to constitute a FMEA. I do not consider it meets the ASME requirements for analysis and documentation (ASME requirements IE-A1, IE-D1 and IE-D2).

55. The provision of FMEA for the AP1000 plant systems is an existing assessment finding from GDA Step 4 (Ref. 11: AF-AP1000-PSA-025[§]). I consider that when this work is undertaken it should include analysis to confirm the completeness with which initiating event and support systems dependencies has been done. The GDA Step 4 PSA report assessment findings AF-AP1000-PSA-011 and AF-AP1000-PSA-017 have also captured the requirement to use a robust process for the identification of initiating events and dependencies. I am raising this technical item for resolution together with the relevant Step 4 assessment findings.

Technical item 17-1 for resolution with Step 4 AF-AP1000-PSA-017: The licensee shall undertake a FMEA to review the potential for dependencies between initiating events and support systems. The FMEA requested under GDA Step 4 AF-AP1000-PSA-025 can be used for this.

4.3.5 Loss of Ultimate Heat Sink Initiating Event

56. The loss of ultimate heat sink initiator for the active secondary side systems has not been included in the PSA. Loss of sea water would be expected to lead to a loss of condenser vacuum/loss of condenser cooling initiating event. It may also cause a loss

[§] *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.*

of the Service Water System (SWS) and consequently contribute to the loss of Component Cooling System (CCS) initiating event. Westinghouse has justified not including the loss of ultimate heat sink as an initiating event because the service water system uses dedicated cooling towers and the raw water system is used as a source of long term makeup to the service water system. Westinghouse states that loss of the raw water system is included in the general transient initiating event based on the assumption that the service water system cooling tower basin has 12 hours capacity before make-up is required.

57. Loss of service water, component cooling water and loss of condenser cooling are included in the PSA and they are very small contributors to risk. I consider including the loss of ultimate heatsink should be done for completeness of the PSA. This can be done during licensing because the impact on risk of its absence is judged to be small. Westinghouse has agreed that loss of ultimate heat sink will be included within the site licencing PSA. I consider that this technical item can be addressed together with the GDA Step 4 assessment finding AF-AP1000-PSA-012[**].

> **Technical item 12-2 for resolution with Step 4 AF-AP1000-PSA-012:** The licensee shall include loss of the raw water system that supports makeup to the circulating water system and service water system as an initiating event.

4.3.6 Grouping of Initiating Events and Dependencies

58. The description of how the initiating faults have grouped together to form initiating events for the PSA is not presented in adequate detail. I consider that an improved description of how the grouping is done would benefit the presentation of the PSA. For example, how the initial plant faults presented in NUREG CR-5750 (Ref. 52) are bounded into an initiating event. Particular items to note are 1) the grouping of a loss of feed to one loop into the general transient category and 2) the allocation of spurious Chemical and Volume Control System (CVS) actuation into the general transient with main feedwater, reactivity control imbalance, or Reactor Coolant System (RCS) high pressure events. The initiating event notebook should provide an explanation of how the initiating events are bounding for these faults. I am recording this as a technical item which is to be resolved together with GDA Step 4 assessment finding AF-AP1000-PSA-011[††] which covers this topic more broadly.

> **Technical item 11-1 for resolution with AF-AP1000-PSA-011:** The licensee shall document more clearly the methodology describing the initiating event grouping process. For example, a table should be provided indicating availability of main and support systems, for example off-site power, SGs, feedwater, condensate, heat sink, etc. for each initiating event – to assist in the explanation.

59. I raised a number of questions with Westinghouse where the grouping of initiating events may not properly represent dependencies within the risk model (RQ-AP1000-1384 Actions A9, A10, A11 and A12: Ref. 44). The following two initiating faults are discussed below:

    1) A spurious low steam line pressure signal.

    2) A spurious low T-cold signal.

[**] *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).*
[††] *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.*

For item 1) this would generate a reactor trip and a safeguards signal. The appropriate steam generator would have its main feed isolated, the Power Operated Relief Valve (PORV) isolated and the Main Steam Isolation Valve (MSIV) closed.

60. Westinghouse states that the success criteria for startup feedwater providing a heat sink is that one PORV is available or one main steam safety valve operating to remove steam from the steam generator. Westinghouse notes in its response that the modelling used is slightly non-conservative if the steam generator chosen for decay heat removal is the one which had the PORV closed due to the spurious low steam line pressure signal (Ref. 47).

61. For item 2) a spurious low T-cold signal would isolate steam generator feed, PORV, MSIV and isolate startup feedwater to both SGs. This fault would result in a power imbalance with pressure rising in the secondary side with the steam generator relief valves opening. It is not clear that the bounding of this event with the opening of steam generator relief valves is appropriate with the general transient (with safeguards signal) initiating event. This is because it is such a broad category of initiating event that mainly covers fault sequences without steam generator relief valve lifts. I questioned whether the dependency of the initiating event on steam generator relief valve lift would be overlooked. Westinghouse responded with a sensitivity study including the dependency that showed the increase in core damage frequency was very small at much less than 1%.

I consider the risk significance of these two items to be small. However, it demonstrates the need to provide additional assurance of the treatment of dependencies between initiating events and the plant systems responding to the fault. I consider that this technical item should be addressed as part of the Step 4 GDA finding AF-AP1000-PSA-017[‡‡] which covers the treatment of dependencies.

> **Technical item 17-2 for resolution with AF-AP1000-PSA-017:** The licensee shall include in the risk model the dependencies identified for a spurious low steam line pressure signal and a spurious low T-cold signal.

4.3.7 Operator Induced Initiating Events

62. The initiating events notebook states that the methodology includes plant failures and operator induced events including those from testing and maintenance activities (Ref. 13). However, no evidence is provided in the notebook on how operator induced events have been identified for inclusion within the PSA. From my assessment of the risk model it is apparent that human failure events are included for the more frequent initiating events and for the operators responses to initiating events. However, the inclusion of human failure events due to testing, calibration and maintenance activities are not currently adequately represented in the PSA. This was also raised in the Step 4 GDA report with assessment finding AF-AP1000-PSA-034 (Ref. 11).

I raised this with Westinghouse in RQ-AP1000-1441 and in its response Westinghouse stated that human induced initiating events are not explicitly developed for the at-power internal events model (Ref. 50). This is because the generic PWR operating experience data used for the general transient initiating event will implicitly include event data for manual reactor trip events.

Within NUREG/CR-5750 (Ref. 52) this category of events is described as “A manual initiation of a reactor trip, either purposely or by human error.” Westinghouse also states that the likelihood of inadvertent initiation of protection systems such as ADS

[‡‡] *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.*

Stage 4 is not considered to be credible because two operators are required to operate two switches located in separate areas in the main control room.

63. I agree that the approach taken by Westinghouse which uses operational experience is adequate to include the more frequent operator errors, and I agree that serious spurious initiations due to operator action can be small due to operational safeguards and training. However, I consider that the identification and inclusion of "pre-initiating event" human failure events within the PSA needs improving in accordance with ONR's PSA TAG (Ref. 7 Table A1-2.5). These include, for example, surveillance tests, calibrations, maintenance activities or operational realignments. I am recording this as a technical item to be addressed along with GDA Step 4 assessment finding AF-AP1000-PSA-034[§§].

> **Technical item 34-1 to be resolved with Step 4 AF-AP1000-PSA-034:** The licensee shall carry out a systematic review of pre-initiating event operator errors and include them in the PSA.

4.3.8 Manual Shutdown due to Technical Specification Requirements

64. Manual shutdowns are mandated within the technical specifications if equipment unavailability or plant faults require it. Westinghouse include manual shutdowns in the PSA if the technical specifications require a shutdown within 8 hours of the change in plant status. However, it is not clear from the documentation which initiating events have been included based on the technical specification requirements, or whether the risk model includes the corresponding equipment unavailability for the relevant manual shutdown initiating events. This was raised with Westinghouse for which a response was provided (Ref. 53: RQ-AP1000-1441 comment 11).

65. The response provided a brief description taken from the initiating event notebook, but did not provide adequate information to explain how the approach was applied and how equipment unavailability is taken into account for the initiating events identified and included in the PSA. I consider that Westinghouse should provide a more robust justification. This should include consideration of technical specification requirements for PSA related systems for allowable outage times of up to 24 hours. This is to provide a demonstration that PSA significant initiating event are not being excluded for allowable outage times of between 8 and 24 hours. Further consideration should be given to whether this identifies additional initiating events for inclusion in the PSA, with account taken of the corresponding equipment unavailability in the accident sequence models. This is therefore raised as a technical item for resolution with Step 4 Assessment Finding AF-AP1000-PSA-012[***] which addresses the completeness of initiating events.

> **Technical item 12-3 for resolution with Step 4 AF-AP1000-PSA-012:** The licensee shall provide a more robust justification for the approach taken to identify manual shutdown initiating events due to technical specification requirements. This should include consideration of technical specification requirements for PSA related systems for allowable outage times of up to 24 hours. If necessary, additional initiating events should be included in the PSA.

[§§] *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 FFEs 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.*

[***] *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).*

4.3.9 Intact Circuit Fault Initiating Event Frequency Data

66. The risks presented in a PSA are directly proportional to the frequency of the initiating events. Therefore realistic estimates are needed to provide a best estimate PSA. Westinghouse has used the initiating event frequency data primarily from NUREG-6928 (Ref. 54) and is supplemented by NUREG/CR-5750 (Ref. 52) which is representative of US nuclear power plants. These NUREG/CR-5750 data are now more than 20 years old. The USNRC website has an update to NUREG/CR-5750 data for the period 1988-2013 (Ref. 55).

67. I requested Westinghouse to provide information on how more recent operating experience is considered in the identification and quantification of initiating events in RQ-AP1000-1441. Westinghouse's response to RQ-AP1000-1441 (Ref. 50: comment 15) justified the use of the 2007 NUREG/CR-5750 data by demonstrating that the initiating event frequencies used are more conservative compared to more recent data sources.

68. I consider this is adequate for my understanding of the risks for GDA. However, the development of the PSA during licensing should update the initiating event frequencies with the most recent data to preserve the best estimate philosophy of PSA. The Step 4 GDA PSA report raised the revision of initiating event frequencies with AF-AP1000-PSA-036[†††]. I have therefore raised a technical item for resolution together with the Step 4 assessment finding.

> **Technical item 36-1 for resolution with Step 4 AF-AP1000-PSA-036:** The licensee shall update the initiating event frequencies in the PSA with the most recent operating experience.

4.3.10 Loss of Coolant Accident Initiating Event Frequency Data

69. The LOCA Initiating Event Frequency (IEF) estimates presented for the internal events at-power PSA within (Ref. 13) are based on the NUREG-1829 methodology (Ref. 23). This uses an expert elicitation process which consolidates operating experience and insights from probabilistic fracture mechanics studies with knowledge of plant design, operation, and material performance.

70. The expert elicitation process is focused on developing generic, or average, estimates for the commercial fleet of US reactors. The following areas are considered in broad terms within NUREG-1829 – the plant system, materials, geometry, degradation mechanism, loading, mitigation/maintenance. The study does not consider plant specific differences in developing LOCA initiating event frequencies for use in PSA modelling.

71. I raised a number of questions with Westinghouse to address whether there are any plant specific aspects of the AP1000 plant design, not reflected in the NUREG-1829 approach. If so, this would require further consideration to derive initiating event frequency data that are suitable for the AP1000 plant (Ref. 24). My questions included the following topics:

    1) Are there any unique operating characteristics that apply to the AP1000 plant design that could alter the LOCA frequencies significantly from those presented in NUREG-1829? For example, thermal transients for the plant as a whole, thermal transients or particular structural design features for the new passive decay heat removal systems.

[†††] *AF-AP1000-PSA-036. The Licensee shall provide revised frequencies, properly justified and documented, for all the initiating events in the PSA.*

2) Is the surge line between the pressuriser and the reactor coolant circuit for the AP1000 plant subject to thermal transients significantly different from existing PWR plant? The pressuriser surge line is usually a high fatigue part of PWR reactor plant.

72. Westinghouse provided its response to these items in Ref. 25 in which it stated that there are no unique features to the AP1000 plant that would preclude usage of NUREG-1829 as a source of LOCA frequencies. The AP1000 design uses similar or improved materials in comparison to operating plants, and the piping systems are designed to industry accepted codes, which all have appropriate factors of safety.

73. Westinghouse did state that the passive safety functions can cause more severe thermal transients due to the reactor cooling pumps tripping off for every safeguards actuation. However, these have been included as design transients. In addition Westinghouse stated that the AP1000 design may induce more severe thermal transients on the pressuriser surge line, but these transients have also been addressed in the design basis over the plant lifetime. The surge line would be expected to have an equivalent margin with respect to pipe breaks as any operating plant.

74. I requested the structural integrity inspector to consider the arguments that the plant transients and surge line fatigue analysis gave rise to fatigue usage factors comparable to the existing fleet of US PWR plant to validate the use of NUREG-1829 data for the AP1000 plant. The structural integrity inspector discussed this item with Westinghouse and provided me with assurance that the AP1000 plant structural integrity performance was sufficiently similar to the existing fleet of PWR reactor plant that the NUREG-1829 data was adequate to represent the AP1000 plant (Refs 26 and 27).

75. Westinghouse also stated that the AP1000 design differs from the existing operating fleet of PWRs because it has fewer reactor coolant system valves and welds, or uses newer materials that have the benefit of development from operating experience. This helps to justify that the overall frequency of LOCAs from the AP1000 plant may be lower than for existing PWRs.

76. I understand that the NUREG-1829 methodology is an industry standard choice as the source of LOCA event frequencies. It is also used for the source of LOCA frequency data for the European Pressurised Water Reactor (EPR) and UK Advanced Boiling Water Reactor (ABWR) PSAs. I consider that it contains the largest collection of operating experience known to be available, and includes a broad range of expert judgement. It is therefore a suitable source of LOCA data for the AP1000 plant PSA.

4.3.11 Rupture of Multiple Tubes in the PRHR

77. The PSA models the rupture of one PRHR tube and uses steam generator tube rupture data to derive the initiating event frequency. This initiating event is treated in the PSA in a similar manner as a small LOCA of up to 4” in diameter. Westinghouse does not present any discussion of multiple PRHR tube ruptures and whether the decay heat removal function of the heat exchanger would be maintained

78. My assessment raised RQ-AP1000-1384 (Ref. 44) requesting Westinghouse to provide additional information on the justification of the frequency for multiple PRHR tube ruptures, and to state whether the success criteria is adversely affected for multiple PRHR tube breaks such that its treatment as a small LOCA may not apply.

79. Westinghouse responded by stating that the heat exchanger tube sizes are similar to those used in the steam generators and the water quality is less challenging in the IRWST than in the steam generators. I consider there are other qualitative criteria not

discussed by Westinghouse in its response, for example, stagnant flow conditions when not in use, the tube surveillance programme, leak detection and repair criteria. If these differ significantly to the PRHR then the comparison with steam generator tube rupture date may not be valid.

80. Regarding the success criteria for multiple PRHR tube ruptures Westinghouse has not carried out any PSA success criteria analysis to demonstrate that the PRHR heat exchanger can maintain its function with more than one tube ruptured. I consider that a multiple PRHR tube rupture initiating event is credible and a justification should be provided for whether the PRHR can maintain its function following the failure of multiple tubes.

81. However, I agree with Westinghouse that a postulated multiple PRHR tube rupture event that is large enough to significantly reduce the effectiveness of PRHR is not anticipated to be risk significant since a success path is still available as a small or medium LOCA, and the initiating event frequency should be smaller than that for a single tube failure (4% for core damage frequency: Ref. 18). I consider that further consideration is needed to fully justify the PRHR tube rupture frequency and to account for multiple PRHR tube ruptures in the PSA. An assessment finding is considered appropriate to enhance the comprehensiveness of the PSA.

> **Assessment Finding (CP-AF-AP1000-PSA01-01):** The licensee shall provide the success criteria for multiple PRHR tube ruptures, and include this in the PSA. It should be determined whether PRHR tube rupture data may be better represented by heat exchanger data rather than steam generator tube rupture data.

4.3.12 Spurious Opening of the Turbine Bypass Valves

82. I requested that Westinghouse explain why spurious opening of the turbine bypass valves is not currently included as an initiating event (RQ-AP1000-1384 item A5 Ref. 44). Westinghouse explained in its response that the performance of the plant to this fault is bounded by a steam line break downstream of the main steam isolating valves (Ref. 46). Westinghouse also reviewed the frequency of pipework failures and spurious operation of the turbine bypass valves (6 off) and concluded that the likelihood of the valves spuriously opening is expected to be higher than the likelihood of steam line pipe breaks.

83. I agree with these observations and Westinghouse has stated that it will update the isolatable and non-isolatable steam line break initiating event frequencies to account for excessive steam demand events due to valves spuriously opening. Westinghouse provided a sensitivity study which showed that an upper estimate of the impact on core damage frequency from including spurious turbine bypass valves is 4%.

84. I consider that this improvement to the PSA can be done during licensing. This is based on the relatively low sensitivity of the core damage results and there is no significant impact on risk model insights. I am recording this as a technical item to be resolved together with the Step 4 GDA assessment finding AF-AP1000-PSA-012[‡‡‡] which addresses the completeness of initiating events (Ref. 11).

> **Technical item 12-4 for resolution with Step 4 AF-AP1000-PSA-012:** The licensee shall include spurious opening of the turbine bypass valves as an initiating event.

[‡‡‡] *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).*

4.4 Validation of the Human Reliability Data within the PSA

85. My assessment of the human reliability analysis within the PSA is primarily reported in the sections which discuss the event tree and success criteria modelling, the systems analysis, the Level 2 PSA analysis and the shutdown PSA. This is because I considered human reliability in an integrated manner in the context of the overall operator contribution to system reliability. However, the validation of human reliability data within the PSA using insights from the main control room simulator trials is reported separately in this section of my report.

86. The dominant contributors to risk are presented by Westinghouse in its overall summary of the PSA (Ref. 18). I observed that if the automatic initiation of the passive safety systems by the PMS does not occur then many of the fault sequences require managing by operator actions to safely shutdown the reactor and actuate the appropriate safety systems. The risk importance measures presented within the PSA show that the core damage frequency and large release frequency are sensitive to the failure of these operator actions.

87. I consulted the ONR human factors inspector on the robustness of the human factors analysis used to justify the most safety significant operator claims. Together we agreed with Westinghouse that a selection of operator tasks would be reassessed under GDA issue GI-AP1000-HF-01 (RQ-AP1000-1324 Ref. 56). This included 12 human based safety claims that I identified as important to the management of the dominant fault sequences in the PSA. These would be addressed with detailed qualitative human factors analysis. This would be followed by a risk impact study and would also take into account the Integrated System Validation (ISV) trials.

88. The ISV trials provide a comprehensive human performance based assessment using Westinghouse's AP1000 plant simulator-driven main control room and remote shutdown room interface (Ref. 57). Westinghouse advised that it had included risk significant operator tasks in its ISV trials, and that three of the PSA significant tasks ran out of time before completion. This would affect three of the 12 PSA significant human based safety claims agreed for reassessment. The ONR human factors inspector is addressing the improvements to the main control room simulator human engineering deficiencies highlighted in the ISV trials as part of GDA issue GI-AP1000-HF-01.

89. Westinghouse presented its risk sensitivity study on the 12 human based safety claims in (Ref.60). This took into account the results of the ISV trials information. This review states that three of the human based safety claims are no longer substantiated but the others are. The three that are not currently substantiated are applicable to medium and large LOCAs. The operator response for small LOCAs is substantiated. The human based safety claims that are not substantiated have been revised by Westinghouse to a value of 1.0. This was necessary for those tasks which ran out time when exercised in the main control room simulator, and are currently not considered achievable by the operators.

90. Three out of twelve (25%) of the risk important human based safety claims in the PSA have been revised by Westinghouse to a value of 1.0. This represents a significant reduction in the reliability of operator performance for these particular operator tasks. Together with the ONR human factors inspector RQ-AP1000-1721 (Ref 59) was issued to request information from Westinghouse on whether any of the remaining human based safety claims would require significant revision.

91. Westinghouse stated in its response that the three human based safety claims revised to 1.0 are based on the ISV trials not supporting successful completion of the task. For the remaining operator tasks important to the PSA the human factor assessments identified additional time and/or recovery actions which provide confidence that the

data used in the PSA remain appropriate (Ref. 61). I have discussed this with the ONR human factors inspector and agree with Westinghouse's position.

92. Westinghouse in its response to RQ-AP1000-1721 (Ref. 61) also responded to ONR's question on whether the dependency of these three operator tasks on the successful completion of other tasks had been considered and whether there are common qualitative reasons that could affect other human based safety claims. Westinghouse responded that the time available to the operators is the common factor identified between the three operator tasks that have been revised. No other common factors were found during the review that would impact the human error dependencies analysis for the PSA. I consider this statement to be reasonable as my assessment of human error dependency modelling within the PSA has found it to consistently follow Westinghouse guidance when applied. This is acceptable for GDA noting that there are human factors assessment findings to be addressed during licensing which are presented in ONR's Step 4 PSA and human factors reports (Refs 11 and 62). However, a number of potential dependency modelling queries are discussed further in Section 4.7.12.

93. I requested Westinghouse to provide additional information on what ALARP options are currently being considered to ensure that these operator actions can be completed successfully to reduce risks ALARP, and enable credit for these operator actions to be taken in the PSA. I also requested Westinghouse to state how this issue will be recorded for future resolution.

94. Westinghouse stated that it will be considering optimising the design of operating procedures, and would be reviewing the plant performance analysis to determine whether more accurate time windows could apply. Selective automation has already been considered and agreed with ONR as not required.

95. I am aware that there is a programme for improving the main control room interface and the ISV trials will then be repeated, but this is a longer term project and will be completed outside of GDA. Westinghouse stated that it will be recording this item using its human factors issues tracking system.

96. Westinghouse provided a sensitivity study in response to my request in RQ-AP1000-1721 (Ref. 61). This shows that the core damage frequency increases by a factor of 4 when the revised human based safety claims are used in the PSA. The core damage frequency remains within the ONR BSO for target 8.

97. There is further work to be completed by Westinghouse which includes 1) reviewing the time available for the operators to act, 2) taking account of improvements to the operating interface as the human engineering deficiencies in the ISV trials are addressed and 3) optimising the operating procedures. This work needs to be completed before the necessary modifications to the PSA will be clear. I am raising an assessment finding to address this.

> **Assessment Finding (CP-AF-AP1000-PSA01-02):** The licensee shall validate the dominant human error probabilities in the PSA as follows:
>
> 1) review the time available for the operators to act,
>
> 2) take account of improvements to the operating interface as the human engineering deficiencies in the ISV trials are addressed and
>
> 3) optimise the appropriate operating procedures. The licensee shall demonstrate that the risk important human actions claimed within the PSA reduce risks to ALARP. The PSA shall be revised to reflect the outcome of this work.

4.5 Review of MAAP Parameter File, MAAP Analysis and MAAP 5 Validation Status

98. The Modular Accident Analysis Programme (MAAP version 4.0.7) was used to support the success criteria for the internal events at-power PSA. MAAP is a computer code that simulates the response of a light water reactor during fault conditions. MAAP represents the reactor plant as a series of control volumes which make up the major vessels and pipework of the reactor coolant circuit and the steam generators. It treats a broad range of accident phenomena, simultaneously modelling the thermal hydraulics, fission product behaviour and conditions within the containment. The input to MAAP is a fault sequence and the automatic and manual actions to actuate safety systems. MAAP then predicts the plants response as the accident progresses. MAAP is used to generate evidence that a fault sequence is protected or not. This information is then built into the logical structure of the risk model. MAAP4 has been benchmarked against experiments and other similar codes to validate its output.

99. MAAP5 (version 5) was used by Westinghouse to support the AP1000 plant specific success path justification for the shutdown PSA. My assessment of this shutdown PSA work is presented elsewhere in this report. However, this section discusses those comments that are directly MAAP4 related.

100. My assessment of the MAAP analysis used the input to the MAAP code (MAAP parameter file), the output of the MAAP analysis to support the success criteria, the use of MAAP to support the long term cooling analysis (Refs 14, 16 and 17 respectively). I raised various RQs specifically addressing the MAAP analysis: RQ-AP1000-1657 (Ref. 41 comments 1 to 11), RQ-AP1000-1733 (Ref. 71 comments 1 to 5) and RQ-AP1000-1735 (Ref. 113). This assessment raised a selection of technical areas which I considered needed responses from Westinghouse. These are listed below:

- the use of engineering judgement due to limitations of MAAP for certain plant characteristics or physical phenomena:
- the predicted timing of passive containment cooling actuation;
- the state of the containment isolation valves in success criteria runs;
- the use of fragility analysis to determine containment failure pressure;
- the clarity required for the containment negative pressure analysis;
- the validation of MAAP4 and MAAP5;
- the presentation of MAAP inputs;
- the application of MAAP to PSA success criteria justifications for the performance of ADS stages 2 and 3.
- questions related to human actions and mitigation equipment credited in the logic model and potential MAAP analysis limitations.

101. My assessment comments concerning the validation of MAAP (4.0.7) and the benchmarking of MAAP5 against MAAP4 and other similar codes were adequately addressed by Westinghouse. Noting that the MAAP code is widely used to support light water reactor PSAs internationally, I consider that the use of the MAAP code represents relevant good practice and Westinghouse has adequately assessed its suitability for undertaking success criteria analysis for the AP1000 plant. The

responses received from Westinghouse show that the MAAP5 analysis compares well with the previous MAAP4 analysis, as well as other similar codes.

4.5.1 Use of expert judgement

102. I requested Westinghouse to explain how judgement has been used and minimised in the analysis for AP1000 plant unique events where the MAAP code lacked the necessary sophistication to model the plant design. This applied to, for example, a DVI line break, PRHR line break and spurious actuation of the squib valves (RQ-AP1000-1657, Ref. 41). I asked whether any additional work has been performed to supplement the limitations of MAAP for these events. For example, whether or not other computer codes have been used or whether MAAP5 could model these events.

103. Westinghouse is aware of the limitations of MAAP and has outlined its approach to the use of expert judgement in the success criteria notebook (Section 5.1 Ref. 16). Westinghouse has used alternative codes where needed. For example the LOFTRAN code has been used where neutron modelling is needed for ATWS events. The application of judgement is described by Westinghouse as using a conservative approach and information provided by design basis analysis codes. Westinghouse also used an expert panel to apply judgement when necessary.

104. I consider Westinghouse's response to the use of expert judgement was generally reasonable. However, I have a residual concern that Westinghouse does not appear to have a programme for developing additional analysis capability to address the limitations of MAAP as applied to the AP1000 reactor plant design. This does not adversely affect the adequacy of the success criteria analysis for GDA, but is a wider issue regarding the development of the computational methods to support future PSA work. I have therefore raised this issue as a minor shortfall for consideration during licensing.

> **Minor Shortfall (CP-MS-AP1000-PSA01-02):** Computational methods should be developed so that the use of expert judgement to derive success criteria for the AP1000 plant can be reduced in the future.

4.5.2 PCS Actuation for Long Term Containment Cooling

105. The long term cooling event tree modelling assumes success for the manual actuation of the passive containment cooling system (PCS) at 17 hours (Ref. 17). The request to justify this was raised with Westinghouse in RQ-AP1000-1657 (Ref. 41 comment 4) and RQ-AP1000-1735 (Ref. 113 comment 2). MAAP results to fully justify this time window are not available.

106. Westinghouse in its response accepted that MAAP analysis had only been performed with a 4.4 hour delay for passive containment cooling based on automatic actuation on high containment pressure. Westinghouse has agreed to review the human error modelling for this scenario and has provided arguments in its responses that this is not risk sensitive. However, I consider that further justification is needed for the success criteria applicable to the plant conditions in the long term cooling event trees. This assumes that manual actuation of passive containment cooling at 17 hours will result in a successful end state. I consider that an assessment finding is needed to record this item.

> **Assessment Finding (CP-AF-AP1000-PSA01-03):** The licensee shall perform sufficient bounding analysis to justify manual actuation of the PCS in the long term cooling models, and justify the time window assumed for manual actuation of PCS. These analyses should assume an unisolated containment.

4.5.3 Containment Under-Pressure Failure – MAAP Justifications

107. The information presented by Westinghouse in its Level 2 PSA notebook (Ref. 19; Figure 6.2-2) indicates a small margin to the under pressure failure criterion of -7.25 psid. The -7.25 psid criteria is based on a design failure pressure of -2.9 psid with an assumed 2.5 factor of safety removed. The basis for this safety factor was not presented by Westinghouse.

108. The analysis to justify the fault sequences against the under pressure failure criterion is a small LOCA. I questioned whether this choice of initiating event would present the limiting case. For example, a steam leak could displace air from the containment and when the containment is isolated the condensed steam would leave a reduced air volume in the containment which could produce a lower residual pressure. I also questioned whether account has been taken of the potential for containment bypass routes in the analysis.

109. I raised these two comments related to the adequacy of the justifications in the PSA that containment failure due to under pressure would not occur with Westinghouse in RQ-AP1000-1657 (Ref. 41).

110. The response from Westinghouse states that the analyses performed were aimed at establishing the sensitivity of operator actions to isolation time, rather than identifying a bounding scenario (Ref. 112). Westinghouse also stated that in its view sufficient margin is expected to buckling for the negative pressures predicted in PSA scenarios. It also stated that extremely low temperatures coupled with low containment heat loads that would give lower containment pressures are overly conservative for treatment in PSA. Westinghouse stated that it will consider updating this section of the analysis in future revisions to clarify its position.

111. I consider that insufficient evidence has been provided to determine whether the transient selected for the analysis of containment failure due to underpressure is bounding. The frequency of a steam leak upstream of the main steam isolating valves is very similar to that of a small LOCA, but may be more limiting.

112. I consider that the frequency of containment underpressure challenges may be low frequency as it may need a containment isolation failure to result in a bypass route together with an initiating LOCA or steam leak. However, in the context of the very low fission product release frequency claimed by Westinghouse for the AP1000 plant, I consider that further work should be pursued to provide confidence in the analysis.

113. The GDA Step 4 PSA report raised assessment finding AF-AP1000-PSA-065 which required the licensee to provide a revised containment performance analysis for the Level 2 PSA. I consider that this technical item can be considered for resolution together will the Step 4 assessment finding AF-AP1000-PSA-065[§§§].

> **Technical item 65-1 for resolution with Step 4 AF-AP1000-PSA-065:** The licensee shall perform further analysis to bound scenarios that may lead to containment underpressure challenges. This shall include a justification of the maximum differential under pressure that the containment can withstand which is suitable for use in PSA.

4.5.4 ADS Stage 2 and Stage 3 Valve Opening MAAP Model

114. The fault tree models assume that an ADS stage 2 valve and an ADS stage 3 valve are equivalent in achieving success, although the valves have slightly different

[§§§] *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.*

discharge coefficients. When the success criteria is two ADS 2 or 3 valves, all of the following lead to success according to the fault tree model: one ADS stage 2 valve and one ADS stage 3 valve, 2 ADS stage 3 valves, and 2 ADS stage 2 valves. The assumptions in the supporting MAAP success criteria should therefore bound all these possible cases. However, it was not clear to me that the modelling used by Westinghouse bounds all relevant combinations with respect to the assumed timings of the opening of the valves. I raised RQ-AP1000-1734 (Ref. 63) and further questions to Westinghouse in Ref. 71 which questioned the accuracy of the MAAP input data used.

115. The responses from Westinghouse confirmed that the bounding case has not been included in the MAAP analysis used for all parts of the PSA. However, the long term cooling MAAP analysis is not affected because an updated version of the MAAP input files are used (Refs 70 and 72).

116. In its response Westinghouse confirmed its confidence that the success criteria would not be significantly changed by updating the analysis for the relevant areas of the PSA affected. However, this item relates to success criteria results that are used throughout the PSA. I therefore consider that the analyses should be updated and I have raised this as an assessment finding. This assessment finding is presented together will another from Section 4.5.5 below which also addresses further MAAP analysis.

4.5.5 Success Criteria for PCS in the Long Term Cooling (LTC) PSA

117. The event tree with fault sequences on path LTC-003 model failure of containment isolation together with successful passive containment cooling. This fault sequence is given a successful outcome (page B-4 of Ref. 17). Passive containment cooling can operate successfully in the event of an unisolated containment but this depends upon the amount of mass lost. For the LTC-003 fault sequence I was unable to find any MAAP analyses to support this specific fault sequence. It also appears that MAAP analysis supporting the long term cooling analysis assumes a larger passive containment cooling system flow rate than the fault tree logic would permit from the systems available. I requested clarification from Westinghouse in RQ-AP1000-1735 (Ref. 113 comments 1 and 3).

118. Having assessed the response from Westinghouse I do not consider that sufficient MAAP runs have been carried out to adequately justify fault sequence LTC-003. Additional MAAP runs are needed which show that containment leakage other than large (as represented by basic event PCS-PIP-LLK-NRM) together with a minimum flowrate and an unisolated containment result in a successful end state. Depending upon the outcome of this analysis the fault tree modelling may need to be updated.

119. I consider that an assessment finding is appropriate to record the need for additional MAAP analysis. This is because there may be a significant number of fault sequences for which the LTC-003 success criteria applies.

> **Assessment Finding (CP-AF-AP1000-PSA01-04)**: The licensee shall carry out the following MAAP analysis:
>
> 1) Update the MAAP success criteria runs with updated parameter files (to Rev 1 or a later QA'd parameter file version) to generate an appropriate bounding case for the actuation of ADS2 and 3 valves. Any changes in the results in terms of ADS success criteria or time windows for human error probabilities shall be evaluated and the PSA updated accordingly.
>
> 2) carry out MAAP analysis to justify the long term cooling fault sequences on event tree path LTC-003.

4.6 Review of Success Criteria and Accident Sequence Analysis

120. My review of the success criteria and accident sequence modelling was done together by sampling the event tree model for 7 initiating events. This involved assessing the relevant information in the following documents:

- The accident sequence analysis notebook (Ref. 15).
- The success criteria analysis notebook (Ref. 16).
- The long term cooling (LTC) analysis (Ref. 17).
- The human reliability analysis notebook (Ref. 21).

121. The definition and quantification of human error probabilities is dependent on the context of the actions within the event tree models. For this reason my assessment of the human reliability aspects of the risk model was carried out as part of the event tree modelling review. The scope of the event tree review also included the long term cooling models and the functional fault tree models that support the event trees.

122. My assessment comments are recorded in RQ-AP1000-1540 (Ref. 74) and RQ-AP1000-1655 (Ref.75) and covers the following topics:

- dependencies between human actions;
- requests for additional information on MAAP analyses performed for certain sequences;
- the MAAP analysis for the long term cooling analysis;
- the containment isolation modelling for the long term cooling analysis;
- the human reliability modelling for the long term cooling models;
- the logic in the start-up feedwater fault tree for the long term cooling analysis;
- the stable end state modelling in the long term cooling analysis;
- the modelling for SG overfilling and ADS actuation in steam generator rupture fault sequences;
- information on the time windows for the small LOCA event tree;
- the modelling of dependency between initiating event and mitigation responses (also see section 2.1)

123. The response by Westinghouse to both RQs (Refs 73 and 79) provides useful information that explains the approach to addressing the human error modelling and shows that Westinghouse has based its approach on current EPRI industry guidance and this has been applied consistently throughout the risk model. Westinghouse also provided full details of the requested MAAP analyses supporting the modelling of system actuations and operator actions. The following aspects of my assessment merit further discussion.

4.6.1 Startup Feedwater in the Long Term Cooling Analysis

124. The long term cooling event tree LTCP includes modelling for decay heat removal using the startup feedwater system if passive containment cooling fails. I raised the

comment that the logic includes automatic start for the startup feedwater system when in reality manual actuation would be required in these long term scenarios (RQ-AP1000-1655 comment 7: Ref.75). The long term cooling event tree (LTCP) is used in situations where passive residual heat removal is expected to eventually become ineffective due to the eventual boil off and loss of water level in the IRWST. However, the logic for switching on the need for manual actuation is not captured in the fault tree.

125. Westinghouse presented a sensitivity study to show that the increase in core damage frequency from including the modelling of manual actuation is very small. The need for updated modelling of the startup feedwater fault trees is captured in GDA Step 4 assessment finding AF-AP1000-PSA-028[****] (Ref. 11). I consider this modelling improvement should be recorded as a technical item for resolution together with Step 4 AF-AP1000-PSA-028.

> **Technical item 28-1 for resolution with AF-AP1000-PSA-028:** The licensee shall use a fault tree model for sequences in the LTCP event tree model for startup feedwater that includes a requirement for manual rather than automatic actuation. The licensee shall review and, if necessary, update of the dependency post-processing rules should be done to capture any new combinations of human error probabilities that may arise.

4.6.2 Long Term Stable Plant State

126. The long term cooling event tree fault sequences involving success of passive containment cooling are claimed as being successful in the PSA whether the containment is assumed to be isolated or unisolated. This is because of continued operation of the passive residual heat removal system which rejects decay heat to the IRWST. However, the return of condensate from the inner surfaces of the containment to the IRWST is not completely efficient, and the IRWST water level will eventually reduce by boiling away and decay heat removal will become inadequate.

127. The ONR SAPs and PSA TAG (ESS.1 and Table A1-2.2 respectively) consider that a safe stable state is one which can be maintained in the “long-term” without the actuation of additional systems. It could be argued that the passive residual heat removal system cannot produce a fully stable end state. Hence I requested further information from Westinghouse to show how the plant state can be fully stabilised in a reliable manner such that the PSA is not underestimating the risk or missing insights (RQ-AP1000-1655, Comment 8: Ref. 75).

128. Westinghouse provided justification to show that, when using the passive residual heat removal system, overheating of the plant does not occur until 14 days on a best estimate basis (Ref. 77 and Ref. 32: chapter 9C). This work supports the closure of GDA Issue GI-AP1000-FS-06 (Ref. 78) which addresses the validation of the IRWST cooling function for the passive residual heat removal system. I have confirmed that the ONR fault studies inspector is content with this position.

129. If it is not possible to re-establish decay heat removal using the secondary systems then a number of operator actions are needed to establish open loop cooling which can be described as the final safe shutdown plant state. Open loop cooling requires manual actuation of the ADS4 valves, IRWST injection and passive containment recirculation. Extended passive residual heat removal may not correspond directly to the definition of a safe stable state in the SAPs. However, significant timescales are available for restoring power and active cooling systems. In addition, passive recirculation is available if needed.

[****] *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.*

130. I acknowledge that the passive residual heat removal system establishes an effective and justified "short-term" safe stable plant state, and that there is a straightforward route to put the plant into a longer term safe stable state.

131. However, the total frequency of entering the long term cooling (LTCP) event tree with successful decay heat removal using the passive residual heat removal system is of the order 1/year (fault sequences 1 and 4). Hence I question whether these fault sequences, even claiming credit for additional measures over an extended timescale, could present core damage sequences that are of overall importance to the PSA. I have therefore raised an assessment finding to explore this.

> **Assessment Finding (CP-AF-AP1000-PSA01-05):** The licensee shall estimate the frequency of not achieving the stable end states claimed in sequences 1, 4 and 7 of the LTCP event tree and include this in the plant core damage frequency. The licensee can also consider carrying an assessment of repair times as part of an updated quantification.

4.6.3 Initiating Events and Mitigation Systems Dependency for the PMS

132. The models for spurious actuations caused by the PMS do not include any dependency between the safety system fault trees used to mitigate the fault sequences and the initiating event. I raised this in RQ-AP1000-1655 (comment 14: Ref.75) for the initiating events of spurious actuation of passive recirculation, IRWST injection, ADS4 actuation and ADS1 to 3 actuation. All of which could involve spurious PMS signals arising from, for example, PMS common cause software faults.

133. Westinghouse confirmed that independence was assumed between the spurious actuations and the ability of PMS to respond to the fault (Ref. 76). I explored this topic further with Westinghouse in RQ-AP1000-1715 to specifically address the sensitivity of assuming that PMS would not be available after the initiating event (Ref. 92) . The response from Westinghouse showed that it was the spurious actuation of the ADS4 valves which was most sensitive as the other initiating events could be mitigated using manual intervention (Ref. 97).

134. In its response Westinghouse presented a sensitivity study which showed that the core damage frequency assuming that PMS was not available after the initiating event increased by a factor of 10. In this case the overall core damage frequency remains small and just above the ONR target 8 BSO. However, I would not expect complete dependency to apply in all cases. The frequency of core damage is small because the frequency of spurious initiating events are beyond design basis faults. This is accomplished by the design including a "blocking" device between the PMS and the field equipment. The blocking device is designed prevent spurious signals from reaching the field equipment, but to permit genuine signals for operation on demand of the field equipment.

135. I consider that the fault tree models for the actuation of safety systems following a spurious PMS initiating event should include the relevant dependency modelling. This topic has been raised previously in ONR's Step 4 GDA PSA report using assessment finding AF-AP1000-PSA-017[††††]. This captures the requirement to develop accident sequence models with adequate treatment of dependencies. I have therefore raised this as a technical item for resolution together with AF-AP1000-PSA-017.

[††††] *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.*

Technical item 17-3 for resolution with AF-AP1000-PSA-017: The licensee shall include the dependency between the initiating event and the fault tree models for the actuation of safety systems following a spurious PMS initiating event.

4.7 Review of Data Analysis

136. My assessment of the data analysis used by Westinghouse is focussed on the common cause failure data and associated modelling used for the PMS. This is because common cause failure is an important contributor to the results of a PSA, and the dominant minimal cutsets for the internal events at-power PSA highlight the importance of the PMS.

137. I raised RQ-AP1000-1734 (Ref. 63) for my assessment of the common cause modelling presented by Westinghouse in (Ref. 22). It covers the following topics:

- beta factor values and their confidence intervals;
- beta factors and common cause failure unavailabilities;
- the treatment of mean times to repair (MTTR);
- the ASME PRA standard and the use of beta-factors for consistency with the maturity of the design at GDA;
- the adequacy of the use of Westinghouse proprietary WCAP-16672-P input data (Ref. 67);
- the modelling of combinations of common cause groups of components greater than 3 using the alpha factor method;
- the modelling the inter-system common cause failures;
- use of the shape parameter < 0.5 in gamma and beta distributions for uncertainty analysis;
- The use of staggered versus non-staggered testing of components.

138. A selection of items above do not merit discussion in this report. For example, Westinghouse do not expect inter-system common cause failures to be significant because there is diversity in design between the PMS, PLS and DAS. There is also diversity in the software between PMS and PLS. This issue is being address separately for GDA issue GI-AP1000-CI-03 (Ref. 68). However, Westinghouse acknowledge there is a gap with the ONR PSA TAG on this item and this gap will be closed during the PSA update to support site licensing. Westinghouse will review staggered testing during site licensing and the PSA will be updated at that time to reflect best available anticipated operational practices.

139. There are a number of residual concerns from my assessment of the items listed above. These are discussed immediately below.

4.7.1 Beta Factor Methodology

140. The response from Westinghouse to the comments raised in RQ-AP1000-1734 (Ref 65) states that the beta factors used for the PMS common cause failure analysis are developed using the methodology presented in Annex D of the international standard IEC 61508-6 (Ref. 66). Although an acceptable methodology in principle, I consider that this analysis has not been correctly applied in all cases where it has been

used. Westinghouse has used a mathematical formula that mixes the beta factor for detected failures with the probability of undetected failures in a single PMS channel. This is not considered consistent with the method presented in section D.5 of the standard (Ref. 66). My interpretation of the standard is that the correct mathematical formula should separately account for the beta factor for undetected failures and the beta factor for detected failures. This would correctly account for detection of a potential common cause failure with corrective action taken in a timely manner before a second failure could occur. My judgement is that the overall core damage frequency would increase, but this would not be significant with respect to the ONR numerical targets. However, it could influence the ranking of minimal cutsets in the PSA and I consider that the modelling should be improved. A technical item to address all common cause failure improvements is discussed below.

4.7.2 Mean Time to Repair Modelling

141. Westinghouse has used the same mean time to repair multipliers for single component failures and their common cause failures. My concern here is that use of the same mean time to repair for a single component could lead to unrealistic assessments of the mean time to repair for multiple failures. It is very likely that the repair time for a large group of components will be far higher than for a single failure, unless there are multiple crews available. I consider that the licensee should revise the common cause failure analysis to include an appropriate mean time to repair for multiple failures. A technical item to address all common cause failure improvements is discussed below.

4.7.3 Approach to Large Common Cause Failure Groups

142. Westinghouse has taken the approach for common cause failure groups that only failure combinations of two, three or all components are modelled. Westinghouse has stated that for group sizes greater than 4 components, inclusion of the additional failure combinations with 4 or more components is not practical as it greatly increases the size of the model and has negligible impact on the results.

143. Whilst I agree that the inclusion of all additional failure combinations with 4 or more components may not be practical, I consider that further work is required to support the statement that inclusion of these events would have a negligible impact on results. Westinghouse states that the Fussel-Vessely importance for combinations which includes two failures is less than 0.1% ,and for combinations including three failures is 0.01%. However, the low impact of 2oo8 or 3oo8 component groups may not be sufficient to demonstrate that the impact of 4oo8 is small. This is because the impact depends on the level of redundancy and the system design. A system designed so that the coincident failure of 1, 2 or 3 components would not fail the system, is a system in which failure of 4ooN groups should be accounted for. A technical item to address all common cause failure improvements is discussed below.

4.7.4 WCAP Data Source

144. Westinghouse has used WCAP16672-P data which was developed under a PWR Owners Group (PWROG) programme. Peer review has been undertaken by external members of this group. However, I consider that more robust peer review would have involved external bodies who are not members of the PWROG. The justification for the data used in this work has not been visible during my review.

145. The ASME PSA standard from 2013, in safety requirement DA-C1 recommends the use of NUREG/CR-5497 and NUREG/CR-6268 for common cause failures, which contains data from different sources other than WCAP-16672. Use of these USNRC data would provide a larger database for common cause failure information.

146. I questioned why the alpha factors for failures on demand have been reduced by a factor of 2 when applied to operating or running failures (Ref. 63). Westinghouse stated that it was usual practice within the WCAP approach, but insufficient evidence was provided.

147. My sampling has observed one case where that the common cause failure probabilities can be numerically very close to the probabilities for independent coincident failures. An example of this applies to the main AC power system breakers. The failure probability of basic event ECS-CBK-FTO-61(52) is 2.5×10^{-3}/demand. The probability of random coincident failures of both ECS-CBK-FTO-61(52) and ECS-CBK-FTO-62(52), assuming their independence would be 6.5×10^{-6}/demand. However, their common cause failure, which is denoted by basic event ECS-CBK-FTO-08-01_7_8, has been assigned a failure probability of 7.7×10^{-6}/demand. This is almost the same as their independent coincident failure probability. These data are not consistent with ONR SAP EDR.3 (common cause failure) which advises that common cause failure data better than 10^{-5}/demand are not expected and require particular justification or revision. Based on engineering judgement alone, it would appear that this common cause failure probability is too small. This will reduce the perceived importance of these components within the PSA. I consider that such small common cause failure probabilities need to be reviewed and justified to ensure their importance is properly represented within the PSA.

148. I note that the main AC power system is not needed to support decay heat removal once the AP1000 plant passive safety systems are initiated. This will reduce the overall importance of these components in the PSA when compared to conventional PWR plant which require power supplies for decay heat removal. For this reason I am content for this item to be addressed during licensing.

149. The use of reliability data within the PSA and the revision of common cause failure modelling has been raised previously in the ONR Step 4 GDA PSA report as assessment findings AF-AP1000-PSA-039[‡‡‡‡] and AF-AP1000-PSA-042[§§§§] (Ref. 11) respectively. I consider that the common cause failure improvements discussed above can be resolved together with these two Step 4 assessment findings.

> **Technical item 42-1 for resolution with Step 4 AF-AP1000-PSA01-042:** The licensee shall resolve the following common cause failure modelling items in the PSA:
>
> 1) The beta factor analysis should be revised to include beta factors for both detectable and non-detectable failures.
>
> 2) The common cause failure analysis should be use a higher value of mean time to repair for multiple failures than for single failures.
>
> 3) Further work is needed to demonstrate that inclusion of common cause failure events with 4 or more combinations of components will not have a significant impact on the total core damage frequency.
>
> 4) Evidence should be provided that WCAP16672-P data is adequate for common cause modelling by making the independent peer reviews available, and considering whether the USNRC data should also be used to enhance the size of the database.

[‡‡‡‡] *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."*
[§§§§] *AF-AP1000-PSA-042: "The Licensee shall provide revised CCF probabilities properly justified and documented"*

5) A justification should be provided for reducing the alpha factors by a factor of 2 for operating equipment.

6) Within the PSA there are common cause failure probabilities that have a similar value to the independent coincident failure of the components by chance (beta factors of less than 1%). The justification for these values needs review and the common cause failure probabilities modified accordingly.

4.7.5 Review of Level 2 PSA and New Plant Damage States

150. My assessment of the Level 2 analysis notebook (Ref. 20) and risk model (Ref. 18) covered the Plant Damage State (PDS) definitions, the overall structure of the Level 2 PSA and a sample of sequence and phenomenological issues.

151. I raised RQ-AP1000-1588 (Ref 84) which covered the following topics:

- the treatment of long term cooling transfers;
- the simplified treatment of the Large Bypass (BL) end state;
- the quantification of the risk model;
- PDS grouping simplifications and the carry through of specific PDS characteristics to the Level 2 model;
- modelling omissions related to In-Vessel Retention (IVR) and Induced Steam Generator Tube Rupture (ISGTR) phenomenological events;
- the timing for containment isolation claims in the Level 2 model;
- the Containment Event Trees (CET) for Small Bypass (BS) and BL PDS;
- human error probability dependencies;
- the calculation of containment failure probability due to overpressure;
- the modelling impact of PRHR on containment failure timing.

152. The following section discusses the residual matters arising from my assessment where I consider that further work is needed to improve the Level 2 PSA.

4.7.6 Transfers of Bypass Fault Sequences to LTC Event Trees

153. RQ-AP1000-1588 (Ref 84 :comment 1) requested Westinghouse to explain the observation that there are some fault sequence transfers from the Level 1 event trees for SGTR to the long term cooling event trees which lose the containment bypass nature of the initiating event. This logic does not appear to be recovered in the Level 2 model. The modelling therefore appears to be optimistic. For example, there may be pressurised fault sequences which could result in releases via secondary side safety valves should long term cooling fail. The fault sequences of concern are SGTR sequences 1, 2, 3, 5, 11, 13, 18, 20, 25, 27, 32, 33, 34, 36, 43, 45, 51, 53, 59, 61, 67 and 69.

154. In response to the question Westinghouse provided an adequate explanation for plant damage states in which ADS stage 1 to 4 had successfully operated and the plant would be depressurised (fault sequences 19, 21, 22, 52, 54 and 55 of SGTR). However, these fault sequences do not transfer to the LTC event trees and the

containment bypass nature of the fault sequences is retained. Westinghouse did not provide adequate explanation for the SGTR fault sequences listed above which transfer to the LTC event trees and may be treated as non-bypass fault sequences, whether pressurised or not (Ref. 83).

155. This may be a shortfall in the Level 2 risk model, which could lead to optimistic results. The concern is that the sequences in question are containment bypass events on entry to the long term cooling modelling but they are transferred to the Level 2 in a way which leads to them being subsequently treated as non-bypass events. The ONR GDA Step 4 PSA report raised assessment finding AF-AP1000-PSA-058[*****] which required revised analysis of the interface between the Level 1 and Level 2 PSA regarding allocation of Level 1 PSA fault sequences into plant damage states and transfer of these into the Level 2 PSA. I am raising this concern as a technical item to be considered together with the Step 4 assessment finding.

> **Technical item 58-1 for resolution with Step 4 AF-AP1000-PSA01-058:** The licensee shall review the risk model to ensure that the bypass character of the fault sequences transferred from the Level 1 model to the Level 2 model is not lost.

4.7.7 Conservative Treatment of Large Bypass Fault Sequences

156. RQ-AP1000-1588 (comment 2: Ref 84) noted that the Level 2 model has some degree of conservatism due to the large bypass plant damage state treatment being simplified. This is because it does not credit secondary side scrubbing in the steam generators. The ASME standard for large early release frequency refers to using a realistic treatment of secondary side scrubbing. I discussed this with Westinghouse and it stated that the main objective of the Level 2 PSA is to calculate large release frequency rather than the full range of source terms to characterise societal risk (Ref. 83). I consider that this modelling improvement should be incorporated in anticipation of the need to provide more refined risk measures against ONR numerical targets during licensing.

> **Assessment Finding (CP-AF-AP1000-PSA01-06):** The licensee shall include secondary side scrubbing for steam generator tube rupture events in the Level 2 risk model.

4.7.8 Quantification of the Model

157. I raised RQ-AP1000-1588 (comment 3: Ref 84) because I could not reproduce the numerical results from the Level 2 PSA. The comment requested Westinghouse to provide the CAFTA quantification settings for re-producing the results of the Level 2 PSA. This was discussed with Westinghouse and it presented the relevant information in its response to RQ-AP1000-1588 (Ref. 83). I was able to reproduce Westinghouse's quantitative results for the Level 2 PSA using this information. However, I found that in order to quantify the model without an error message, a change was required in the Flags Quant.txt file, as follows:

> Original line: FL-GTRAN-WS .T
>
> Modified line: FL-GTRAN-WS EQU .T

[*****] *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.*

158. "EQU" was missing for the original file. Making this change did not appear to alter the numerical results†††††. I consider that the flag file should be corrected. Because the results do not appear to be affected, and the model will undergo re-quantification as it is developed during licensing, I have therefore assigned this model item as a minor shortfall.

> **Minor Shortfall (CP-MS-AP1000-PSA01-03):** The "Flags Quant.txt" file should be corrected.

4.7.9 Additional Containment Challenges from Severe Accident Phenomena

159. I raised RQ-AP1000-1588 (comment 4: Ref 84) to clarify a simplification in the containment event trees. The question to establish the status of small containment isolation failure is asked after it has been established that no large containment isolation failure has occurred. The modelling appears to be incomplete and potentially optimistic. This is because the small isolation failure status of the containment appears to have been established prematurely. The modelling does not allow for severe accident phenomena, such as an induced steam generator tube rupture, to occur later in the fault sequence. Such an event could produce a larger release. The large early release frequency may therefore be under predicted and additional containment bypass routes need to be included.

160. Westinghouse agreed that the modelling needs to be improved, and provided a sensitivity study (Ref. 83). Westinghouse stated that the large release frequency would increase by up to 27%. The revised large release frequency remains within ONR target 9 BSO.

161. The ONR Step 4 GDA PSA report includes assessment finding AF-AP1000-PSA-070‡‡‡‡‡ which identifies shortcomings in the Step 4 containment isolation model. I have assigned this as a technical item to be resolved together with the Step 4 assessment finding.

> **Technical item 70-1 for resolution with Step 4 AF-AP1000-PSA01-070:** The licensee shall update the containment event tree models used in the Level 2 PSA so that relevant severe accident phenomena are also evaluated in sequences where a small loss of containment isolation has occurred.

4.7.10 Plant Damage State Simplifications

162. In RQ-AP1000-1588 (comment 5: Ref 84) I requested justification of some simplifications implicit in the plant damage state grouping and subsequent treatment in the Level 2 containment event trees. The simplifications implied that Anticipated Transient Without Scram (ATWS) events were treated identically to non-ATWS high pressure core damage sequences. My concern is that an ATWS could be more onerous for Level 2 phenomena than a high pressure fault sequence without an ATWS. For example, an induced steam generator tube rupture could be a more severe challenge to the steam generator tube integrity following an ATWS. Westinghouse did not provide an adequate justification for this treatment (Ref. 83). I conclude that as a minimum the models require further documented justifications, but there may also be some degree of optimism in the models due to the non-bounding treatment of ATWS core damage sequences.

163. RQ-AP1000-1588 (comment 7: Ref 84) concerned the transfer of fault sequences from the plant damage states to the HP6 containment event tree: 1) ATWS with no ADS

---

††††† *It should be noted however, that a full cut set comparison was not performed.*
‡‡‡‡‡ *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.*

(AN), 2) ATWS with no ADS and no reflood (ANF), 3) high pressure with no ADS (HN), 4) high pressure with no ADS and no reflood (HNF), and 5) high pressure with no IRWST injection (HI). For the first four plant damage states the status of IRWST injection and recirculation is unknown. In the fifth (HI) plant damage state IRWST injection is known to have failed. I consider that the boundary conditions applicable to event tree HP6 should be that IRWST injection has not happened, and as HN and HNF (etc.) are grouped to represent a high reactor coolant system pressure, it should also be assumed that the accumulators and CMTs are unable inject. The current approach appears to introduce optimism into the model. I requested Westinghouse to justify that following core damage there is sufficient water covering the core debris to remove decay heat in sequence 1 of HP6 without any IRWST, CMT or accumulator water.

164. Westinghouse argued that for all the different possibilities transferred into containment event tree HP6, reactor coolant circuit water is expected to be in the reactor cavity (Ref. 83) and therefore available for core cooling. However, the levels of water present in the cavity for the different combinations of CMT, accumulator and IRWST injection success or failure were not discussed and no MAAP analysis was presented. I consider the response is insufficient to demonstrate that the scenarios are adequately bounding and that timings, ex-vessel cooling or other accident progression phenomena would not be affected to a greater or lesser extent by the variations between the grouped scenarios. As a minimum, I consider that documentation improvements are needed.

165. I raised a further question on the grouping of plant damage states in RQ-AP1000-1588 (comment 24: Ref. 84). The following two plant damage states are treated identically in the Level 2 risk model, 1) reactor coolant system pressure high, ADS discharge into containment, IRWST injection failed (HCI) and 2) reactor coolant system pressure high, ADS sparging into the IRWST then into containment, IRWST injection failed (H2I). This implies that the presence of hydrogen in the IRWST (then discharged into containment) can be treated the same as hydrogen discharged into the ADS4 compartments. Westinghouse in its reply provided a clear explanation of the modelling used but agreed that improved documentation and possibly some refinement of the modelling would be appropriate (Ref. 87).

166. The justification of the plant damage state groupings is raised in ONR's Step 4 GDA PSA report using assessment finding AF-AP1000-PSA-057[§§§§§]. I have therefore raised the technical items associated with plant damage state simplifications to be resolved together with the Step 4 assessment finding AF-AP1000-PSA-057.

> **Technical item 57-1 for resolution with Step 4 AF-AP1000-PSA01-057:** The licensee shall address the following items within the plant damage state and Level 2 modelling:
>
> 1) Separate plant damage states should be considered for ATWS and reactor coolant system high pressure core damage fault sequences.
>
> 2) The transfers of plant damage states AN, ANF, HN, HNF and HI to containment event tree HP6 and the implied loss of detail related to CMT, accumulator and IRWST injection should be reviewed and if necessary modified.
>
> 3) The documentation explaining the treatment of plant damage states H2I and HCI should be improved.

[§§§§§] *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.*

4.7.11 Induced Steam Generator Tube Rupture (ISGTR)

167. Westinghouse includes induced steam generator tube rupture in its risk model when the primary side is at high pressure and the secondary side is depressurised. Westinghouse assigns a probability of zero to induced steam generator tube rupture when the secondary side is pressurised. I raised RQ-AP1000-1588 (comment 8: Ref 84) to address this.

168. I consider that the stress across the steam generator tubes is reduced if the secondary side is pressurised, but it does not follow from this that the probability of induced steam generator tube rupture is zero in such a scenario. It only follows that the probability would be lower than in the case of a depressurised secondary side. NUREG-1570 (Ref. 80) supports this interpretation. The response by Westinghouse discusses MAAP analysis using default assumptions is useful but I do not consider it to be sufficient (Ref. 83). A wider range of variations in the input parameters for the MAAP analysis is needed. The results of these additional analyses should be used as part of a robust process to generate a probability of severe accident induced steam generator tube rupture probability for accident sequences where the secondary side of the SG remains pressurised.

169. I consider that the modelling for induced steam generator tube rupture is not adequately complete. This may result in the large release frequency being underestimated because a steam generator tube rupture can bypass containment. I have therefore assigned this as an assessment finding.

> **Assessment Finding (CP-AF-AP1000-PSA01-07) :** The licensee shall perform a more detailed assessment of severe accident induced steam generator tube rupture in accordance with NUREG-1570 for scenarios where the steam generator secondary side remains pressurised. A probability of induced steam generator tube rupture for this case should be generated and included in the containment even trees.

4.7.12 Level 2 Human Error Dependency Modelling

170. For fault sequences with multiple operator actions it needs to be determined whether the later actions are influenced by the success or failure of the previous actions. I consider this aspect of the modelling used by Westinghouse to be generally acceptable across the majority of the PSA. However, when assessing this aspect of the Level 2 PSA and I raised RQ-AP1000-1588 (comment 13: Ref 84) where it appears that the level of dependency may have been inadequately addressed and therefore optimistic. My comments apply to operator actions undertaken to depressurise the plant before and after core damage. The cases identified in my comment are:

> 1) HEPO-ADS-GT (operator fails to depressurise the reactor coolant circuit using ADS1 to 3) and HEPO-COG-CORECOOLING (operator fails to diagnose inadequate core cooling).
>
> 2) HEPO-ADS-GT and HEPO-L2-ADS13 (operator fails to depressurise the reactor coolant circuit with ADS 1 to 3 on loss of core cooling).

171. Four coupling factors are applicable to these operator actions, these being:

- The same people are involved (the main control room team);
- A very similar time window applies (there is an additional 5 minutes available for the second Level 2 actions);

- Same response is required by the operators;
- Similar cues to prompt operator actions are expected.

172. Westinghouse in its response address only the time window aspects (Ref. 83), arguing that the actions in the combinations identified above are “not simultaneous” and are “expected to be over 30 minutes apart”. This is acknowledged, however additional considerations apply as explained below.

173. The end of the time window for HEPO-ADS-GT is imminent core damage which is an irreversible state. In the cutsets where HEPO-ADS-GT is failed it is implicit that the operators have failed to act correctly at that time. This is a key point to note. It cannot be argued that the two operator actions are decoupled based on normal expected timings if the situation being assessed is a failed initial operator response. On a failure sequence the normally expected operator actions have not been achieved in a timely manner.

174. In the fault sequence the operator action HEPO-ADS-GT is failed at the time of core damage, and there is only an additional 5 minutes to the cue for the second operator action, which is short compared to the 54 minute time window available for HEPO-ADS-GT. I consider that high or complete dependence should be considered as the appropriate assignment of dependency in this case.

175. My review concludes that the dependency level is underestimated and that there may be further similar cases where the dependency level was underestimated. This broader review of the modelling was not addressed by Westinghouse in its response. The concern is that the current modelling approach to operator dependency may under-estimation the large release/large early release frequency.

176. However, following discussion with Westinghouse I recognise that well defined guidance has been followed systematically for modelling dependency within the risk model, but I consider that the guidance applied should be reconsidered in this specific case. The GDA Step 4 PSA report raised assessment finding AF-AP1000-PSA-059[******] which required a revised treatment of dependencies between the human actions before and after core damage. I have therefore assigned this technical item to be addressed together with the Step 4 assessment finding.

> **Technical item 59-1 to be resolved with Step 4 AF-AP1000-PSA-059:** The licensee shall review the operator dependency modelling in the PSA as follows:
>
> 1) Where combinations of human error probabilities occur in which the end of the time window for the first human error probability is close in time to the cue for the second one, the level of dependency should be reviewed. This should be done for the PSA as a whole.
>
> 2) If separation in time has been used as the reason to reduce dependency levels, the licensee should consider whether the dependency level should be increased.
>
> 3) The licensee should review the guidance used for the assignment of dependency and consider whether or not these rules need to be modified to account for cases such as those described in his section of this report. A justification for the final decision to update the dependency assignment rules or not should be developed and documented.

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

4.7.13 MAAP Analysis Supporting Containment Overpressure

177. My comment in RQ-AP1000-1588 (comment 14: Ref 84) requested Westinghouse to explain the MAAP analysis results used to justify the containment over pressure failure probability. This is for over pressure when the reactor pressure vessel has failed, a molten core concrete interaction occurs and passive containment cooling has failed. The containment pressure at 24 hours is used to determine the failure probability (Ref. 19: Table 7.3-16). The MAAP run shows that the containment pressure initially rises then falls after approximately 9 hours then continues to rise thereafter. An explanation of the pressure trend in the MAAP analysis is needed to confirm whether the correct analysis has been used. I consider the fault sequences to be low frequency but the consequence can be a large release. I consider that an assessment finding is appropriate.

> **Assessment Finding (CP-AF-AP1000-PSA01-08):** The licensee shall provide justification that the results of the MAAP analysis adequately support the derivation of the containment over pressure probability (L2-CF-EV1).

4.7.14 Changes to the GDA Step 4 Plant Damage States

178. A steam line break inside containment was mapped to a single plant damage state in the GDA Step 4 Level 2 PSA. This would capture any unique elements of the fault sequence. However, a steam line break has been lumped together with other plant damage states which are treated identically in the current Level 2 PSA. I raised RQ-AP1000-1588 (comment 16: Ref 84) which requested explanation. Westinghouse states that the change has mapped a steam line break inside containment to a general high reactor coolant system pressure plant damage state. I do not consider this explanation to be adequate. This is because a steam line break inside containment will produce an elevated pressure inside containment. This has the potential to adversely influence the probability of containment failure. It is not apparent that the current plant damage state treatment recognises this characteristic of a steam line break inside containment.

179. I consider that additional investigation is needed of the resulting containment pressure from a steam line break inside containment, and justified against the plant damage state treatment currently used. Westinghouse should also consider whether the Level 2 plant damage state assignments and subsequent containment event tree modelling needs to be modified.

180. The GDA Step 4 PSA report raised assessment finding AF-AP1000-PSA-057[††††††] which concerns the justification of the plant damage states. I consider this technical item can be resolved together with the Step 4 assessment finding.

> **Technical item 57-2 for resolution with Step 4 AF-AP1000-PSA01-057:** The licensee shall provide justification for the plant damage state grouping of steam line break core damage fault sequences.

181. The GDA Step 4 PSA distinguishes between steam generator tube rupture fault sequences resulting in early or late core damage. The new Level 2 PSA treats all core damage fault sequences arising from steam generator tube ruptures as large containment bypass events. Westinghouse states that its risk model is currently used to address the frequency of a large release. However, differentiation between the timing of the releases is lost and this is likely to influence the impact of radioactive decay on the fission product source terms used within a Level 3 analysis.

[††††††] *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.*

182. I consider that the plant damage treatment used in the Step 4 Level 2 analysis provided a more appropriate level of detail, as it distinguishes between the two different cases. I have assigned this item as a technical item to be addressed during the licensing phase so that the PSA will support the calculation of the risk metrics required by the ONR SAPs. This will support the development of the Level 3 PSA during licensing and can be resolved together with Step 4 assessment finding AF-AP1000-PSA-057.

Technical item 57-3 for resolution with Step 4 AF-AP1000-PSA01-057: The licensee shall update the steam generator tube rupture Level 2 modelling so that early core damage and late core damage fault sequences and treated separately.

4.7.15 Systems Analysis Assessment

183. My assessment of the systems analysis is based on sampling various aspects of the PMS, PLS and DAS. The Protection and Safety Monitoring System (PMS) is a software controlled class 1 SSC which is used to actuate the class 1 passive safety systems. The Plant Control System (PLS) is used for normal plant operations and control of the non-Class 1 safety systems and equipment. The Diverse Actuation System (DAS) is a solid state class 2 SSC which provides diverse backup to the PMS. The DAS and the PMS use independent and separated power sources and internal power supplies.

184. My assessment concentrates on the PMS because it appears in the dominant minimal cutsets of the PSA and therefore plays an important role in demonstrating that risk is very small for internal events at-power. I have also assessed the systems modelling for the some of the equipment actuated by the PMS.

185. My assessment uses the PMS systems analysis notebook supporting the PSA as its basis (Ref. 88). This includes the supporting information for various aspects of the system analysis methodology, and I have sampled the electronic event tree/fault tree models using the CAFTA computer code.

186. My assessment is presented in RQ-AP1000-1589 (Ref. 89) and RQ-AP1000-1715 (Ref. 92) which include input and discussion with ONR control & instrumentation and mechanical engineering inspectors. These RQs explore Westinghouse's claims in the systems analysis and the sensitivity to risk of various uncertainties identified in my assessment. The technical items explored are presented below:

- The claims for software common cause failure of the PMS and PLS.
- The claims for the frequency of spurious actuations of safety systems due to common cause failure of the PMS.
- The availability of PMS functions after a spurious PMS actuation.
- The blocking device to prevent spurious actuation of the squib valves.
- The risk benefits and detriments of a safe-arm device to prevent spurious actuation of the ADS4 valves.
- The modelling used for spurious opening of IRWST injection valves**.**
- Dependent failure modelling for the PMS hardware.
- The reliability of the DAS.

- Failure on demand of ADS 1-3 Valves.
- Failure on demand of the IRWST gutter bypass isolation valves.
- Failure on demand of the Automatic Depressurisation System (ADS) Stage 4 (ADS4) valves.

My assessment of the ADS 1-3 valves and the IRWST gutter bypass isolation valves is reported within the common cause failure analysis sections of this report (Sections 4.7.1 to 4.7.4). My assessment of the final item in the above list did not give rise to any specific items for which a response from Westinghouse was required (Ref. 85).

4.7.16 Software Common Cause Failure of the PMS and PLS

187. The ONR C&I Inspector advised me that the reliability claimed by Westinghouse in the PSA for PMS failing on demand due to software common cause failure at $1.2x10^{-6}$/demand is not consistent with advice presented in the international regulators' common position paper on the licensing of safety critical software for nuclear reactors (Ref. 93). This position paper states that claims of ultra-high software reliability cannot be demonstrated with current techniques, therefore a decision needs to be made on the limit that can be claimed for a computer based system.

188. The common regulators' position that reliability claims for a single software based system important to safety of lower than 10^{-4} (either "on demand" or as an annual frequency) shall be treated with extreme caution. It also states that the sensitivity of plant risk to variation of the reliability assumed shall be assessed. I therefore requested Westinghouse to undertake a risk sensitivity study by using a broad selection of alternative common cause failure data for the PMS and PLS software. For the PMS this covered software common cause failure data between 10^{-6}/demand to 10^{-3}/demand. For the PLS this covered common cause failure data from 10^{-6}/demand to 10^{-2}/demand.

189. Westinghouse presented the sensitivity study for the core damage frequency in its response to RQ-AP1000-1589 (Ref. 90) and RQ-AP1000-1715 (Ref. 76). This demonstrates that for the most conservative values of PMS and PLS common cause software failure probabilities (10^{-3}/demand and 10^{-2}/demand respectively) the core damage frequency increases by a factor of 13. The combined impact of increasing the software common cause failure probabilities to 10^{-4}/demand for the PMS and 10^{-3}/demand for the PLS, is an increase in the core damage frequency by less than a factor of 3.

190. In its response to RQ-AP1000-1589 (Ref. 90) Westinghouse stated that it would update its PSA data for PMS and PLS software common cause failure from $1.2x10^{-6}$/demand for both the PMS and PLS to 10^{-4}/d for the PMS and 10^{-3}/d for the PLS. This change increases the core damage frequency by less than a factor of 2 and it remains within ONR target 8 BSO.

191. I acknowledge that the derivation of best estimate software reliability data for use in PSAs is a difficult area where relevant good practice is not well developed. However, the revised data selected by Westinghouse is at the lower end of the range advised by the regulators' guidance. I consider this is not unreasonable for use in a PSA where it is used to explore the impact of best estimate judgements.

192. Westinghouse has agreed to update the data used for the PMS and PLS in the next revision of the PSA. I am recording the update of the common cause failure data for PMS and PLS software as an assessment finding.

Assessment Finding (CP-AF-AP1000-PSA01-09): The licensee shall include in the PSA the updated data for software common cause failure for both the PMS and PLS.

4.7.17 Frequency of Spurious PMS Initiating Events

193. The common cause failure of PMS software to generate spurious signals is modelled in the PSA as a series of initiating events. This failure mode of the PMS may potentially cause spurious actuations of the three sets of squib valves on the plant. These are:

- The ADS4 squib valves which control the final stage of depressurisation.
- The IRWST injection squib valves which open to permit gravity injection into the core following a LOCA.
- The IRWST recirculation squib valves which open to permit recirculation of water between the containment sump and the core.

194. The frequency used by Westinghouse for software common cause failure of the PMS to generate spurious signals is based on guidance in ONR SAP EDR.3 (Ref. 3: clause 185). This clause discusses limitations on the expected claims for common cause failures depending upon the complexity and novelty of the system. Although the PMS is not a novel system as it has been implemented in multiple plants, it is a relatively complex system. Consequently Westinghouse has chosen the minimum acceptable value for use in nuclear safety cases for dangerous failures as 10^{-3}/year.

195. Westinghouse makes the assumption that 10% of the total frequency for spurious actuations is due to software common cause failure and the initiating event frequency for the PMS is therefore assumed to be 10^{-4}/year. The justification for this approach is not made robustly by Westinghouse, but I note that the derivation of best estimate software reliability data is an area in which the relevant good practice not well developed. I asked Westinghouse to present a sensitivity study by using 10^{-3}/year for the initiating event frequency instead of using 10^{-4}/year. The core damage frequency increases by less than a factor of 2 and remains within the ONR target 8 BSO (Ref. 90).

196. The AP1000 plant design has now been fitted with a “blocker” between the PMS and the squib valves. The blocker is a solid state electronic device which will not permit a PMS actuation signal to the squib valves unless it confirms the plant state is changing accordingly. The blocker reduces the initiating event frequencies for PMS spurious actuation of the squib valves to lower than 10^{-6}/year. I consider that these faults are beyond design basis initiating events when assessed with respect to ONR target 4. This is supported by closure of GI-AP1000-CI-04 which addresses the safety justification for PMS spurious operation (Ref. 91). The blocker reduces the core damage frequency from spurious PMS initiating events to a very small value. I consider that the risk is insensitive to the modelling used in the PSA and no findings are necessary to take this further.

4.7.18 Spurious ADS4 Actuation ALARP Analysis

197. A spurious ADS4 initiating event results in a LOCA the size of which depends on the number of valves that open. The spurious opening of one ADS4 valve results in a medium LOCA and the opening of 2 or more ADS4 valves results in a large LOCA. The success paths available are presented by Westinghouse in the spurious ADS4 event tree and the accident sequence notebook (Ref. 15 Section 7.11). The accident sequence notebook and the PSA currently identify a success path for all spurious ADS4 initiating events. This is because Westinghouse assumes within the PSA that

PMS is always available to undertake rapid automatic actuations of the passive safety systems. This assumption applies for all failure modes of the PMS including a spurious actuation due to a common cause software fault.

198. For spurious opening of 2 or more ADS Stage 4 valves the common cause failure of PMS software combined with failures of the blocking device is the dominant failure mode. All other PMS hardware failures combined with failure of the blocking device is an order of magnitude lower. I therefore investigated the potential for common cause failure between the initiating event and the response of PMS to the fault in RQ-AP1000-1715 (Ref. 92). I raised this particularly to address the impact of the PMS software being the common cause of the PMS becoming unavailable after the initiating event occurs.

199. The response from Westinghouse stated that for a spurious opening of 2 or more ADS4 valves, automatic PMS is the only available means to support core cooling since manual actions cannot currently be justified on the short times needed to protect a LOCA of this size (Ref. 98). However, spurious opening of only 1 ADS stage 4 valve can be protected by operator action.

200. The response from Westinghouse indicates that the current risk model does not reflect the core damage fault sequences arising should the PMS not be available following a spurious opening of 2 or more ADS4 valves. I requested a sensitivity study from Westinghouse to understand the risk impact of these additional core damage fault sequences.

201. Westinghouse presented a sensitivity study which considered a conditional probability that PMS would be failed after the initiating event (Ref. 98). This uses values ranging between 0 (the PMS never fails) and 1.0 (the PMS always fails). The core damage frequency increases by a factor of 3 for a conditional probability of 0.1, and a factor of 10 for a conditional probability of 1.0. For the latter sensitivity study the core damage frequency is at the ONR target 8 BSO.

202. I understand that the derivation of best estimate software reliability data for PSAs is a difficult area where relevant good practice is not well developed. It remains uncertain which best estimate data should apply. However, the PSA has played a useful role in understanding the risk sensitivity, and I consider that the PSA needs to be updated to include the potential for PMS software common cause failure modes with the spurious PMS initiating events.

203. The sensitivity is such that I investigated the potential for ALARP options in discussions with Westinghouse (Ref. 104). The sequencing of operator actions in response to a large LOCA with PMS failed is an item for further investigation. However, this requires careful consideration for the potential impact on other LOCA events. I agreed with Westinghouse that this can be investigated during the licensing phase.

204. I also investigated with Westinghouse whether core protection could be demonstrated with delayed operator action for a spurious ADS4 event with PMS failure. This may influence the development of the operator response. Westinghouse stated that it had not investigated the performance of the reactor for this fault sequence. I consider this analysis should be addressed because it may influence the development of operating procedures and the ALARP position. An assessment finding has therefore been assigned so that this specific modelling issue is considered in the development of the PSA for licensing.

> **Assessment Finding (CP-AF-AP1000-PSA01-10):** The licensee shall carry out ALARP analysis for the core damage sequences from spurious ADS4 actuation arising from software common cause failure. This shall include the

potential for optimising the operators response and whether a delayed operator response can protect the plant.

4.7.19 The Blocker Design

205. The PMS will include a blocking device in each division to prevent spurious actuation signals reaching the ADS, IRWST and containment recirculation squib valves. The blocking device uses conventional analogue components and does not rely on software. The blocking device is being redesigned by Westinghouse to address assessment work for the GDA C&I issues (Ref. 91). I requested Westinghouse to confirm whether the current PSA includes the redesigned blocking device in RQ-AP1000-1589 (Ref. 89).

206. In its response to RQ-AP1000-1589 (Ref 90) Westinghouse stated that the latest blocking device design is not credited in the risk model for at-power internal events. The redesigned blocker reduces the dependency on the Component Interface Modules (CIMs). The ONR C&I Inspector confirms that the new design is expected to be more reliable than the existing design assumed within the current PSA. Once the blocking device is finalised for the UK AP1000 plant, I consider that the PSA should be updated during site licensing. A minor shortfall is considered appropriate for this technical item.

Minor Shortfall (CP-MS-AP1000-PSA01-04): The PSA should include the latest blocker design.

4.7.20 Risk Balance of Fitting a Safe-Arm Device

207. The ONR mechanical engineering inspector raised the use of a safe-arm device as a further ALARP measure to reduce the frequency of spurious squib valve actuations arising from faults in the PMS. A safe-arm device is an electromechanical component that provides a small metal plate between the two squib valve charges. It interrupts the explosive train in the event of a spurious signal to the valve. The metal barrier is motorised and can be moved aside when a genuine actuation is required. The proposed design would permit actuation of the valve on low Core Make-Up (CMT) level which indicates a LOCA has occurred. A safe-arm device would have a positive benefit in reducing the likelihood of a spurious squib valve opening but would have a negative impact on the reliability of a squib valve to open on demand.

208. Westinghouse was requested by ONR to provide a risk balance analysis as part of a broader ALARP review for the safe-arm device option at a cross-discipline meeting (Ref. 103). Design alternatives for a safe-arm device and the risk balance analysis is presented by Westinghouse in its response to RQ-AP1000-1715 (Ref. 98 Section 5.2).

209. The risk balance includes a range of sensitivity studies to address parametric uncertainty for the failure modes of the safe-arm device: failure to open on demand, failure to block a spurious actuation signal and common cause failure for both of these failure modes for multiple squib valves. The sensitivity studies showed that the safe-arm device was effective at blocking spurious signals. However, it also demonstrated that the expected range of reliability for its mechanical components to operate on demand to remove the barrier between the explosive train was a limiting feature, and was less reliable than the squib valves themselves. The safe arm device would protect against one failure mode of the PMS, but the limiting feature would reduce the reliability of the squib valves to actuate on demand for all LOCA initiating events.

210. Given that the ADS4 valves play a crucial role in depressurising the plant to permit the passive safety features to operate effectively, the risk balance analysis shows that there was an overall increase in core damage frequency if a safe-arm device was fitted. In my judgement the risk balance clearly shows that the safe-arm device is an overall risk detriment. I provided this judgement to the mechanical engineering

inspector to support his overall judgement that fitting a safe-arm device is not needed to demonstrate that risk is reduced ALARP (Ref. 99).

4.7.21 Dependent Failure Modelling for the PMS Hardware

211. My assessment of the overall approach used to model PMS hardware common cause failure in the PSA showed that Westinghouse has used the work done for the Swedish Ringhals Unit 2 reactor for use within the current AP1000 plant PSA. Westinghouse technology is used on the Ringhals plant for the reactor protection system and the analysis was undertaken in 2005.

212. I requested that Westinghouse presents a justification of equivalence between the Ringhals and AP1000 designs to justify the read across of the Ringhals common cause failure beta factor analysis for the PMS hardware to the more modern AP1000 PMS design (RQ-AP1000-1589 Ref. 89). Westinghouse explained in its response (Ref. 95) that the common cause failure beta factors for the PMS were reviewed and judged to be applicable to the AP1000 PMS. This was based on similarity of the design and application of the same modules. For example, the Ringhals reactor protection system and the AP1000 PMS use of the same ABB Advant Controller 160 platform.

213. Westinghouse also explained that the common cause failure beta factors were originally developed for the Ringhals reactor protection system using the widely accepted methodology presented in the international standard IEC 61508-6 (Annex D) (Ref. 106). Westinghouse also provided the beta factor categories used and the table of factors derived to determine the beta factors.

214. The GDA PSA resolution plans were to develop the PSA to the ASME PSA standard "capability category II" requirements. The PSA standards do not normally recommend the beta factor method for calculating common cause failure data for capability category II PSAs. However, it is considered acceptable in cases where the data is not available for other methods, such as the alpha factor. On balance I judge that the IEC standard beta factor approach is suitable in this case due to the pre-operational status of the design at GDA stage. However, a more appropriate common cause failure methodology should be used for the PMS within the licensing phase when a full capability category III PSA is needed. The GDA Step 4 PSA report raises assessment finding AF-AP1000-PSA-042 which requires a revised common cause failure analysis to be done. I am raising the use of a common cause failure methodology for the PSA as a technical item which can be resolved together with AF-AP1000-PSA-042[‡‡‡‡‡‡].

> **Technical item 42-2 for resolution with Step 4 AF-AP1000-PSA01-042:** The licensee shall use a common cause failure methodology which is suitable for a capability category III PSA during the licensing phase.

215. The categories described by Westinghouse correspond to those normally associated with beta factor methods: separation, segregation, redundancy, diversity, complexity, degree of analysis undertaken, the human interface and safety culture, environmental control and testing. The beta factors derived by Westinghouse for various classes of PMS component are of the order 1% or 2% (Ref. 95). In my experience these small beta factors imply very good defences against common cause failure which require robust justification. The C&I inspector agrees with this view and expressed concerns regarding the use of a read across analysis to justify very small beta factors, rather than a detailed AP1000 plant specific analysis.

[‡‡‡‡‡‡] *AF-AP1000-PSA-042. The Licensee shall provide revised CCF probabilities properly justified and documented.*

216. To investigate the risk significance of this I requested Westinghouse provide a PSA sensitivity study for the PMS C&I beta factor hardware analysis. This sensitivity study was to assume that a beta factor of x5 and x10 applies to all the beta factors together. The results of this sensitivity study are presented by Westinghouse in Ref. 95 (attachment 4). It states that increasing the PMS hardware beta factors by a factor of 5 (to approximately 0.1) increases the core damage frequency by a factor of 6. Increasing the PMS hardware beta factors by a factor of 10 (to approximately 0.2) increases the core damage frequency by a factor of 10. The large release frequency follows a similar trend. For the sensitivity study using beta factors of 0.2 the core damage frequency and large release frequency just exceed the ONR target 8 and target 9 BSOs.

217. The sensitivity study shows that core damage frequency and large release frequency is sensitive to the PMS common cause failure beta factors, and therefore will be sensitive to the defences against this within the engineering design. I do not necessarily expect that an AP1000 plant specific analysis would reveal sensitivities of the order used by Westinghouse in its sensitivity study. However, beta factors of 0.1 and 0.2 are not unexpected unless design specific consideration is applied to reduce them.

218. I consider that plant design differences could develop between the AP1000 design and the Ringhals plant during the licensing phase when detailed design will be done. For example, the layout of modules and power supplies, and the maintenance and inspection procedures used. Together with the C&I inspector we decided that an AP1000 plant specific PMS hardware common cause failure analysis is needed during the licensing phase. This is being addressed within the control and instrumentation inspector's assessment report for GDA issue GI-AP1000-CI-08 (Ref. 86). The topic of this GDA issue is the adequacy of the safety case for the PMS. There is no need for me to raise any findings on this topic in this report other than to record the need to update the PSA once the appropriate PMS common cause failure analysis is complete. The technical item below can be resolved together with Step 4 assessment finding AF-AP1000-PSA-042.

> **Technical item 42-3 for resolution with Step 4 AF-AP1000-PSA01-042:** The licensee shall update the PSA with the AP1000 plant specific PMS hardware common cause failure information when it becomes available.

4.7.22 Reliability of the DAS (Redundancy of the Solenoid Controls)

219. My assessment of the DAS identified a design feature that meant the same DAS solenoid is used to control redundant passive core cooling equipment trains. This may have been a logic error or mis-labelling in which the inputs to the Channel B signal in DAS are assigned with Channel A, and whether this might have any potential impacts on the risk model. I requested Westinghouse to clarify this using RQ-AP1000-1733 (comment 8: Ref. 63). Westinghouse responded that there is no error or mis-labelling and that in some cases the same DAS solenoid controls redundant passive core cooling system equipment trains.

220. This represents a single point of failure within the DAS. This does not necessarily contravene ONR SAP EDR.4 (single failure criterion) as this applies to failure of a safety function rather than a safety system. However, it does represent a limitation in the reliability of the DAS to support the PMS. The adequacy of the safety case for the DAS is addressed in GDA issues GI-AP1000-CI-01 and GI-AP1000-CI-02 (Ref. 64). This report covers the redesign of the DAS for the UK AP1000 plant. It is not necessary to raise any findings in this report.

4.7.23 Quantification of the Reliability of the Safety Measures in the Safety Case

221. My assessment of the systems analysis observes that the reliability on demand of the safety systems claimed is not presented in the PSA or in the PCSR (Ref. 32). The core damage frequency and large release fault trees generated for the PSA are not evaluated at intermediate positions to provide this information. It is my expectation that the safety case and the PSA would present this information for the system engineering to demonstrate consistency with ONR SAP ECS.2 (safety classification of SSC) and ONR TAG003 Safety Systems: Section 5.4 Table (Ref. 33).

Table 2: Section 5.4 of TAG003 (Safety Systems)

System Class	Probability of failure on demand (pfd)
Class 1	$10^{-3} \geq pfd \geq 10^{-5}$
Class 2	$10^{-2} \geq pfd > 10^{-3}$
Class 3	$10^{-1} \geq pfd > 10^{-2}$

222. I therefore requested that a sample selection of “end-to-end” probabilities of failure on demand (pfd) for the various safety functions and safety systems be presented. This is to provide evidence that the systems are adequately reliable with respect to their classification and to present numerical evidence to support the mechanical, electrical and C&I engineering justifications of the safety functions and safety systems for the plant (RQ-AP1000-1663: Ref. 34 and RQ-AP1000-1741: Ref. 35). These requests concentrated on the reliability of automatic and/or manual actuation of reactor trip, passive residual heat removal, passive containment cooling, primary circuit depressurisation, passive recirculation, in-containment reactor water storage tank injection, RNS injection and containment isolation.

223. Westinghouse provided its response in Ref. 38 and a number of meeting clarifications (Refs 109 and Ref. 110) in which the failure probability of the respective safety functions is presented. This was supplemented by technical support contractor independent review (Ref. 111).

224. The majority of the probabilities of failure on demand for the system hardware are within the range expected for class 1 and class 2 systems when actuated by PMS or DAS respectively. However, a number of the sample reliabilities merit further discussion.

225. One of the sample, that for PMS actuation of CMT injection for a large LOCA, is within the expected range of reliabilities for a class 2 system rather than a class 1 system. This is due to dependence on the PMS tripping all of the RCP pumps in order for CMT injection to be successful. I note that this safety function is backed by DAS actuation.

226. One of the sample, that for DAS actuation of containment isolation on high containment temperature is within the expected range of reliabilities for a class 3 system rather than a class 2 system. This may be due to the PSA modelling for the DAS representing the US design rather than the improved UK design.

227. One of the sample, that for RNS injection via manual PLS actuation is within the expected range of reliabilities for a class 3 system rather than a class 2 system.

228. I consider the sample of reliability analysis for the PMS, DAS and PLS actuation of safety systems claimed in the PSA presents an adequate demonstration that the ONR guidance for safety systems in TAG003 is largely met. This is adequate for GDA. However, a modestly sized sample has revealed one example of a PMS, DAS and

PLS actuated safety function that is not consistent with ONR guidance. This does not compromise the PSA demonstrating that the core damage frequency and large release frequency is small and meets relevant targets. However, there may be some inconsistencies in the assessed reliability of the safety systems claimed in the safety case and PSA, and their classification. I consider it appropriate to identify those that display a shortfall in reliability, and to undertake an ALARP analysis to justify improvements to system reliability. I have assigned this issue as an assessment finding and I am content that this shortfall can be resolved during licensing.

> **Assessment Finding (CP-AF-AP1000-PSA01-11):** The licensee shall assess during detailed design the reliability of the safety functions/safety systems claimed in the safety case and PSA. Confirmation shall be provided that the reliability for each meets the expectations with respect to the categorisation and classification system.

4.8 Low Power and Shutdown PSA

229. The resolution plan defined the scope of work for the low power and shutdown PSA. This was for Westinghouse to provide a “limited scope success path analysis” for the AP1000 Low Power and Shutdown (LPSD) PSA (Ref. 29). The limited scope analysis was to carry out new MAAP analysis to explore whether using the AP600 plant success criteria analysis previously submitted was acceptable for the AP1000 plant success criteria analysis. The intention was for the new MAAP analysis to address concerns about the applicability of the AP600 plant results to the higher powered AP1000 plant design.

230. The work presented by Westinghouse discusses the plant operational states (POS) and the event tree models used, and presents a series of new MAAP analyses (Ref. 29). The main conclusions presented by Westinghouse are that the new MAAP analyses justifies the success sequences in the existing AP600 plant event tree models; but that, as in the full power analysis, the passive containment cooling system is required for long term containment cooling, unless the Normal Residual Heat Removal System (RNS) is restored. Westinghouse argues that this requirement for passive containment cooling system operation is not significant (Ref. 29). This is discussed further in the next sub-section.

231. I identified the following topics for further discussion with Westinghouse and these are presented in RQ-AP1000-1657 (Ref. 41):

- the differences in the timing of events between the AP1000 plant analysis and the AP600 plant analysis and the potential impact this would have on human error probabilities;
- the significance of the requirement for the passive containment cooling system to be available for long term containment cooling;
- the impact of needing passive containment cooling on the plant operating state definitions;
- the absence of updates to the low power and shutdown PSA CAFTA model;
- the significance of the MAAP prediction that core can become uncovered.

232. My assessment has identified a number of residual technical items arising which are discussed immediately below.

4.8.1 Impact of Timings on Low Power and Shutdown Human Error Probabilities

233. The higher decay heat for the AP1000 plant may give rise to the reactor and containment conditions changing more quickly than for the lower power AP600 plant design. This may result in shorter times for operator actions. I explored this with Westinghouse in RQ-AP1000-1657 (comments 12 and 18 Annex A: Ref. 41) to clarify the insights from the new MAAP analyses.

234. The response from Westinghouse (Ref. 42) states that it had carried out a review of the AP1000 Step 4 PSA submitted for GDA Step 4 (Ref. 116). This review considered the impact of shorter operator response times for the AP1000 plant. Westinghouse provided some high level details, for example, it is stated that the "shorter times in the estimate were conservative as they equated hot leg drained to core damage" and that "during shutdown most operator actions have significant time available". However, these statements are not quantitative or extensive, and no comparison of the times available from the two separate success criteria analysis were presented.

235. I do not consider that a sufficient level of detail of the differences in timings has been presented, and therefore I do not have adequate confidence that the AP600 plant prediction of risk for low power and shutdown is valid for the AP1000 plant. The Step 4 GDA assessment finding AF-AP1000-PSA-050[§§§§§§] has captured the requirement to develop a full scope LPSD PSA. I have raised this as a technical item that can be resolved together with the Step 4 assessment finding.

> **Technical item 50-1 for resolution with Step 4 AF-AP1000-PSA01-050:** The licensee shall undertake AP1000 plant specific success criteria analysis for the low power and shutdown PSA. This shall ensure that a full and comprehensive analysis of human error probabilities and recoveries is included.

4.8.2 Additional Requirement for PCS Long Term Containment Cooling During Shutdown

236. Passive containment cooling is needed to provide long term cooling should the decay heat be above approximately 6 MW (thermal). Below this decay heat air cooling can be used to remove decay heat from the external surface of the containment. The need for passive containment cooling to remove decay heat in the shutdown plant operating states is not as extensive in the AP600 plant analysis, but this has currently been applied by Westinghouse for the AP1000 plant PSA.

237. I raised a number of questions requesting Westinghouse to clarify the importance of this item for the AP1000 plant shutdown PSA. I also requested Westinghouse to provide a sensitivity analysis to understand the risk significance (RQ-AP1000-1657 comments 13 and 18: Ref. 41). Westinghouse provided arguments that the inclusion of passive containment cooling more extensively in the AP1000 risk model would only increase the core damage frequency by 0.5% (Ref. 112).

238. This sensitivity value was generated by Westinghouse using the fault tree model for passive containment cooling in the internal events at-power PSA. I agreed that this is a reasonable way to generate an estimated impact of the model change. However, to explore this item further I requested my TSC to perform an independent sensitivity study (Ref. 100). This sensitivity study is based on quantification of the passive containment cooling fault tree (PCS-1-PX-DX) which is used in fault sequence 2 of the long term cooling event tree from the internal events at-power risk model. The minimal cutsets generated by a standalone quantification of PCS-1-PX-DX fall into the following three groups:

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

- Cutsets which contain the loss of offsite power initiating event (%LOOP);
- Cutsets which contain the medium voltage AC power initiating event (%MVAC);
- Cutsets for all other initiating events.

239. The sensitivity study estimated the conditional core damage probability for these three groups of cutsets, applied the initiating event frequencies, applied a 7% plant availability factor for shutdown operations to derive a core damage frequency of 1.2×10^{-9}/year. This represents a 1% increase in core damage frequency which is a little higher than Westinghouse's estimate. However, the fault tree gate for the reliability of passive containment cooling (PCS-1-PX-DX) assumes that PMS signals for automatic passive core cooling actuation will be generated, but this may not be the case for some shutdown plant operating states, particularly if the containment is open[*******]. My sensitivity study therefore assumes a probability of 10^{-2} that the containment is not isolated, or that manual actuation of passive containment cooling fails. The resulting core damage frequency is 2×10^{-9}/year. This represents 2% of the core damage frequency presented for the GDA Step 4 low power and shutdown PSA (Ref. 101). This is a small increase but nevertheless illustrates the need to adequately represent the need for passive containment cooling in the shutdown plant operating states.

240. The GDA Step 4 assessment finding AF-AP1000-PSA-050[†††††††] has captured the requirement to develop a full scope LPSD PSA. I have assigned this as a technical item for resolution together with the Step 4 assessment finding.

> **Technical item 50-2 for resolution with Step 4 AF-AP1000-PSA01-050:** The licensee shall update the PSA with AP1000 plant specific MAAP analysis for passive containment cooling in the low power and shutdown plant operating states.

4.8.3 Core Uncovery in Shutdown Plant Operational States

241. The MAAP5 analysis carried out for the low power and shutdown PSA predicted that temporary core uncovery would occur for some fault sequences. The core was predicted to recover again after the actuation of the ADS4 valves to depressurise the reactor coolant circuit and permit IRWST gravity injection.

242. I raised RQ-AP1000-1657 (comment 17: Ref. 41) to explore whether this phenomena was associated with automatic or operator actuations and to understand the timing of the events. I consider that temporary core uncover should be questioned if it is automatic actuations which provide the mitigation. I also requested Westinghouse to comment on what it is was doing to avoid the prediction of core uncover to demonstrate that risk is ALARP.

243. Westinghouse stated that 1) the analyses assumed bounding plant conditions suggesting that for other shutdown conditions uncovery would probably not be predicted, and 2) a time delay is modelled within MAAP for IRWST injection (Ref. 42), this being related to the time needed to evacuate floodable containment areas. Westinghouse also stated that the MAAP5 predictions of core uncover have been sent to its design and procedures group to investigate whether the conditions for core uncovery are realistic under actual outage conditions and to determine whether procedure changes could be made to actuate ADS4 depressurisation sooner in the fault sequences.

[*******] *If the containment is open a high containment pressure signal could not be generated.*
[†††††††] *AF-AP1000-PSA-050: The Licensee shall provide a full scope, modern and well documented Low Power and Shutdown PSA specific for the AP1000.*

244. I do not expect the core damage frequency to be sensitive to this item as core uncover is predicted to be temporary and it is reflooded before the fuel temperatures rise sufficiently to result in thermal damage to the fuel. The GDA Step 4 assessment finding AF-AP1000-PSA-050 has captured the requirement to develop a full scope LPSD PSA. I have therefore assigned this item as a technical item to be resolved together with the AF-AP1000-PSA-050 during licensing.

> **Technical item 50-3 for resolution with AF-AP1000-PSA01-050:** The licensee shall carry out further analysis to:
>
> 1) identify more precisely the shutdown conditions/plant operating states that may be vulnerable to temporary core uncover, and
>
> 2) investigation and possibly implementation of design or procedure changes to reduce or eliminate the possibility of core uncovery during shutdown fault sequences.

4.9 Dominant Contributors to Risk and Single Point Failures in the PSA

245. My assessment of the dominant Minimal Cutsets (MCS) for the internal events at-power PSA shows that there is one single order MCS (RPV failure) which results in core damage and two failure events which if they occur together with in initiating event result in core damage (Ref. 18). They are:

- Failure of the RPV.
- A LOCA followed by debris from the containment blocking the containment sump screens or the IRWST screens which fails long term passive and active recirculation. Debris can also enter the RPV and restrict coolant flow to the fuel elements.
- A LOCA followed by leakage from the IRWST which prevents adequate gravity injection and therefore prevents adequate passive recirculation.

246. The dominant minimal cutsets also include common cause failure of the PMS which requires operator action to initiate the safety systems that would otherwise have been initiated by the PMS. The dominant fault sequences are LOCAs for which the PMS would normally initiate the passive safety systems. I have assessed the reliability of the PMS and the associated operator actions within the section of this report that addresses the systems analysis and operator modelling (Section 4.7.15).

4.9.1 RPV failure

247. RPV failure is a single point failure that prevents all decay heat removal safety functions from being effective. This is dealt with by providing an RPV which is designed to satisfy “incredibility of failure” principles. This aspect of RPV integrity is discussed in SAP paragraph 291 (Ref. 3) where it is noted that an RPV must have a very low frequency of gross failure. However, such low frequencies cannot be demonstrated to sufficient levels of confidence using actuarial statistics or theoretical modelling. Instead the approach is one of sound engineering practice that gives a high level of confidence in the ability of the vessel to deliver its safety functions throughout its life (SAPs EMC.1 to EMC.34). These SAPs are not demonstrated within the PSA but in the structural integrity safety case for the RPV. I assume here that an adequate structural integrity justification for the RPV implies a very small failure frequency sufficient to conclude that this single failure is not risk significant for the AP1000 design.

4.9.2 Blockage of containment sump screens or the IRWST screens

248. The safety claims for the AP1000 plant are dependent upon reliable operation of the passive core cooling system, this system relies on natural convection flow of water from the containment sump to the reactor core to remove decay heat. The containment sump screens prevent debris entering the primary circuit, however, if they block they could prevent cooling water being circulated. Two containment recirculation screens and three IRWST screens are installed on the AP1000 plant.

249. The USNRC has recognised the potential for debris to block long term cooling recirculation systems in the current fleet of US PWRs and BWRs. It therefore opened Generic Safety Issue GSI-191 (Ref. 125) in 1996 which was followed by USNRC Generic Letter 2004-02 (Ref. 126) which required all PWR licensees to reassess their design basis for long term core cooling using an acceptable methodology for assessing debris blockage, and make necessary modifications to provide reasonable assurance that long term core cooling can be maintained for design basis accidents.

250. NUREG-1793 (Ref. 127) is the USNRC regulatory assessment of the AP1000 plant, and includes an evaluation of the debris blockage issue. The document addresses a comprehensive list of technical areas relevant to in-core, sump screen and IRWST screen blockage. The USNRC concludes from NUREG-1793 that its regulatory requirements for long term cooling for design basis accidents have been adequately met, and the issue is closed for the AP1000 design. This conclusion is based on the cleanliness requirements specified in the safety analysis being met when the reactor enters operations.

251. I have assessed NUREG-1793 (Ref. 127) and consider it to be comprehensive and detailed in its review and its summary of analytical and experimental evidence to support its conclusions (Ref. 128). NUREG-1793 refers to various supporting analysis, and the AP1000 PSA refers to a number of documents which support the claims made in the PSA, that debris blockage effects are very unlikely for any AP1000 plant initiating event. I have also assessed these documents and judge that the analysis is based on reference to an extensive body of evidence on debris blockage, and take confidence from the formal expert panel review undertaken by Westinghouse upon which the AP1000 PSA data is based.

252. The AP1000 plant specific work presented by Westinghouse in the PSA for debris blockage is not accompanied by a formal ALARP justification. However, it is apparent from the documents I have reviewed that an options review and design change process has been used, and this process is based on extensive AP1000 plant specific safety analysis supported by experimental evidence (Ref. 128). Examples of the design features for the AP1000 plant which minimise the potential for debris to block the long term cooling injection and recirculation flow paths include:

- Metal Reflective Insulation (MRI) which produces less debris than traditional materials is used for the AP1000 plant for primary circuit components which may be subject to jet impingement following a LOCA.
- Other sources of fibrous debris that might be generated post-LOCA are located outside the zone of influence of a LOCA jet.
- The sump screens and IRWST screens use large surface areas, and recirculation velocities are low because of natural circulation flows thereby minimising the potential for debris to transport to the screens.
- Materials that might corrode and produce large quantities of chemical precipitates have been reduced relative to earlier designs.

- The containment recirculation screens are orientated vertically and have protective plates located above and to the side of the screens with debris curbs along the floor. These prevent debris reaching the screens.

- Extensive testing has been used to demonstrate that debris is very unlikely to block in-core flow paths.

- Westinghouse has proposed a cleanliness program to limit debris in containment which is derived from both analysis and testing.

253. I am able to conclude that the AP1000 design is less susceptible to debris-induced failure of long term cooling relative to existing PWR designs, and the pursuit of additional design improvements is not required.

254. The data used in the PSA claims that the likelihood of blockage of flow paths from debris is very small and therefore makes a very small contribution to the core damage frequency. However, it should be noted that this is a generic issue with any PWR design and my judgement is that it is unlikely to lead to any design change on the AP1000.

4.9.3 IRWST External Leakage When in Standby

255. The IRWST provides the water mass for the closed circuit PRHR heat sink for intact circuit faults, and also the water mass for gravity injection into the RPV to maintain the water inventory in the core after depressurisation from a LOCA event. Following a LOCA or depressurisation through the ADS 4 valves the IRWST water makes its way through the core then out of the break or ADS Valves to the containment sump to support passive recirculation. In the absence of an adequate water inventory in the IRWST due to failure modes which result in external leakage from the tank, the PSA is unable to demonstrate that the core is protected for many LOCAs. The PSA therefore claims a very high reliability for the IRWST when in standby to maintain its integrity in the event of a LOCA.

256. The IRWST operates at atmospheric pressure when in standby reducing the likelihood of external leakage. A significant leak in the IRWST when in standby will be highlighted to the operators by appropriate level alarms. The technical specifications will state whether a shutdown is required. The integrity of this boundary is supported by the engineering standards that will be applied to its construction and operation resulting from its designation as a Class 1 SSC (SAP ECS.2). I consider that a small probability of failure on demand is justified for the IRWST when in standby, and not subject to any internal hazards. This enables me to conclude that the single failure of tank and cooler interface when in standby is not risk significant for the AP1000 design.

4.9.4 IRWST External Leakage When Subject to Pipe Whip

257. Westinghouse convened an expert panel to undertake the structural integrity classification of the AP1000 plant to meet UK expectations. This panel could not rule out the potential for damage to the IRWST as a result of a pipe whip from a double ended guillotine break of the PRHR heat exchanger return line (Ref. 133). If fracture of the PRHR heat exchanger return line is postulated, the whipping pipe subjects the mounting ring welds at the end of the pipe to structural loading. The mounting rings are situated at the outlet plenum to the IRWST and failure of the mounting ring welds provides a route to drain the IRWST. In the absence of adequate IRWST injection a PRHR return line failure results in core damage.

258. Westinghouse initiated a study to assess the consequences for the integrity of the mounting ring welds and concluded that the component is adequately safe. However, the ONR structural integrity inspector judges that the margins demonstrated by

Westinghouse with respect to ASME requirements required additional substantiation, as discussed within the SI-01 close-out report (Ref. 138: Assessment Finding CP-AF-AP1000-SI-02). The PSA does not include this failure mode of the IRWST so I requested Westinghouse to clarify the risk implications and consequences of IRWST failure due to pipe whip of the PRHR return line in RQ-AP1000-1679 (Ref. 130).

4.9.5 Risk Implications of IRWST Failure due to Pipe Whip

259. RQ-AP1000-1679 was presented to obtain clarity from Westinghouse on the potential impacts of a PRHR heat exchanger line break, specifically:

> 1) The leak rate from the IRWST mounting ring welds that would enable plant protection to be claimed.
>
> 2) Where the IRWST water would accumulate and would this be available to support delayed passive recirculation.
>
> 3) Whether there is any safety equipment in the vicinity of the PRHR heat exchanger line break that is needed to protect against the fault that would be made unavailable by the pipe whip. For example the ADS Stage 1, 2 & 3 valve cabling which are in the same compartment as the IRWST heat exchanger lines. A risk sensitivity study assuming this equipment is failed by pipe whip.

260. For item 1) Westinghouse in its reply (Ref. 131) states that there is conceptually a leak rate where IRWST gravity injection is maintained for an adequate period of time following a PRHR line break. However, this leak rate has not been estimated due to uncertainties in the pipe whip/mounting ring failure modes.

261. I have undertaken a bounding risks sensitivity study assuming that a PRHR heat exchanger line gross failure always results in excessive leakage from the IRWST. The core damage frequency is the initiating event frequency of $1x10^{-6}$/year which compares with the ONR BSO for target 8 of 10^{-6}/year. I would expect the likelihood of IRWST leakage to be significantly less than 1.0 due to the margins in the structural analysis demonstrated by Westinghouse.

262. For item 2) Westinghouse states that water leakage from the IRWST would be into compartments that are part of the containment flood-up volume. Therefore the water would be available for passive recirculation. However, passive recirculation would occur without this water having been through the core. The plant performance analysis to examine whether core protection can be claimed for passive recirculation in these circumstances has not been carried out.

263. For item 3) it was confirmed by Westinghouse that the electrical conduit and junction boxes for one bank of the ADS1, 2 and 3 valves are located in the same area as the PRHR heat exchanger pipework. This equipment could be damaged by gross failure of the PRHR heat exchanger line.

264. However, Westinghouse states that gross failure of a PRHR heat exchanger line does not require depressurisation from both banks of ADS1, 2 and 3 valves and these are not critical for mitigation of the event. The second group of ADS 1/2/3 valves is located in another room and is unaffected by the PRHR heat exchanger line failure. In addition the critical success criterion for this event is depressurisation using the ADS 4 valves, which are not within the proximity of the postulated PRHR failure event and will remain unaffected.

265. With IRWST water available but with on one bank of ADS1, 2 and 3 valves unavailable the sensitivity presented by Westinghouse shows that the core damage frequency increases by a factor of 10. However, the overall risk remains very small and within

ONR BSO for target 8 due to the small initiating event frequency and the availability of IRWST gravity injection in this case.

266. My exploration of the PSA clarifies that the consequences of a PRHR heat exchanger line break cannot discount core damage if pipe whip causes failure of the heat exchanger mounting ring weld, and this results in leakage of water from the IRWST. I consider that preventing core damage, mitigating a single failure mode in the PSA (SAP EDR.4) and achieving risks that are ALARP is highly dependent upon the integrity of the mounting ring weld.

267. I have provided this risk information to ONR's structural integrity inspector to support his judgements reported within his GI-AP1000-SI-01 assessment report (Ref.138).

4.9.6 Mechanical and Structural Success Criteria for the ADS4 Valves

268. The fourth stage of the automatic depressurisation system (ADS) consists of four normally closed squib valves, two on each loop of the reactor coolant system hot legs. The ADS4 squib valves are designed to open after the ADS 1 to 3 valves to complete the depressurisation of the primary circuit to near the containment pressure. This permits gravity driven injection of the IRWST water into the RPV to maintain water inventory and remove decay heat.

269. The spurious actuation of one or more ADS4 valves at normal operating pressure is a credible although beyond design basis fault. However, the pipework between the ADS4 valves and the reactor coolant system was not designed for the loads that would occur if the ADS4 valves opened spuriously at full RCS pressure. This creates uncertainty regarding the structural integrity of the high pressure pipe work.

270. There are two potential consequences of this:

> 1) The ADS4 valve pipework could deform as it moves closing off the pressure relief path necessary to depressurise the primary circuit and permit IRWST gravity injection to occur. Core protection following a spurious ADS4 actuation is justified within the PSA providing an adequate pressure relief path is available.
>
> 2) The ADS4 pipework could whip or the high pressure water jet could damage other safety equipment in the vicinity which is needed to protect the fault.

271. The PSA models one or more ADS4 valves spuriously actuating but the success criteria assume that the two potential consequences above do not occur. The ONR structural integrity and mechanical engineering inspectors pursued their respective deterministic justifications regarding the justification of the pipework. I raised the potential consequences and risk implications with Westinghouse in RQ-AP1000-1589 (Ref. 89) and RQ-AP1000-1715 (Ref. 92). These RQs request that Westinghouse clarify the consequences and risk sensitivity for the two potential consequences presented above.

272. Westinghouse convened an expert panel meeting to explore the best estimate consequences of spurious ADS4 actuation. The expert panel claims that there would be a 30^{o} displacement of the ADS4 valves and pipework following their spurious actuation. The pipework would not crimp to any significant extent and the depressurisation function of the valves would be preserved.

273. The expert panel also identified other safety equipment within a 3.3m (10ft) zone of influence of the ADS4 valves that may not survive due to pipe whip impact or high pressure jet effects (Ref. 135). This equipment is one of the two Core Make-Up Tank

lines to the primary circuit. Westinghouse presented its responses to RQ-AP1000-1715 in Refs 97 and 98.

274. Westinghouse argues that loss of the water volume from one CMT would not compromise the success criteria because there is a second CMT available and also the water volumes from the two accumulators is available. The surge line is in one of the ADS4 compartments and Westinghouse considered it for completeness even though it would not be damaged by movement of the ADS4 valves. Westinghouse also argued that failure of the pressuriser surge line does not compromise the success criteria because water from the pressuriser does not normally reach the core during depressurisation. This is because its water is entrained within the ADS4 flow which is out of the primary circuit and into the containment sump. Failure of both the CMT line and the pressuriser surge line will assist the depressurisation. The risk sensitivity study presented by Westinghouse shows that the core damage frequency increases by 1% and is insensitive to the loss of redundancy if only one CMT is available (Ref. 98).

The ONR structural integrity inspector has assessed the claims by Westinghouse that the pipework deflection is limited to 30^{o} and that the pressure relief path will remain available following spurious ADS4 actuation at full pressure. The conclusions of this assessment supports the claims made by Westinghouse (Ref. 102).

I consider that the beyond design basis risk implications of spurious actuation of the ADS4 squib valves has been adequately explored. A success path has been demonstrated by Westinghouse. However, the potential for loss of one CMT line should be included in the PSA. The sensitivity to risk from this missing failure mode is small. I have assigned this issue as an assessment finding because it is associated with the comprehensiveness of the PSA. This assessment finding is grouped together with another in Section 4.9.7 below which together address the modelling of spurious squib valve initiating events.

4.9.7 Mechanical and Structural Success Criteria for the IRWST Injection Lines

275. The IRWST provides a large volume of water for gravity injection into the RPV in the event of a LOCA. Gravity injection is initiated by the opening of the IRWST squib valves which are between the IRWST and the RPV. Included in each of the four injection lines is a non-return valve between the squib valve and the IRWST. These non-return valves are to stop flow from the high pressure primary circuit to the low pressure IRWST in the event that one or more squib valves spuriously open. There is a 2mm (1/8”) hole in each non-return valve for pressure balancing. Therefore spurious opening of one or more IRWST squib valves, followed by closure of the non-return valves will prevent a large LOCA, but will give rise to an RCS leak into the IRWST. This RCS leak is protected using the passive safety systems by depressurising the plant, at which point the non-return valves will then open permitting IRWST gravity injection into the RPV.

276. The expert panel considered the performance of the non-return valves for this fault sequence and concluded that the non-return valves would experiencing a beyond design basis loading when closing under full primary circuit pressure. The expert panel concluded that the non-return valves could seize closed and fail to open when RCS pressure drops later in the accident progression (Ref. 135). The success criteria for protecting a RCS leak is one out of four IRWST injection lines open to permit gravity injection. Hence it is the spurious actuation of all four IRWST squib valves that is of concern.

277. The PSA currently does not include the failure mode for the non-return valves failing to open and is therefore potentially optimistic. However, if all four IRWST injection lines are unavailable, an alternative success path is available which is low pressure injection using the RNS taking its water from the IRWST. The expert panel also noted that the

IRWST squib valves are located in the vicinity of the RNS pipework that takes its suction from the IRWST. ONR requested that Westinghouse considers whether pipe whip or water hammer effects from squib valve spurious actuation could damage the RNS suction pipework rendering the RNS success path unavailable (RQ-AP1000-1715 Ref. 92).

278. To address the dependency Westinghouse presented structural integrity arguments claiming that the IRWST squib valve pipework would not move sufficiently to damage the RNS pipework. Westinghouse confirmed through a response to RQ-AP1000-1731 (Ref. 136) that the RNS pipework in the vicinity of the IRWST squib valves and non-return valves remains intact after a spurious actuation of the IRWST squib valves. ONR structural integrity inspector has assessed this claim by Westinghouse and agrees with its conclusion (Ref.102).

279. Westinghouse also carried out a risk sensitivity study which considered the non-return valves as failed following a spurious IRWST squib valve(s) actuation. The sensitivity analysis showed that the increase in core damage frequency due to the additional non-return valve failure mode small at 1%.

280. I consider that Westinghouse has demonstrated that the spurious actuation of the IRWST squib valves(s) followed by failure of the non-return valves to open has a valid success path using RNS injection from the IRWST. The risk sensitivity to the additional non-return valve failure mode is small. I have assigned this issue as an assessment finding because it is associated with the comprehensiveness of the PSA.

> **Assessment Finding (CP-AF-AP1000-PSA01-12):** The licensee shall update the PSA to ensure that the initiating events of spurious squib valve actuation are appropriately modelled. In particular the following consequential events should be included: 1) the loss of one of the two CMT lines for the spurious ADS4 initiating events, and 2) the failure mode of the non-return valves failing to open following spurious actuation of the IRWST squib valves.

4.10 Codes and Standards for UK Class 2 and Class 3 Systems

281. The ONR structural integrity inspector raised RQ-AP1000-1779 to clarify the codes and standards proposed by Westinghouse for UK class 2 pressure equipment and storage tanks (Ref. 137). This structural integrity RQ is relevant to a number of other ONR technical disciplines. For example, mechanical, electrical and control & instrumentation engineering where the reliability on demand of the whole system is relevant for reactor safety. The RQ raises a number of areas in need of clarification to inform ONR's decision of what codes and standards are applicable to the UK class 2 (and class 3) SSC. To assist the resolution of this topic I have investigated the sensitivity to risk of the UK Class 2 and Class 3 SSC.

282. Westinghouse has presented a sensitivity study and importance information in the PSA to clarify the risk importance of the UK class 2 and class 3 SSC (Ref. 18: Tables 8.7-3 and 8.7-1). The first table shows that removal of all credit for the UK Class 2 and Class 3 SSC increases the core damage frequency by a large amount sufficient to exceed ONR target 8 BSO by a factor of one hundred. This is clearly an extreme case but it does illustrate the collective importance of these systems to achieving ONR policy for GDA - that the numerical target BSOs should be met subject to the application of the ALARP principle.

283. The second table shows that individual class 2 and class 3 SSC can have "system level" risk achievement worth values which range from approximately 10^1 to 10^3. The system level risk achievement worth represents the amount the core damage frequency would increase if no credit was taken for the individual system in the PSA. This demonstrates that the class 2 and class 3 SSC are individually risk sensitive.

284. The information presented in the PSA demonstrates that the justification of which codes and standards should apply to the UK class 2 and class 3 SSC should take into account the risk sensitivity of the SSC, both individually and collectively. The structural integrity inspector considers this item should be resolved post-GDA. I consider that the licensee should take into account the following factors when justifying the relevant codes and standards applicable to the UK class 2 and class 3 SSC:

- The risk importance of the SSC for their impact on the core damage frequency and large release frequency in both the normal and shutdown plant operating states.
- The SSC reliability claims within the PSA.
- The overall balance of safety offered by different SSC to demonstrate that the overall risk from the plant is reduced ALARP.

285. I have discussed this with the structural integrity and mechanical engineering inspectors for inclusion of this risk informed approach into the structural integrity inspectors assessment report (Ref. 138).

4.11 Design Change Proposals and Gap Analysis

286. The PSA documented by Westinghouse is based on the AP1000 plant design as agreed with myself at the start of the close-out phase. For the PSA this corresponds to the design as described in Revision 17 of the AP1000 plant DCD (Ref. 117) and on the most recent approved revisions of the SSDs and P&IDs as of 1 September 2010. The use of this Design Reference Point (DRP) for the PSA was based on a judgement that major changes to the design that would substantially influence the risk was not expected during the GDA close-out phase. To substantiate this judgement Westinghouse agreed to provide a qualitative analysis of the class 1 and class 2 design changes made after the internal events-at power PSA was developed to provide a comparison with the UK GDA design reference point.

287. This “gap” analysis presents a discussion of the methodology in Ref. 118 and a comprehensive listing of the design change proposals under the following headings in Ref. 119:

- The design change proposals that have occurred between the PSA freeze date and UK GDA design reference point.
- The design change proposals that were not incorporated at Step 4 but have since been incorporated into the PSA model for the close-out phase of GDA.
- The UK specific design change proposals that are not incorporated at this time but will be during the licensing phase.

288. I selected the following sample of the design change proposals for assessment, concentrating on those design change proposals originating between the PSA design freeze date and the present time. My criteria for selecting these from the extensive list of design change proposals are that 1) a large number of the 200 design change proposals were clearly of no impact to the PSA, 2) Westinghouse stated there was little or no impact on the PSA and I considered this needed further clarification, or 3) the description suggested a technical topic associated with the passive safety systems:

- Passive core cooling system screen flow limit changes for RNS injection to prevent ADS stage 4 actuation.
- Changes to incorporate passive core cooling system partially open check valves in IRWST injection & containment recirculation.

- Beyond design basis for squib valve actuation.
- CIM/ALS (PMS/DAS) diversity changes.
- AP1000 plant electrical package 4 design finalisation.
- AP1000 plant electrical package 5 design finalisation.
- AP1000 plant electrical package 6 design finalisation.
- AP1000 plant electrical package 7 design finalisation.
- AP1000 plant electrical package 8 design finalisation.
- AP1000 plant electrical package 9 design finalization.
- CCS vent line relocation and test connection label.
- Changes to address spurious actuation of the IRWST squib valves.
- ADS & IRWST injection blocking device logic change.

289. I requested further information from Westinghouse in Ref. 120. The further information presented by Westinghouse for this sample of design change proposals shows that the PSA is not impacted by most of them with up to a 10% increase in core damage frequency for two of them (Ref. 121). I am content that the gap analysis does not adversely affect my understanding of the overall risks from the internal events at-power PSA.

4.12 Development of a Living PSA and Risk Monitor

290. My report has identified a relatively large number of assessment findings and technical items. This arises because:

1) Westinghouse has chosen to present a new internal events at-power PSA to address GDA Issue GI-AP1000-PSA-01, and

2) the PSA is a very detailed and extensive analysis requiring an understanding of many different technical areas.

For this project I consider that the shortfalls identified need to be resolved by the licensee to ensure that the PSA is developed to be as realistic and comprehensive as practicable. This will support the development of a useful living PSA which is able to support design development during the licensing phase, and ultimately development into a risk monitor to support operational decision making (see GDA Step 4 AF-AP1000-PSA-051[‡‡‡‡‡‡‡]).

4.13 Discussion of the AP1000 Plant Risks

291. The core damage frequency can be compared with ONR SAP numerical target 8, and the large release frequency can be compared with ONR numerical target 9. However, as a radiological dose analysis was not required for GDA this comparison can be conservative. This is because the frequency with which a radiological dose would be received off-site would be lower than the core damage frequency due to the mitigating effects of containment. The frequency of 100 or more fatalities off-site can be lower

[‡‡‡‡‡‡‡] *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.*

than the large release frequency due to the effects of weather and site characteristics. However, based on the current claims by Westinghouse for the internal events at-power PSA, the core damage frequency of 1.7×10^{-7}/year and the large release frequency of 1.2×10^{-8}/year are well within the ONR SAP numerical targets 8 and 9 BSOs of 10^{-6}/year and 10^{-7}/year respectively. I include a table of the overall risks from the AP1000 reactor plant at GDA below to put these values in context.

Table 3: Overall AP1000 Plant Risks at GDA

ONR Numerical Target 8 Dose > 1000 mSv	Core Damage Frequency	ONR Numerical Target 9 ≥ 100 fatalities	Large Release Frequency
BSL 10^{-4}/year BSO 10^{-6}/year	9.4×10^{-7}/year	BSL 10^{-5}/year BSO 10^{-7}/year	6.8×10^{-8}/year
Contributors to the Overall Risks at GDA			
Internal fire at-power	6.7×10^{-7}/year	Internal fire at-power	5.6×10^{-8}/year
Internal events at-power	1.7×10^{-7}/year	Internal events at-power	1.2×10^{-8}/year
Internal events low power and shutdown#	1×10^{-7}/year	Internal events low power and shutdown#	Not reported
Internal flooding#	4.4×10^{-9}/year	Internal flooding#	1.2×10^{-9}/year

#: These are the risks applicable at GDA Step 4 for which an update was not required for the GDA close-out phase.

292. The table presents the overall risk from the AP1000 reactor plant given the information available within the PCSR (Ref. 32: Chapter 10). This includes internal events at-power, fire hazards at-power, internal flooding at-power and the contribution from internal events during low power and shutdown. Fire and flooding from low power and shutdown operations, spent fuel pool risks and the contribution from external hazards are not available at this time and will be developed during licensing.

293. The success sequences from the Level 1 PSA are expected to have high frequencies and may result in non-core damage releases from the fuel which could result in low doses which are relevant to ONR numerical target 8. The frequencies of these fault sequences has not been required during GDA and are not available for assessment against the relevant BSL and BSOs.

294. My assessment of the internal events at-power PSA has found that, on balance, it is generally adequate in the technical approach used and is consistent with the ONR TAG expectations. The internal events at-power PSA is a large and complex analysis and it is to be expected that my assessment has identified various shortfalls that need to be resolved as the PSA develops during the licensing phase. There are also a number of gaps identified by Westinghouse which are to be addressed during site licencing.

295. The following shortfalls for the internal events at-power PSA are considered to be those of more significance with respect to the impact on risks:

1) Including dependency between spurious actuation of the PMS and the safety systems needed to protect the fault.

2) Revising the likelihood of losing the offsite power supply following a fault to reflect the design of the UK grid system.

3) Reviewing the methodology and data used for the treatment of common cause failure in the PMS and mechanical equipment it actuates.

4) Including a number of the less significant initiating events. For example, common cause failure of electrical busses and loss of the ultimate heat sink when the site design is developed.

5) Review of the human error data for a number of risk significant operator tasks and including mis-calibration, test and maintenance operator errors.

6) Ensuring a more comprehensive treatment of containment bypass fault sequences.

7) Completing a more thorough treatment of the low power and shutdown PSA, and inclusion of the site specific hazards. This is programmed for completion during licensing.

296. The nature of the shortfalls suggests that a revised analysis would show the core damage frequency and large release frequency for internal events at-power are higher than those currently presented. Sensitivity studies have been undertaken during the project both by Westinghouse and myself and are discussed within the main report. My judgement is that the ONR SAP numerical target 8 and 9 BSOs may well be met for the internal events at-power PSA. This is because the current risks are a factor of 10 below the BSOs. However, it is not possible to accurately estimate the overall impact of these shortfalls without completing the technical work required.

297. A number of the technical areas in the internal events at-power PSA, for which shortfalls have been identified, may also have an impact on the fire PSA. This is because the fire PSA uses the internal events at-power risk model as its basis. When this is considered together with the shortfalls, gaps and inclusion of the site hazards, it is my judgement that the overall risk from the AP1000 design is likely to exceed the ONR SAP target 8 and 9 BSOs, but I consider the risk should be within the respective BSLs with a significant margin.

4.14 Assessment of the ALARP Position

298. The PSA is discussed by Westinghouse in the PCSR (Ref. 32: Chapter 10) in which the main use of the PSA is stated to be the demonstration of compliance with ONR numerical targets and the demonstration that the overall risks from planned operation of the reactor are as low as reasonably practicable. The discussion in the PCSR applies to the broader scope PSA and not just to the internal events at-power PSA. However, the internal events at-power PSA makes a contribution to the overall position stated by Westinghouse in the PCSR.

299. In the PCSR (Appendix 10A) Westinghouse describes how the basic design of the AP1000 plant, and its predecessor the AP600 plant, were reviewed by Westinghouse using insights from successive versions of the PSA to identify reasonably practicable design changes that would significantly reduce the risk from the plant. As a result of these reviews, Westinghouse states that a number of design improvements have been implemented to produce risks that are ALARP. With respect to the ONR SAP numerical targets, Westinghouse states in the PCSR that as the AP1000 plant design develops the PSA will continue to demonstrate that the ONR SAP numerical target

BSOs are met. Therefore Westinghouse considers there is little need to further reduce the AP1000 plant at-power risk.

300. ONR guidance states that the demonstration of ALARP requires the licensee to evaluate the risks and to consider whether it would be reasonably practicable to implement further safety measures beyond the initial proposals (Ref. 72 ALARP TAG para 5.3).

301. The information presented by Westinghouse shows that the overall risk from internal events at-power operations is small and falls within ONR's target 8 and 9 BSOs. I am able to judge that ONR SAP numerical targets 8 and 9 BSOs may well be met for the internal events at-power PSA when the assessment findings in my report are addressed. However, my judgement on the overall risks from the AP1000 reactor plant is that the BSOs may be exceeded, but this is mainly due to other hazards rather than internal events at-power.

302. I have taken this position into account in my assessment in addition to the guidance in the ONR SAPs (paragraph 701). This states that when risks are small inspectors need not seek further improvements from the designer but can confine themselves to assessing the validity of the arguments presented. I have done the latter within the detailed technical assessment of the internal events at-power PSA. However, the designer/duty holder is not expected to stop reducing risks at this level, but if it is reasonably practicable to provide a higher standard of safety, then the duty holder must do so by law.

303. The ONR SAPs are written in terms of legal duty holders and licensees. Within GDA I am considering Westinghouse as fulfilling the function of "duty holder" for the purpose of providing the ALARP analysis, although I note that the legal duty does not apply to GDA requesting parties.

304. In order to address the subject of ALARP further I have assessed the information presented by Westinghouse in its original submissions and its responses to RQs that are ALARP related. Within my assessment I have considered the ALARP position for the dominant contributors to risk, and used the PSA to risk inform other technical areas where design alternatives have been part of other inspectors considerations.

305. I have considered the following areas for their contribution to demonstrating that risks are ALARP:

1) The reliability of the PMS. PMS failure on demand is within the dominant minimal cutsets. My assessment has highlighted the importance of the PMS software and common cause failures of the PMS. The C&I inspector has considered this in assessing the QA expectations for developing the software consistent with its SSC classification. The C&I inspector has included assessment findings in his report which require a UK AP1000 plant specific PMS reliability analysis to be undertaken (including common cause failure), and for the PSA to be updated accordingly. A C&I assessment finding has been raised for an appropriate statistical testing programme to be carried out for the PMS software.

2) The reliability of the operator response. The main control room simulator trials do not currently support a number of operator responses claimed within the PSA. I have raised an assessment finding to review these against future improvements to the main control room simulator and to optimise operating procedures.

3) Spurious actuation of the ADS4 valves. Should the PMS be unavailable after a spurious actuation of 2 or more ADS4 valves, an operator response would be needed. However, the time available does not currently support this. I have raised

an assessment finding to investigate whether an extended operator response is acceptable, and the optimisation of operating procedures.

4) The reliability of the safety systems. I have raised an assessment finding to assess the reliability of the safety systems during detailed design to confirm that the expectations arising from categorisation and classification are met. If not, an ALARP analysis will be needed.

5) Debris blockage of recirculation screens. Highly reliable recirculation is important for the passive safety concept of the AP1000 plant. I have assessed the work supporting this and consider that further measures are not needed at GDA to support the ALARP justification.

6) Safe-arm device. I have assessed the risk benefits and detriments of fitting a safe-arm device to the ADS4 valves. My assessment advises that a safe-arm device is not needed to demonstrate that risks are ALARP.

7) PRHR heat exchanger mounting ring welds. My assessment has advised of the risk sensitivity should these welds fail and drain the IRWST following a PRHR heat exchanger pipework LOCA. The structural integrity inspector has raised an assessment finding to reduce the likelihood of this failure mode to ALARP.

8) Reliability of the DAS. I have advised the C&I inspector of the limitations in the reliability of the DAS due to common cause failures. This has been considered by the C&I inspector in his considerations of an improved UK design for the DAS.

9) The use of non-nuclear codes and standards for UK class2 and class 3 SSC. I have advised the structural integrity inspector of the risk importance of the class 2 and class 3 SSC. The structural integrity inspector has raised an assessment finding to ensure that the choice of codes and standards for these SSC reduces risk ALARP.

306. I have raised additional assessment findings which will support the justification and comprehensiveness of the PSA. This will improve the estimates of risk and the development of a living PSA to support design development during the licensing phase.

307. The PCSR (Ref. 32: Chapter 10A) shows that PSA has been used by Westinghouse during the process for developing the AP1000 reactor plant design from the AP600 reactor plant design. This has identified design features to reduce risks and establish the overall arrangement of the reactor plant and its safety systems. My assessment of the internal events at-power PSA has not found any major areas of the plant design for which ALARP analysis is needed to consider alternative features. This is supported by the small risks presented by Westinghouse. However, my assessment does support findings which have ALARP implications for the detailed design phase.

308. My report identifies findings which will enhance the ability of the PSA to provide insights into the risks, and when complete these will need to be reviewed by the licensee for any ALARP implications. I consider this to be normal regulatory business with the licensee to be pursued during licensing. My assessment has also informed other inspectors' findings with ALARP considerations, again these are to be resolved during licensing. My assessment supports the view that the risks from internal events at-power are being managed ALARP as the AP1000 design process continues through GDA and into the licensing phase.

4.15 Comparison with Standards, Guidance and Relevant Good Practice

309. In Section 2.2 I have listed the standards and criteria I have used during my assessment to judge whether the AP1000 plant internal events at-power PSA submission appropriately addresses the resolution plan, and has been carried out adequately with respect to modern standards.

310. I am able to concluded that the internal events at-power PSA has been carried out adequately with respect to these standards to enable a meaningful GDA assessment to be completed.

4.16 Overseas regulatory interface

311. ONR has formal information exchange agreements with a number of international nuclear safety regulators, and collaborates through the work of the International Atomic Energy Agency (IAEA) and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). This enables us to utilise overseas regulatory assessments of reactor technologies, where they are relevant to the UK. It also enables the sharing of regulatory assessment findings, which can expedite assessment and helps promote consistency.

312. ONR also represents the UK on the Multinational Design Evaluation Programme (MDEP), which is a group of nuclear safety regulators engaged in the technical review of reactor technologies. This helps to promote consistent assessment standards, and enables the sharing of information.

313. The USNRC has completed its design certification of the AP1000 plant. In this assessment, the following information from the USNRC has been used:

- Discussions with USNRC PSA specialist inspectors (Ref. 122). This meeting exchanged information of mutual interest on the AP1000 PSA.
- Technical reports from the USNRC website.
- Minutes of Multinational Design Evaluation Programme (MDEP) meetings undertaken by ONR inspectors.

4.17 Assessment findings

314. During my assessment 12 items are identified for a future licensee to take forward in its site-specific safety submissions. Details of these are contained in Annex 2.

315. These matters do not undermine the generic safety submission and are primarily concerned with the provision of site specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages. These items are captured as assessment findings.

316. Residual matters are recorded as assessment findings if one or more of the following apply:

- site specific information is required to resolve this matter;
- the way to resolve this matter depends on licensee design choices;
- the matter raised is related to operator specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters;
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

4.18 Minor shortfalls

317. During my assessment 4 items were identified as minor shortfalls in the safety case, but which are not considered serious enough to require specific action to be taken by the future licensee. Details of these are contained in Annex 3.

318. Residual matters are recorded as a minor shortfall if it does not:

- undermine ONR's confidence in the safety of the generic design;
- impair ONR's ability to understand the risks associated with the generic design;
- require design modifications;
- require further substantiation to be undertaken.

4.19 Technical Items to be Resolved with Step 4 Assessment Findings

319. My assessment has identified areas of technical work that I consider need resolving during the licensing phase, but are encompassed by earlier assessment findings presented in ONR's Step 4 PSA report (Ref. 11). I have called these areas of technical work 'technical items' to distinguish them from new assessment findings or minor shortfalls. They appear throughout my report as required and are also summarised in Annex 2 together with the associated Step 4 assessment finding. These technical items arise from the new work submitted by Westinghouse to address GI-AP1000-PSA-01. They are raised to ensure that the resolution of the Step 4 assessment findings includes an updated scope of work.

5 CONCLUSIONS

320. This report presents my technical conclusions for the assessment of GDA Issue GI-AP1000-PSA-01 (Success Criteria) relating to the AP1000 plant GDA closure phase.

321. The ONR Step 4 GDA assessment of the AP1000 internal events at-power PSA conducted in 2011 concluded that the AP1000 plant PSA needs considerable improvement to meet ONR's expectations (Ref. 11). Therefore GDA issue GI-AP1000-PSA-01 was raised by ONR. This required revision of the PSA to include AP1000 plant specific success criteria.

322. I reviewed the resolution plan for addressing this GDA issue with Westinghouse at the start of the closure phase to agree the scope of work needed (Ref. 2). This consisted of 10 technical actions and full documentation of the revised PSA.

323. To address GDA issue GI-AP1000-PSA-01 Westinghouse presented a new internal events at-power PSA undertaken to the ASME/ANS RA Sa 2009 PSA standard (Ref. 6). This was undertaken to the extent achievable by a pre-operational plant with an agreed design reference point.

324. My assessment addressed each of the main technical elements of the internal events at-power PSA as presented within the PSA standard. In this way I covered each of the 10 technical areas in the resolution plan. I undertook this assessment by sampling from each technical area of the PSA using ONR SAPs and the ONR TAG on PSA as my benchmark for a modern standards analysis. My assessment was assisted by technical support contractors with specialist knowledge of success criteria analysis and nuclear reactor plant PSAs.

325. I consider the ASME PSA standard to be a suitable basis to use for developing a modern standards internal events at-power PSA. My assessment finds that the PSA has been carried out adequately with respect to this standard, and this has enabled a meaningful GDA to be completed. I am largely satisfied that the internal events at-power PSA meets the guidance in the ONR TAG on PSA.

326. However, my assessment has identified a number of shortfalls with respect to the ASME PSA standard and the ONR TAG on PSA. I have raised a number of assessment findings to address these shortfalls. I have raised assessment findings in the followings areas for the licensee to address:

- The validation of operator error data used in the PSA.
- Including operator errors for mis-calibration, testing and maintenance operations.
- Undertaking additional MAAP analysis to confirm plant performance and operator timelines.
- A more thorough treatment of dependency between initiating events and safety systems.
- Ensuring that the treatment of containment bypass fault sequences is comprehensive.
- Providing a comprehensive analysis of the reliability of the safety systems during the detailed design phase.
- Including a more realistic treatment of losing offsite power supply which reflects the design of the UK grid system.
- Reviewing the methodology and data used for the treatment of common cause failure.
- Including a number of the less significant initiating events.

- Reviewing the treatment of plant damage states where relevant fault sequence information may be lost for the Level 2 PSA.
- Including additional fault sequences identified during the assessment of the PSA.

327. Westinghouse claims that the core damage frequency and large release frequency from internal events at-power is below the ONR BSO for numerical targets 8 and 9 respectively. I note that this comparison is conservative because the targets are stated in terms of radiological dose and 100 or more fatalities respectively. My assessment has considered the risk impact of the shortfalls presented above.

328. My judgement is that the ONR SAP numerical target 8 and 9 BSOs may well be met for the internal events at-power PSA. However, it is not possible to accurately estimate the overall impact of these shortfalls without completing the technical work required.

329. The PCSR presents the overall risks from the AP1000 plant at the GDA stage (Ref. PCSR Rev 1: Chapter 10). When this is considered together with the shortfalls, gaps and inclusion of site hazards during licensing, it is my judgement that the overall risk from the AP1000 reactor plant design is likely to exceed the ONR SAP target 8 and 9 BSOs, but I consider the risk should be within the respective BSLs with a significant margin.

330. I consider that suitable and sufficient work has been presented by Westinghouse to enable GDA issue GI-AP1000-PSA-01 to be closed.

6 REFERENCES

1 ONR, GI-AP1000-PSA-01, Success criteria for the Probabilistic Safety Analysis, Rev 0 (http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-PSA-01.pdf)

2 AP1000 - PSA-01 (Success Criteria) - Resolution Plan (wec-reg-0051r-enclosure-gi-ap1000-psa-01) - March 2015. TRIM 2016/423987.

3 ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition. (http://www.onr.org.uk/saps/saps2014.pdf)

4 ONR-GDA-CR-15-030 - AP1000 - Discussions on Status of Westinghouse PSA Work 5th Meeting - 27th April 2015. TRIM 2015/166363.

5 ONR, Guidance on Mechanics of Assessment within the Office for Nuclear Regulation, Doc No. 697, TRIM 2013/204124.

6 ASME/ANS, "Addendum to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum a," ASME/ANS RA-Sa-2009, American Society of Mechanical Engineers, March 2009.

7 ONR, NS-TAST-GD-030, Guidance on Probabilistic Safety Analysis, Revision 5. (http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-030.pdf)

8 ONR, NS-TAST-GD-051, Nuclear Safety Technical Assessment Guide, The Purpose, Scope, and Content of Safety Cases, Revision 4, July 2016, 2016/230683.

9 ONR, GI-AP1000-CC-02, Westinghouse AP1000® Generic Design Assessment, GDA Issue, PCSR to Support GDA, Revision 3, TRIM 2011/369249.

10 US NRC, Regulatory Guide 1.200, Revision 2, "An Approach For Determining the Technical Adequacy of Probabilistic Risk Assessment Results For Risk-Informed Activities," U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.

11 HSE, Step 4 Probabilistic Safety Analysis Assessment of the Westinghouse AP1000® Reactor, Report ONR-GDA-AR-11-003, Revision 0, 10 November 2011. (http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-psa-onr-gda-ar-11-003-r-rev-0.pdf)

12 APP-PRA-GM-003, AP1000 Plant PRA Revision D. Accident Sequence and Success Criteria Guidebook, Revision D, February 2015, TRIM 2015/43738.

13 APP-PRA-GSC-340, AP1000 Plant At-Power Internal Events PRA, Initiating Event Analysis Notebook, Revision C February 2015, TRIM 2015/74583.

14 APP-PRA-GSC-025 Revision 1 April 2012. AP1000 Plant Parameter File for MAAP4.0.7, TRIM 2015/43745.

15 APP-PRA-GSC-341 Rev D. AP1000 At-Power Internal Events PRA. Accident Sequence Analysis Notebook, TRIM 2015/298342.

16 APP-PRA-GSC-342 Rev D. AP1000 At-Power Internal Events PRA. Success Criteria Analysis Notebook, TRIM, 2015/298352.

17 APP-PRA-GSC-356 - Revision B - AP1000 Plant At-Power Internal Events PRA Long Term Cooling Analysis. TRIM 2016/65825.

18 APP-PRA-GSC-322 Rev B. AP1000 At-Power Internal Events PRA. Quantification Notebook (including CAFTA File - Internal Events PSA At-Power, APP-PRA-GSC-322-RevB.zip_1438777502_APP-PRA-GSC-322). TRIM 2015/298362.

19 APP-PRA-GSC-323 Rev C. AP1000 Plant At-Power Internal Events PRA, Level 2 Analysis Notebook, TRIM 2016/173563

20 APP-PRA-GSC-376 Rev B. AP1000® Plant At-Power Internal Events PRA, Level 2 Quantification Results Notebook, TRIM 2016/173596.

21 APP-PRA-GSC-321 Rev C. AP1000 Plant At-Power Internal Events PRA, Human Reliability Analysis Notebook TRIM 2015/298394.

22 APP-PRA-GSC-343 Rev B. AP1000 At-Power Internal Events PRA, Data Analysis Notebook TRIM 2015/298483.

23 NUREG-1829 April 2008. Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process.

24 WEC-REG-0166N (NPP_JNE_000166) GDA - AP1000 - PSA - Initial PSA Comments on NUREG 1829 - Approach to LOCA Initiating Event Frequencies. May 2015. TRIM 2015/187964.

25 WEC-REG-0299N (NPP_JNE_000299) - Enc.2 - AP1000 Plan PSA-01 - ONR-NUREG-1829-Comment-Resolution-Form-Revised. - 03 September 2015. TRIM 2015/330003.

26 RQ-AP1000-1495 - UK AP1000-SI-02 Pressuriser Surge Line Fatigue Analyses - 6th June 2016 - Full Response. TRIM 2016/230010.

27 RQ-AP1000-1449 - AP1000 GI-AP1000-SI-02 ASME III Class 1 Pipework General Methods Full Response - 11 March 2016. TRIM 2016/109527.

28 LTR-AP1000-PRA-15-013 Rev 0 dated 19 August 2015 (including Attachments 1, 2 and 3). Subject: Generic Design Assessment (GDA) AP1000® Plant PSA Deliverable: Qualitative Assessment of Unincorporated Class 1 and 2 Design Changes, TRIM 2015/318535.

29 APP-PRA-GSC-336 Revision A January 2016. AP1000 Plant Low Power and Shutdown Internal Events, Limited Scope Success Path Analysis Notebook.29, TRIM 2016/46304.

30 Westinghouse Letter LTR-AP1000-PRA-15-026, Rev 01, Generic Design Assessment (GDA) AP1000® Plant PSA-01 Deliverable: Low Power and Shutdown (LPSD) Probabilistic Risk Assessment (PSA) Initiating Event (IE) Review, TRIM 2016/40782.

31 ONR, NS-PER-GD-014, ONR Guide Purpose and Scope of Permissioning, Revision 6, November 2016, TRIM 2016/448079.

32 Westinghouse, UKP-GW-GL-793 Revision 1. AP1000 Pre-Construction Safety Report. Chapter 10: TRIM 2017/43700.

33 ONR, Nuclear Safety Technical Assessment Guide NS-TAST-GD-003 Revision 7. December 2014. Safety Systems. TRIM 2016/323002.

34 ONR, RQ-AP1000-1663 - Comments on Chapter 10 Revision 0B of the AP1000 PCSR - 11th August 2016. TRIM 2016/320447.

35 ONR, RQ-AP1000-1741, Safety Function and Safety System Claims in the Internal Events At-Power PSA, 28th October 2016, TRIM 2016/419002.

36 Westinghouse, AP1000 - TSC Comments on Westinghouse Response to RQ-AP1000-1741 - Reliability of Safety Functions and Safety Systems - MCS for DAS hardware and PMS S-Signal Functions. TRIM 2016/483576.

37 Westinghouse, LTR-AP1000-PRA-16-047 (NPP_JNE_001413 Enclosure 02) - AP1000 Plant PSA Evaluation and Response to UK Regulatory Query RQ-AP1000-1741 (Response to RQ-AP1000-1741) - 18th November 2016. TRIM 2016/451034.

38 Westinghouse, LTR-AP1000-PRA-16-047 (NPP_JNE_001499 Enclosure 01) - AP1000 Plant PSA Evaluation and Response to UK Regulatory Query RQ-AP1000-1741 - 20th December 2016. TRIM 2016/498151.

39 Westinghouse, APP-PRA-GSC-353 Revision C, Plant At-Power Internal Events PRA, Interfacing System Loss of Coolant Accident Initiating Event Analysis, 25 February 2015, TRIM 2015/74593.

40 Westinghouse, JNE_NPP_000713 - Issue 2 - Comment Resolution Form (Response to RQ-AP1000-1441) - 26 February 2016. TRIM 2016/88436.

41 ONR, RQ-AP1000-1657 - MAAP Parameter File and Low Power and Shutdown Success Criteria Review, 3rd August 2016, TRIM 2016/309100.

42 Westinghouse, NPP_JNE_001292 - AP1000 Plant Parameter File for MAAP 4.0.7 Level 2 Analysis Notebook Comment Form (Response to RQ-AP1000-1657) - 28th September 2016. TRIM 2016/380344.

43 ONR, RQ-AP1000-1441 Issue 2, Assessment of the Initiating Event and ISLOCA Initiating Events Notebooks, 8 December 2015, TRIM 2015/461450.

44 ONR, RQ-AP1000-1384, Clarifications on the Completeness of Initiating Events for the PSA-01 (Success Criteria) Project, 14th August 2015, TRIM 2015/305356.

45 Westinghouse, WEC-REG-0353N, WEC-REG-0353N, Transmittal of Partial response to RQ-AP1000-1384, 2 October 2015, TRIM 2015/368888.

46 Westinghouse, LTR-AP1000-PRA-16-002, Spurious Opening of Turbine Bypass Valves Response to RQ-AP1000-1384, 28 January 2016, TRIM 2016/40536.

47 WEC-REG-0916N - Enclosure 1 - Resolution Form - Response to TRIM 2015/462007 Review Comments Against Westinghouse Responses to RQ-AP1000-1384 - 27th April 2016. TRIM 2016/176489.

48 ONR, RQ-AP1000-1442, PSA-01 - Initiating Events Notebook Assessment - Document Request. 25 November 2015. TRIM 2015/444723.

49 WEC-REG-0513N - Letter from Westinghouse - Transmittal of Full response to RQ-AP1000-1442 - PSA - 02 December 2015. TRIM 2015/456609.

50 WEC-REG-0713N, RQ-AP1000-1441 - AP1000 ONR Assessment of the Initiating Event and ISLOCA Initiating Events Notebooks (Issue 2) Full Response, 26 February 2016.

51 US NRC, Re-evaluation of Station Blackout Risk at Nuclear Power Plants, NUREG/CR-6890, Vol 2, December 2005.

52 US NRC, NUREG CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 – 1995.

53 Westinghouse, JNE_NPP_000713 Issue 2, AP1000 Plant At-Power Internal Events PRA, Initiating Event Analysis Notebook and Interfacing Systems Loss of Coolant Accident Initiating Event Analysis Notebook, Comment Resolution Form (Response to RQ-AP1000-1441), 26 February 2016. TRIM 2016/88436.

54 US NRC, NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, February 2007.

55 US NRC, INL/EXT-14-31428, Initiating Event Rates at U.S. Nuclear Power Plants, 1988–2013, Revision 1, February 2015. http://nrcoe.inel.gov/resultsdb/publicdocs/InitEvent/initiating-event-frequencies-and-trends-2013.pdf

56 ONR, RQ-AP1000-1324, Request for ISV Trials information, 25th March 2015, TRIM 2015/113796.

57 APP-OCS-GER-320 Revision 0 - AP1000 Human Factors Engineering Integrated System Validation Report. September 2015. TRIM 2016/25679.

58 WEC-REG-0629N , Transmittal of RQ-AP1000-1324 Full Response, 29th January 2016 TRIM 2016/41020.

59 ONR, RQ-AP1000-1721, Impact of Revision to HEPs Following ISV Trials and Further WEC Qualitative HF Analysis, 14th October 2016, TRIM 2016/400361.

60 WEC-REG-1219N - Enclosure 1 - LTR-AP1000-PRA-16-035 - AP1000 Plant Human Factors Qualitative Error Analysis Comparison to the Probabilistic Safety Assessment - 29th August 2016. TRIM 2016/341251.

61 WEC-REG-1375N - Letter from Westinghouse - Transmittal of Full Response for RQ-AP1000-1721 - 4th November 2016. TRIM 2016/430580.

62 ONR-GDA-AR-11-012 Revision 0 dated 11 November 2011. Generic Design Assessment – New Civil Reactor Build. Step 4 Human Factors Assessment of the Westinghouse AP1000® Reactor. http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-hf-onr-gda-ar-11-012-r-rev-0.pdf

63 ONR, RQ-AP1000-1734, “Data and Common Cause Failure Modelling in the Internal Events At-Power PSA”, 24 October 2016, TRIM 2016/411430.

64 ONR-NR-AR-16-029-AP1000 Revision 0. GDA issues GI-AP1000-CI-01: DAS Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0: DAS Adequacy of Architecture. 2016/274937.

65 Westinghouse, NPP_JNE_001396, Enclosure 06, AP1000 Plant At-Power Internal Events PRA Data Analysis Notebook, APP-PRA-GSC-343 - Revision B, (Response to RQ-AP1000-1734), 14th November 2016, TRIM 2016/443615

66 IEC, International Electrotechnical Commission. “Functional safety of electrical/electronic/programmable electronic safety-related systems”. Part 6 Annex D. IEC 61508-6. May 1997

67 WCAP-16672-P, Revision 1, Common Cause Failure Parameter Estimates for the PWROG.

68 ONR-NR-AR-16-030-AP1000 Revision 0. GDA issue GI-AP1000-CI-03 – Diversity of the DAS from the PLS/DDS and the PMS. TRIM 2016/274940.

69 ONR, RQ-AP1000-1733, Systems Modelling for ADS2&3 and IRWST Gutter Bypass Isolation Values, 24th October 2016, TRIM 2016/411318.

70 Westinghouse, NNP_JNE_001396 - RQ-AP1000-1733 Comment Resolution Form (Response to RQ-AP1000-1733) - 14th November 2016. TRIM 2016/443595.

71 ONR, RQ-AP1000-1733 - Clarifications Requested from Westinghouse on ADS2/3 Dependency and MAAP Files - 23 January 2017. TRIM 2017/38428.

72 ONR, RQ-AP1000-1733 - Westinghouse Response to Clarifications on ADS2/3 Dependency and MAAP files - 27 January 2017. TRIM 2017/38422.

73 Westinghouse WEC-REG-0243R (NPP_JNE_000243), APP-PRA-GSC-341-Revision D and APP-PRA-GSC-342 Revision D, RQ-AP1000-1540 - Comment Resolution Form - Accident Sequence Analysis Notebook and Success Criteria Analysis Notebook (Response to RQ-AP1000-1540) - 1st July 2016. TRIM 2016/265900.

74 ONR, RQ-AP1000-1540 - ONR Assessment of the Internal Events At-Power Event Tree Modelling and Success Criteria, 31st March 2016, TRIM 2016/135240.

75 ONR, RQ-AP1000-1655 - ONR Assessment of the Internal Events At-Power Event Tree Modelling and Success Criteria, 29th July 2016, TRIM 2016/303926.

76 LTR-AP1000-PRA-16-044 - AP1000 Plant Probabilistic Safety Assessment Impact Assessment of Spurious Squib Valve Actuation and Consequential Failures of PMS (Response to RQ-AP1000-1715) - 31st October 2016. TRIM 2016/423584.

77 WEC-REG-1204N - Enclosure 2 - UKP-PXS-GLR-001 - Revision 0 - Condensate Return Analysis Summary Report. TRIM 2016/333124.

78 ONR-NR-AR-16-026 Revision 0, AP1000 Assessment Report, Fault Studies, GI-AP1000-FS-06, Validation of the IRWST Cooling Function for the PRHR. TRIM 2016/274920

79 WEC-REG-01291N (NPP_JNE_001291), APP-PRA-GSC-356 - Revision B - Accident Sequence and Success Criteria Comment Form (Response to RQ-AP1000-1655) - 28th September 2016. TRIM 2016/380166.

80 NUREG-1570. March 1998. Risk Assessment of Severe Accident-Induced Steam Generator Tube Rupture.

81 WEC, LTR-AP1000-PRA-16-027, “Human Reliability Analysis Cognitive Errors and Recoveries Response”, July 2016, TRIM 2016/265907.

82 WEC-REG-1363N - Enclosure 1 - APP-PRA-GSC-323 - Revision B - AP1000 Plant At-Power Internal Events PRA Level 2 Analysis Notebook Comments Resolution Form - 1st November 2016. TRIM 2016/424432.

83 NNP-JNE-0001109 - Comment Resolution Form (Response to RQ-AP1000-1588) - 15th July 2016. TRIM 2016/285370.

84 ONR, RQ-AP1000-1588, ONR Assessment of Internal Events At-Power PSA - Plant Damage States and Level 2 PSA, 13th May 2016, TRIM 2016/197489.

85 AP1000 - Technical Assessment Note - Assessment of ADS4 Reliability. January 2016. TRIM 2016/5588.

86 ONR-NR-AR-16-034-AP1000 Revision 0. GDA Issue GI-AP1000-CI-08. PMS Adequacy of Safety Case. TRIM 2016/274946.

87 WEC-REG-1363N, Transmittal of Additional Information for RQ-AP1000-1588 (addressing comments 23 and 24), 1st November 2016 , TRIM 2016/424409.

88 WEC-REG-0243N Enclosure 10, APP-PRA-GSC-319 - Rev.D - AP1000 Plant At-Power Internal Events PRA, Protection and Safety Monitoring System Notebook - 07 August 2015, TRIM 2015/298541.

89 ONR, RQ-AP1000-1589, ONR Assessment of PMS and ADS4 Systems Analysis in the Internal Events At-Power PSA, 13th May 2016, TRIM 2016/197530.

90 WEC-REG-1085N (NPP_JNE_001085), APP-PRA-GSC-319 Revision D, Comment Resolution Form (Response to RQ-AP1000-1589), 6th June 2016. TRIM 2016/272715.

91 ONR-NR-AR-16-031 March 2017. GI-AP1000-CI-04, AP1000 Assessment Report, Control and Instrumentation, PMS Spurious Operation. TRIM 2016/274942.

92 ONR, RQ-AP1000-1715, Further Risk Sensitivity Studies for the PMS and Squib Valves Following the 20 and 21 September 2016 ONR Westinghouse Meeting in the UK, 10th October 2016 TRIM 2016/392678.

93 Licensing of Safety Critical Software for Nuclear Reactors. Common Position of International Nuclear Regulators' and Authorised Technical Support Organisations. Revision 2015. TRIM 2016/155853.

94 IEC, IEC61513:2011, Nuclear Power Plants – Instrumentation and control for systems important to safety – General requirements for systems.

95 WEC-REG-1085N , Transmittal of Partial Response for RQ-AP1000-1589, 6th July 2016, TRIM 2016/272701.

96 WEC-REG-1155N, Transmittal of Full Response for RQ-AP1000-1589, 1st August 2016, TRIM 2016/306391.

97 NPP-JNE-001361 - Comment Resolution Form AP1000 Plant At-Power PRA (Response to RQ-AP1000-1715) - 31st October 2016. TRIM 2016/423575.

98 LTR-AP1000-PRA-16-044, AP1000 Plant Probabilistic Safety Assessment Impact Assessment of Spurious Squib Valve Actuation and Consequential Failures of PMS (Partial response to RQ-AP1000-1715), 31st October 2016, TRIM 2016/423584.

99 ONR-NR-AR-16-014 - AP1000 Assessment Report. March 2017. GDA Close-Out for the AP1000 Reactor. GDA Issue GI-AP1000-ME-01 – Squib Valve Concept and Design Substantiation. TRIM 2016/275007.

100 JA1/ONR-1501 Review of Westinghouse AP1000 Resolution to GI-AP1000-PSA-01 – Success Criteria for the Probabilistic Risk Assessment February 2017.

101 APP-PRA-GSC-236 Revision 1. Westinghouse Probabilistic Risk Analysis ([PRA). TRIM 2011/76409.

102 ONR-NR-AN-16-026 - Westinghouse AP1000 - Assessment Note - Structural Integrity of Squib Valves Supporting ME-01. TRIM 2017/45708.

103 ONR-NR-CR-16-539 - AP1000 GDA Mechanical Engineering Level 4 Meeting with Westinghouse to Discuss GI-AP1000-ME-01 - 20th and 22nd September 2016. TRIM 2016/379366.

104 ONR, ONR-NR-CR-16-710, Contact Record. Discussion of AP1000 PSA Work for PSA-01 & PSA-02 (No 36). TRIM 2016/450846.

105 IAEA, IAEA-TECDOC-648, Procedures for conducting common cause failure analysis in probabilistic safety assessment, May 1992. http://www-pub.iaea.org/MTCD/publications/PDF/te_648_web.pdf

106 IEC, IEC 61508-6:2010 , Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

107 USNRC, NUREG CR-5485, Guidelines on Modelling Common-Cause Failures in Probabilistic Risk Assessment, June 1998

108 ONR-NR-AR-16-034 dated March 2017. GDA close-out for the AP1000 Reactor. GDA issue GI-AP1000-CI-08. PMS Adequacy of Safety Case. TRIM 2016/274946.

109 ONR, ONR-NR-CR-16-745, Contact report, Discussion on the Status of Westinghouse PSA Work for PSA-01 and PSA-02 (No 37), 29 November 2016.

110 ONR, ONR-NR-CR-16-820, Contact report, Discussion of AP1000 PSA Work for PSA-01 & PSA-02 (No 38), 20 December 2016.

111 ONR, Email, TSC Comments on Westinghouse Response to RQ-AP1000-1741 - Reliability of Safety Functions and Safety Systems - MCS for DAS hardware and PMS S-signal functions, 7 December 2016, TRIM 2016/483576.

112 Westinghouse, WEC_REG_1292N, Transmittal of Full response for RQ-AP1000-1657, 28th September 2016, TRIM 2016/380318.

113 ONR, RQ-AP1000-1735 - MAAP and Success Criteria Modelling. Scientech Follow-Up Visit to Westinghouse Cranberry Offices. 14th November 2016. TRIM 2016/443640.

114 Westinghouse, WEC-REG-01396N (NPP_JNE_001496), APP-PRA-GSC-356, Revision B and APP-PRA-GSC-323 Revision B, and APP-PRA-GSC-342 Revision D, AP1000 Plant At-Power Internal Events PRA Long Term Cooling Analysis Level 2 Analysis Notebook (Response to RQ-AP1000-1735) - 14th November 2016. TRIM 2016/443659.

115 Westinghouse, NPP-JNE-001292 - AP1000 Plant Parameter File for MAAP 4.0.7 Level 2 Analysis Notebook Comment Form (Response to RQ-AP1000-1657), 28th September 2016, TRIM 2016/380344.

116 Westinghouse, UKP-GW-GL-022, UK AP1000 Probabilistic Risk Assessment, Rev. 0, 5 November 2007, TRIM 2011/81970

117 Westinghouse, AP1000 plant Design Control Document, Revision 17.

118 LTR-AP1000-PRA-15-013 dated 19 August 2015. Generic Design Assessment (GDA) AP1000® Plant PSA Deliverable: Qualitative Assessment of Unincorporated Class 1 and 2 Design Changes. TRIM 2015/318535.

119 LTR-AP1000-PRA-15-013 dated 19 August 2015. Attachment 1 TRIM 2015/318657. Attachment 2 TRIM 2015/318674 and Attachment 3 TRIM 2015/318690.

120 ONR Email to Westinghouse. Clarifications Requested from Westinghouse on Gap Analysis DCPs. 24 January 2017. TRIM 2017/40128).

121 Westinghouse, LTR-AP1000-PRA-17-005 Revision 0, Westinghouse Response to Gap Analysis Questions – Clarification on Incorporated DCPs Post PSA Design Freeze Date 2010. 26 January 2016. TRIM 2017/36079.

122 ONR-NR-CR-16-853- AP1000 - Discussion of AP1000 PSA Work with USNRC - 11 January 2016. TRIM 2017/16041.

123 APP-GW-GEE-2411, Rev 0, ADS Diverse Actuation Block, 28 March 2016, TRIM 2016/132667.

124 Westinghouse, APP-GW-GEE-4291, Revision 0, Change to Address Spurious Actuation of the IRWST Squib Valves (Response to RQ-AP1000-1651), 5th August 2016, TRIM 2016/312971

125 US NRC, GSI-191, “Assessment of Debris Accumulation on PWR Sumps Performance,” Footnotes 1691 and 1692 to NUREG-0933, 1998,” Nuclear Regulatory Commission, May 14, 1997

126 US NRC, Generic Letter 2004-02 dated September 13 2004. OMB Control No.: 3150-0011. Potential Impact of Debris Blockage on Emergency Recirculation During Design Basis Accidents at Pressurized Water Reactors.

127 US NRC, NUREG-1793, Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design Docket No 52-006, Chapter 4, September 2004

128 ONR, AP1000 Technical Note, Assessment of Single Failures of Safety Measures in the Internal Events At-Power PSA, 15 June 2016, TRIM 2016/241814.

129 Westinghouse, NPP_JNE_001011 Enclosure 04, LTR-RAM-I-12-075, Expert Panel for Estimating Reference Probabilities for Debris-Induced Failure of Long Term Core Cooling for the AP1000® Plant, 11 January 2013, TRIM 2016/280220.

130 ONR, RQ-AP1000-1679, Risk Sensitivity and Consequences to the IRWST (and Other Safety Measures) due to a PRHR Line Break, 26th August 2016, TRIM 2016/340047.

131 NPP-JNE-001299 - Comments Resolution Form (Response to RQ-AP1000-1679) - 30th September 2016. TRIM 2016/382709.

132 UKP-GW-GLR-114, Rev 1, UK AP1000 Plant Internal Hazards Topic Report - Pressure Part Failure, January 2017, TRIM 2017/24720.

133 WEC-REG-0741N Enclosure 3, UKP-1100-S3C-030 , Revision 0, IRWST Impact Response to Gross Failure of PRHR HX Return Pipe L103, 4th March 2016, TRIM 2016/98959.

134 WEC-REG-1415N Enclosure 1, UKP-ME02-Z0C-001, Revision 1, PRHR HX Mounting Ring Welds Evaluation for PRHA Loads on Outlet Nozzle, 21st November 2016, TRIM 2016/453817.

135 Westinghouse, WNS_DCP_002234, Revision 0, 28 July 2016: AP1000® Plant Spurious ADS Stage 4 and IRWST Injection Expert Panel Assessment. TRIM 2016/306425.

136 Westinghouse, NPP_JNE_001412, Full response to RQ-AP1000-1731, AP1000 Squib Valve Safety Case - Pressure Boundary and Support Integrity, 18th November 2016 TRIM 2016/450952.

137 RQ-AP1000-1779 – Proposed Codes and Standards for UK Class 2 Pressure Equipment and Storage Tanks (SI06 A1) – 13 January 2017 – Full Response. TRIM 2017/18426.

138 ONR-NR-AR-16-010 Revision 0. GDA Close-Out for the AP1000 Reactor. GDA Issue GI-AP1000-SI-01. Avoidance of Fracture. TRIM 2017/74011.

Table 3

Relevant Safety Assessment Principles for Probabilistic Safety Analysis Considered During the Close-Out Phase

SAP Number 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 ONR judgements on the safety of the facility and whether the risks of its operation are being made as low as reasonably practicable.	Assessed in Section 4 of this report. The need for PSA has been recognised from the start of the GI-AP1000-PSA-01 closure project.
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.	Assessed in various sub-sections in Section 4 of this report. The PSA has been conducted to an agreed design reference point that represents a pre-operational plant (See Section 4.11 of this report).
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 of this report. The scope of GI-AP1000-PSA-01 project is by agreement with ONR limited to internal events when operating critical at-power, and is intended to addresses only the radioactivity in the reactor core.

SAP Number 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.	Assessed in detail within Section 4 of this report. The adequate representation of the plant is assessed against the agreed design reference point. The scope of assessment needed is presented in Section 4.1 of this report.
FA.14 Fault analysis: PSA Use of PSA	"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.	Assessed in detail in Section 4.13 and 4.14 of this report. The internal events at-power PSA has been used to identify and assess improvements with the intention to reduce risk to ALARP.
Numerical Targets NT.1	Target 8: The total predicted frequency of accidents on an individual facility which would give doses to any person off the site. Target 9: Target 9 is the frequency of 100 or more fatalities from all accidents at the site.	BSL/yr BSO/yr Offsite dose 0.1-1 mSv 1 10^{-2} Offsite dose 1-10 mSv 10^{-1} 10^{-3} Offsite dose 10-100 mSv 10^{-2} 10^{-4} Offsite dose 100-1000 mSv 10^{-3} 10^{-5} Offsite dose >1000 mSv 10^{-4} 10^{-6} BSL 10^{-5}/year BSO 10^{-7}/year	Assessed in Section 4 of this report and in particular within Sections 4.13 and 4.14 where the numerical risks are assessed with respect to the ONR numerical targets and used to support the ALARP analysis. Section 4.13 of this report discusses the interpretation of these targets for the risk measures of core damage frequency and large release frequency presented to support the PSA.

SAP Number and Title	Description	Interpretation	Comment
EDR.3 Common Cause Failure	"Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability"	This SAP is relevant to my assessment of the plant features which display redundancy. In particular the PMS and the field equipment actuated by the PMS such as the valves needed to actuate the passive safety systems. This SAP advises that common cause failure data better than 10^{-5}/demand is not expected and would require particular justification should such claims arise.	I have considered this SAP for my common cause failure assessment of the PMS software, and the beta factor analysis of the PMS hardware. I have also considered this SAP when assessing the common cause failure modelling of the passive core cooling gutter isolation valves, and the main AC breakers.
EDR.4 Single Failure Criterion	"During any permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function"	This SAP advises that the principle means of fulfilling a category A safety function should always be designed to meet the single failure criterion.	I have applied this SAP when assessing a single point of failure within the DAS, noting that the DAS is a class 2 system supporting the PMS to fulfil a category A safety function. (See Section 4.7.22) I have applied this SAP when considering the function of the IRWST. (See Section 4.9.3)
ECS.2 Safety Classification of Structures, Systems and Components	"Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety"	This SAP is relevant to my assessment because the PSA calculates the reliability of the AP1000 plant safety systems.	I have applied this SAP when considering the reliability on demand of the reactor plant safety systems, and whether these have been presented within the PSA and the PCSR. (See Section 4.7.23) I have also considered it to highlight when high reliability of the safety system or component is being

SAP Number and Title	Description	Interpretation	Comment
			claimed in the PSA. For example, the IRWST. (See Section 4.9.3)
ESS.1 Provision of Safety Systems	"All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined stable, safe state"	The safe stable state in this SAP is considered with respect to the ability of the passive safety systems to maintain long term cooling of the core.	I have considered this SAP with respect to the ability of the passive residual heat removal system to maintain stable plant conditions in the long term given that the efficiency of the condensate return to the IRWST is less than 100%. (See Section 4.6.3)

Annex 1

Assessment Findings to be addressed during the Forward Programme – PSA-01 (Success Criteria – Internal Events At-Power)

Assessment Finding Number	Assessment Finding	Reference Information
CP-AF-AP1000-PSA01-01	The licensee shall provide the success criteria for multiple PRHR tube ruptures, and include this in the PSA. It should be determined whether PRHR tube rupture data may be better represented by heat exchanger data rather than steam generator tube rupture data.	4.3.11 Rupture of Multiple Tubes within the PRHR
CP-AF-AP1000-PSA01-02	The licensee shall validate the dominant human error probabilities in the PSA as follows: 1) review the time available for the operators to act, 2) take account of improvements to the operating interface as the human engineering deficiencies in the ISV trials are addressed and 3) optimise the appropriate operating procedures. The licensee shall demonstrate that the risk important human actions claimed within the PSA reduce risks to ALARP. The PSA shall be revised to reflect the outcome of this work.	4.4 Validation of the Human Reliability Data within the PSR
CP-AF-AP1000-PSA01-03	The licensee shall perform sufficient bounding analysis to justify manual actuation of the PCS in the long term cooling models, and justify the time window assumed for manual actuation of PCS. These analyses should assume an unisolated containment.	4.5.2 PCS Actuation for Long Term Containment Cooling

Assessment Finding Number	Assessment Finding	Reference Information
CP-AF-AP1000-PSA01-04	The licensee shall carry out the following MAAP analysis: 1) Update the MAAP success criteria runs with updated parameter files (to Rev 1 or a later QA'd parameter file version) to generate an appropriate bounding case for the actuation of ADS2 and 3 valves. Any changes in the results in terms of ADS success criteria or time windows for human error probabilities shall be evaluated and the PSA updated accordingly. 2) To justify the long term cooling fault sequences on event tree path LTC-003.	4.5.4 ADS Stage 2 and Stage 3 Valve Opening MAAP Model 4.5.5 Success Criteria for PCS in the Long Term Cooling PSA
CP-AF-AP1000-PSA01-05	The licensee shall carry out further MAAP modelling to demonstrate that a stable situation can be reached for the success states claimed in sequences 1, 4 and 7 of the LTCP event tree. The frequency of not achieving this stable state shall be estimated and included in the plant core damage frequency. The licensee can also consider carrying an assessment of repair times as part of an updated quantification.	4.6.3 Long Term Stable Plant State
CP-AF-AP1000-PSA01-06	The licensee shall include secondary side scrubbing for steam generator tube rupture events in the Level 2 risk model.	4.7.7 Conservative Treatment of Large Bypass Fault Sequences
CP-AF-AP1000-PSA01-07	The licensee shall perform a more detailed assessment of severe accident induced steam generator tube rupture in accordance with NUREG-1570 for scenarios where the steam generator secondary side remains pressurised. A probability of induced steam generator tube rupture for this case should be generated and included in the containment even trees.	4.7.11 Induced Steam Generator Tube Rupture (ISGTR)
CP-AF-AP1000-PSA01-08	The licensee shall provide justification that the results of the MAAP analysis adequately support the derivation of the containment over pressure probability (L2-CF-EV1).	4.7.13 MAAP Analysis Supporting Containment Overpressure Analysis

Assessment Finding Number	Assessment Finding	Reference Information
CP-AF-AP1000-PSA01-09	The licensee shall include in the PSA the updated data for software common cause failure for both the PMS and PLS.	4.7.16 Software Common Cause Failure of the PMS and PLS
CP-AF-AP1000-PSA01-10	The licensee shall carry out ALARP analysis for the core damage sequences from spurious ADS4 actuation arising from software common cause failure. This shall include the potential for optimising the operators response and whether a delayed operator response can protect the plant.	4.7.18 Spurious ADS4 Actuation ALARP Analysis
CP-AF-AP1000-PSA01-11	The licensee shall assess during detailed design the reliability of the safety functions/safety systems claimed in the safety case and PSA. Confirmation shall be provided that the reliability for each meets the expectations with respect to the categorisation and classification system.	4.7.23 Quantification of the Reliability of the Safety Measures in the Safety Case
CP-AF-AP1000-PSA01-12	The licensee shall update the PSA to ensure that the initiating events of spurious squib valve actuation are appropriately modelled. In particular the following consequential events should be included: 1) the loss of one of the two CMT lines for the spurious ADS4 initiating events, and 2) the failure mode of the non-return valves failing to open following spurious actuation of the IRWST squib valves.	4.9.6 Mechanical and Structural Success Criteria for the ADS4 Valves 4.9.7 Mechanical and Structural Success Criteria for the IRWST Injection Lines

Annex 2

Technical Items to be addressed with the GDA Step 4 PSA Assessment Findings – PSA-01 (Success Criteria – Internal Events At-Power)

Step 4 PSA Assessment Finding	Technical Item	Report Section Reference
AF-AP1000-PSA-011	Technical Item 11-1: The licensee shall document more clearly the methodology describing the initiating event grouping process. For example, a table should be provided indicating availability of main and support systems, for example off-site power, SGs, feedwater, condensate, heat sink, etc. for each initiating event – to assist in the explanation.	4.3.6 Grouping of Initiating Events and Dependencies
AF-AP1000-PSA-012	Technical Item 12-1: The licensee shall carry out a loss of HVAC analysis, with heat-up calculations used, to establish whether there are any additional initiating events, and to inform MCR habitability considerations. Technical Item 12-2: The licensee shall include loss of the raw water system that supports makeup to the circulating water system and service water system as an initiating event. Technical Item 12-3: The licensee shall provide a more robust justification for the approach taken to identify manual shutdown initiating events due to technical specification requirements. This should include consideration of technical specification requirements for PSA related systems for allowable outage times of up to 24 hours. If necessary, additional initiating events should be included in the PSA. Technical Item 12-4: The licensee shall include spurious opening of the turbine bypass valves as an initiating event.	4.3.1 Loss of HVAC Cooling 4.3.5 Loss of Ultimate Heatsink Initiating Event 4.3.8 Manual Shutdown due to Technical Specification Requirements 4.3.12 Spurious Opening of the Turbine Bypass Valves

Step 4 PSA Assessment Finding	Technical Item	Report Section Reference
AF-AP1000-PSA-017 AF-AP1000-PSA-025	Technical Item 17-1: The licensee shall undertake a FMEA to review the potential for dependencies between initiating events and support systems. The FMEA requested under GDA Step 4 AF-AP1000-PSA-025 can be used for this. Technical Item 17-2: The licensee shall include in the risk model the dependencies identified for a spurious low steam line pressure signal and a spurious low T-cold signal. Technical Item 17-3: The licensee shall include the dependency between the initiating event and the fault tree models for the actuation of safety systems following a spurious PMS initiating event.	4.3.4 Support System Initiating Events 4.3.6 Grouping of Initiating Events and Dependencies 4.6.4 Initiating Event and Mitigating System Dependency for the PMS
AF-AP1000-PSA-019	Technical Item 19-1: The licensee shall update the probability of consequential loss of offsite power to take into account the characteristics of the UK high voltage grid and the site specific switchyard design. The potential for a higher probability of loss of offsite power following a LOCA events shall be included. Recovery for short term loss of offsite power events shall be credited in order to remove conservatism from the model.	4.3.3 Consequential Loss of Offsite Power (LOOP)
AF-AP1000-PSA-028	Technical Item 28-1: The licensee shall use a fault tree model for sequences in the LTCP event tree model for startup feedwater that includes a requirement for manual rather than automatic actuation. The licensee shall review and, if necessary, update of the dependency post-processing rules should be done to capture any new combinations of human error probabilities that may arise.	4.6.2 Start-Up Feedwater in the Long Term Cooling Analysis

Step 4 PSA Assessment Finding	Technical Item	Report Section Reference
AF-AP1000-PSA-034	Technical Item 34-1: The licensee shall carry out a systematic review of pre-initiating event operator errors and include them in the PSA.	4.3.7 Operator Induced Initiating Events
AF-AP1000-PSA-036	Technical Item 36-1: The licensee shall update the initiating event frequencies in the PSA with the most recent operating experience.	4.3.9 Intact Circuit Fault Initiating Event Frequency Data
AF-AP1000-PSA-042	Technical Item 42-1: The licensee shall address the following common cause failure modelling items in the PSA: 1) The beta factor analysis should be revised to include beta factors for both detectable and non-detectable failures. 2) The common cause failure analysis should be using a higher value of mean time to repair for multiple failures than for single failures. 3) Further work is needed to demonstrate that inclusion of common cause failure events with 4 or more combinations of components will not have a significant impact on the total core damage frequency. 4) Evidence should be provided that WCAP16672-P data is adequate for common cause modelling by making the independent peer reviews available, and considering whether the USNRC data should also be used to enhance the size of the database used. 5) A justification should be provided for reducing the alpha factors by a factor of 2 for operating equipment. 6) Within the PSA there are common cause failure probabilities that have a similar value to the independent coincident failure of the components by chance. Justification for these values is required.	4.7.4 WCAP Data Source

Step 4 PSA Assessment Finding	Technical Item	Report Section Reference
	Technical Item 42-2: The licensee shall use a common cause failure methodology which is suitable for a capability category III PSA during the licensing phase. Technical Item 42-3: The licensee shall update the PSA with the AP1000 plant specific PMS hardware common cause failure information when it becomes available.	4.7.21 Dependent Failure Modelling for the PMS Hardware 4.7.21 Dependent Failure Modelling for the PMS Hardware
AF-AP1000-PSA-050	Technical Item 50-1: The licensee shall undertake AP1000 plant specific success criteria analysis for the low power and shutdown PSA. This shall ensure that a full and comprehensive analysis of human error probabilities and recoveries is included. Technical Item 50-2: The licensee shall update the PSA with AP1000 plant specific MAAP analysis for passive containment cooling in the low power and shutdown plant operating states. Technical Item 50-3: The licensee shall carry out further analysis to: 1) identify more precisely the shutdown conditions/plant operating states that may be vulnerable to temporary core uncover, and 2) investigate and possibly implementation of design or procedure changes to reduce or eliminate the possibility of core uncovery during shutdown fault sequences.	4.8.1 Impact of Timings on Low Power and Shutdown Human Error Probabilities 4.8.2 Additional Requirement for PCS Long Term Containment Cooling During Shutdown 4.8.3 Core Uncovery in the Shutdown Plant Operational States

Step 4 PSA Assessment Finding	Technical Item	Report Section Reference
AF-AP1000-PSA-057	Technical Item 57-1: The licensee shall address the following items within the plant damage state and Level 2 modelling: 1) Separate plant damage states should be considered for ATWS and reactor coolant system high pressure core damage fault sequences. 2) The transfers of plant damage states AN, ANF, HN, HNF and HI to containment event tree HP6 and the implied loss of detail related to CMT, accumulator and IRWST injection should be reviewed and if necessary modified. 3) The documentation explaining the treatment of plant damage states H2I and HCI should be improved. Technical Item 57-2: The licensee shall provide justification for the plant damage state grouping of steam line break core damage fault sequences. Technical Item 57-3: The licensee shall update the steam generator tube rupture Level 2 modelling so that early core damage and late core damage fault sequences and treated separately.	4.7.10 Plant Damage State Simplifications 4.7.14 Changes to the Step 4 Plant Damage States 4.7.14 Changes to the Step 4 Plant Damage States
AF-AP1000-PSA-058	Technical Item 58-1: The licensee shall review the risk model to ensure that the bypass character of the fault sequences transferred from the Level 1 model to the Level 2 model is not lost.	4.7.6 Transfer of Bypass Fault Sequences to Long Term Cooling Event Trees

Step 4 PSA Assessment Finding	Technical Item	Report Section Reference
AF-AP1000-PSA-059	Technical Item 59-1: The licensee shall review the operator dependency modelling in the PSA as follows: 1) Where combinations of human error probabilities occur in which the end of the time window for the first human error probability is close in time to the cue for the second one, the level of dependency should be reviewed. This should be done for the PSA as a whole. 2) If separation in time has been used as the reason to reduce dependency levels, the licensee should consider whether the dependency level should be increased. 3) The licensee should review the guidance used for the assignment of dependency and consider whether or not these rules need to be modified to account for cases such as those described in his section of this report. A justification for the final decision to update the dependency assignment rules or not should be developed and documented.	4.7.12 Level 2 Human Error Dependency Modelling
AF-AP1000-PSA-065	Technical Item 65-1: The licensee shall perform further analysis to bound scenarios that may lead to containment underpressure challenges. This shall include a justification of the maximum differential under pressure that the containment can withstand which is suitable for use in PSA.	4.5.3 Containment Under-Pressure Failure – MAAP Justification
AF-AP1000-PSA-070	Technical Item 70-1: The licensee shall update the containment event tree models used in the Level 2 PSA so that relevant severe accident phenomena are also evaluated in sequences where a small loss of containment isolation has occurred.	4.7.9 Additional Containment Challenges from Severe Accident Phenomena

Annex 3

Minor Shortfalls to be addressed during the Forward Programme – PSA-01 (Success Criteria – Internal Events At-Power)

Minor Shortfall Number	Minor Shortfall	Report Section Reference
CP-MS-AP1000-PSA01-01	The documentation should be improved to describe the methodology used to analyse consequential events in the PSA. A list of event trees and associated transfers to assist understanding the initiating event analysis is requested.	4.3.2 Consequential Initiating Events
CP-MS-AP1000-PSA01-02	Computational methods should be developed so that the use of expert judgement to derive success criteria for the AP1000 plant can be reduced in the future.	4.5.1 Use of Expert Judgement
CP-MS-AP1000-PSA01-03	The “Flags Quant.txt” file should be corrected.	4.7.8 Quantification of the Model
CP-MS-AP1000-PSA01-04	The PSA should include the latest blocker design.	4.7.19 The Blocker Design