New Reactors Programme

GDA close-out for the AP1000® Reactor

GDA Issue GI-AP1000-PSA-02 (Fire PSA)

Probabilistic Safety Analysis for the Westinghouse AP1000® Reactor

Assessment Report: ONR-NR-AR-16-018
Revision 0
March 2017

EXECUTIVE SUMMARY

Westinghouse Electric Company LLC 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 the 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 internal fire Probabilistic Safety Analysis (PSA). Specifically this report addresses GDA Issue GI-AP1000-PSA-02 (Fire PSA).

This GDA issue arose in Step 4 because:

- ONR's assessment concluded that the internal fire risk was not representative of the AP1000 reactor design. It was constructed using the Electric Power Research Institute (EPRI) Fire-Induced Vulnerability Evaluation (FIVE) methodology. This was published in 1992 and there are now updated modern standards methodologies.

The Westinghouse GDA issue resolution plan stated that its approach to closing the issue was:

- To present a new fire PSA constructed to the NUREG/CR-6850 guidance and the ASME/ANS RA Sa 2009 fire PSA standard (Refs 4 and 6 respectively). The fire PSA would also be accompanied by analysis to show that risk has been reduced As Low As Reasonably Practicable (ALARP).

My assessment conclusion is:

- I am satisfied that the fire PSA meets the majority of the guidance in the ONR Technical Assessment Guide (TAG) on PSA (Ref. 10).

- Westinghouse claims that the core damage frequency and large release frequency from fires is below the ONR Basic Safety Objective (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 any shortfalls identified with respect to the PSA standards and the ONR TAG on PSA. None of the shortfalls has been found to individually increase the core damage frequency by more than 20%. It is my judgement that the claims made by Westinghouse are supported, and the risks are comparable to the ONR Safety Assessment Principle (SAP) BSOs for numerical targets 8 and 9.

- However, I consider that the risk from fires could change upwards or downwards as additional analysis is undertaken during the licencing phase to reflect detailed design, and the assessment findings included in my report are addressed.

- The ALARP analysis presented by Westinghouse is based on a systematic review of the fire PSA results to identify potential risk reduction measures.

My judgement is based on the following factors:

- I consider the NUREG guidance and ASME fire PSA standard to be suitable for developing a modern standards fire PSA. The fire PSA has been carried out adequately with respect to these standards, and this has enabled a meaningful GDA to be completed.

- I undertook this assessment by sampling from each technical area of the fire PSA using ONR SAPs and the ONR TAG on PSA as my benchmark. My assessment was assisted by technical support contractors with specialist knowledge of fire analysis and fire PSAs, and I conducted many discussions with Westinghouse.

The following matters remain, which are for a 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 and decisions.

I have raised eight assessment findings and seven minor shortfalls. The assessment findings apply where I judge that there is a missing or inadequately developed element of relevant good practice with respect to the NUREG guidance, fire PSA standard or the ONR TAG on PSA. The number of assessment findings is relatively few when considering the large size and complexity of the fire PSA.

My assessment supports the view that fire risks are being managed towards ALARP as the AP1000 design continues through GDA and into the licensing phase. However, I have raised one assessment finding where I judge that further ALARP justification is needed. This is to address the need for fire detection and suppression within a limited number of areas of the plant. The ALARP options for fire detection and suppression are not precluded by the status of the design at the closure of GDA or into the licensing phase. They can be implemented by the licensee if necessary.

In summary, I am satisfied that GDA Issue GI-AP1000-PSA-02 can be closed.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
ASME / ANS	American Society of Mechanical Engineers/American Nuclear Society
BSL	Basic Safety Level
BSO	Basic Safety Objective
CAFTA	Computer Aided Fault Tree Analysis
CDF	Core Damage Frequency
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DCP	Design Change Proposal
DRP	Design Reference Point
EPM	Engineering Planning and Management
EPRI	Electric Power Research Institute
FLASH-CAT	Flame Spread Over Horizontal Cable Trays
FRANX	PSA Computer Code for Manipulating Spatial Information
GDA	Generic Design Assessment
HOW2	ONR Business Management System
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IRWST	In-Containment Refuelling Water Storage Tank
LRF	Large Release Frequency
MCR	Main Control Room
MDEP	Multi-national Design Evaluation Programme
NFPA	National Fire Protection Association
NUREG	US NUclear REGulator document
OECD-NEA	Organisation for Economic Co-operation and Development Nuclear Energy Agency
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PSA	Probabilistic Safety Analysis
PRHR	Passive Residual Heat Removal
PSR	Preliminary Safety Report
PWR	Pressurised Water Reactor
RCP	Reactor Coolant Pump
SAPs	Safety Assessment Principles
SFAIRP	So Far As Is Reasonably Practicable

SSER	Safety, Security and Environmental Report
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
US NRC	United States (of America) Nuclear Regulatory Commission
VBA	Visual Basic Application
WENRA	The Western European Nuclear Regulators' Association
ZRS	Offsite Retail Power System

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1.1 Background

1. Westinghouse Electric Company LLC 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 the 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.

2. 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-02 (Fire PSA).

3. The related GDA Step 4 report (Ref. 1) is published on our website (**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 (**www.onr.org.uk/new-reactors/index.htm**).

1.2 Scope

4. The scope of the work needed to address GDA Issue GI-AP1000-PSA-02 (PSA-02 for brevity) is presented in Annex 2 of the ONR Step 4 PSA report (Ref. 1). At the start of the GDA close-out phase I discussed and agreed a final version of the resolution plan with Westinghouse to ensure that there was an updated and common understanding of the scope of work. The final resolution plan for PSA-02 is presented in Ref. 2.

5. The following high level scope of work is outlined in the resolution plan:

- The fire PSA for GDA Issue GI-AP1000-PSA-02 will address operation of the reactor plant at-power. The Step 4 assessment finding AF-AP1000-PSA-004 will ensure that the licensee provides full-scope fire PSA which includes the spent fuel pool and low power / shutdown operations for the reactor plant.

- The fire PSA will be based on the latest PSA standards available and will use the most recent available cable routeing information available at a date agreed with ONR.

- The fire PSA will use the internal events at-power risk model developed for the GDA Issue GI-AP1000-PSA-01 and reflect the AP1000 plant at an agreed Design Reference Point (DRP). A qualitative analysis will be performed for Class 1 and Class 2 design changes occurring after the internal events PSA was developed to provide a comparison of the fire PSA with the UK GDA design reference point.

6. The following itemised scope of technical work summarises all the individual actions within the resolution plan. Westinghouse has submitted work to address each of these items:

- a methodology guidebook;

- detailed information on the databases developed to support the fire PSA - for example, the list of fire PSA components and equipment failure modes, cable selection and routeing, the physical characteristics of the fire compartments and their inventories, barriers and penetrations, ignition sources, transient combustibles;

- clarity on the modifications to the internal events PSA model required to support the development of the Fire PSA;
- a qualitative and/or quantitative screening analysis of fire compartments;
- a thorough evaluation of hot shorts and multiple spurious actuations;
- an evaluation of fire frequencies;
- fire progression event trees (or equivalent) for all compartments not screened out, and comprehensive consideration of the fire scenarios;
- fire modelling as required;
- evaluation of the reliability of the fire protection measures claimed including human reliability analyses as appropriate;
- fire progression event trees for all relevant multi-compartment fires;
- a fire analysis for the main control room;
- a documented fire PSA model in CAFTA together with the results of the core damage frequency and large release frequency evaluations;
- an ALARP analysis using the fire PSA;
- a Living PSA procedure to allow the fire PSA to be updated as further design information becomes available;
- comprehensive documentation.

7. This scope of work was designed to ensure that the fire PSA adequately represents the AP1000 plant design for the GDA close-out phase, provides an adequate understanding of the risk from fires for an AP1000 plant operating on a generic site, and generates risk insights to inform the development of the design and ALARP analysis.

8. The scope of my assessment work is described in my assessment strategy in Section 4.1 of this report.

1.3 Method

9. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 3).

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 sampling strategy for this assessment was proportionate provided that the sample included review for each of the main technical areas needed to produce a fire PSA. A good understanding of each main technical area of the fire PSA would then enable me to assemble an overall view and then make a judgement on the adequacy of the fire PSA. The technical areas I sampled were chosen from the PSA standards against which the PSA was constructed and the ONR standard for the assessment of PSAs (Refs 4, 6 and 10). Section 4.1 provides further discussion on the scope of my technical sampling strategy.

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report

11. ONR's GDA Guidance to Requesting Parties (www.onr.org.uk/new-reactors/ngn03.pdf) states that the information required for GDA may be in the form of a Pre-Construction Safety Report (PCSR), and Technical Assessment Guide (TAG) 051 sets out the regulatory expectations for a PCSR (www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf) (Refs 11 and 12).

12. At the end of Step 4, ONR and the Environment Agency raised GDA Issue CC-02 (www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf) requiring that Westinghouse submits a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the AP1000 Design Reference Point (DRP) (Ref. 13).

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 focuses on the supporting documents and evidence specific to GDA Issue GI-AP1000-PSA-02 (Fire PSA).

2.2 Standards and Criteria

14. The standards and criteria adopted within this assessment are principally the SAPs (Ref. 14), the internal TAG on PSA (Ref. 10), relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites.

15. For the GDA close-out work Westinghouse has presented numerical measures of core damage frequency and large release frequency. These do not compare directly with ONR numerical targets because Westinghouse has not addressed radiological dose to workers or the public. I agreed with Westinghouse at the start of the closure phase of this work that dose assessments would be undertaken during the licensing phase. This is because the close-out work is an extension of the GDA Step 4 work in which the risk measures of core damage frequency and large release frequency were considered adequate to understand the risk from a generic plant. Dose assessments require site-specific information on workers and the population distribution around the site.

16. The discussion of PSA results presented by Westinghouse for comparison with numerical standards compares the core damage frequency with ONR numerical target 8. Target 8 is for the total predicted frequency of accidents on an individual facility which would give doses to a person off the site. The comparisons presented by Westinghouse are against the most limiting frequency which is the Basic Safety Objective (BSO) of 10^{-6}/year for an off-site dose greater than 1000 mSv. The frequency with which a radiological dose would be received off-site may be lower than the core damage frequency due to the mitigating effects of containment.

17. The predicted frequency of a large release from the PSA can be compared with the ONR 'societal risk' target 9. Target 9 is the frequency of 100 or more fatalities from all accidents at the site. The frequency of 100 or more fatalities may be smaller than the large release frequency because of atmospheric dispersion and other effects which influence dose uptake.

2.2.1 Safety Assessment Principles

18. The key SAPs applied within my assessment are set out in Table 1 at the end of this report.

2.2.2 Technical Assessment Guides

19. The TAG most relevant to the fire PSA that I have used for this assessment is that specifically designed for PSA (Ref. 10).

2.2.3 National and international standards and guidance

20. The international and ONR standards and guidance that I have used for my assessment are primarily the ONR SAPs and the TAG 030 on PSA. Other standards that represent relevant good practice for nuclear reactor PSA are those from the International Atomic Energy Agency (IAEA) (Refs 15, 16 and 17), reference levels from the Western European Nuclear Regulators' Association (WENRA) (Ref. 18) and the United States Nuclear Regulatory Commission (US NRC) guidance on fire PSAs. The SAPs, IAEA standards and WENRA reference levels are embodied and enlarged in ONR's TAG on PSA (Ref. 10) and it is this guide that provides the principal means for assessing the PSA in practice.

21. The US NRC guidance documents are NUREG/CR-6850 (Ref. 4) and the NUREG/CR-6850 supplements (Ref. 5). The American Society of Mechanical Engineers and the American Nuclear Society standards on fire PSAs have also been used. These are ASME/ANS RA-Sa-2009 and Regulatory Guide 1.200 Revision 2 (Refs 6 and 7 respectively). Westinghouse has applied these guidance and standards to the extent achievable by a pre-operational plant with limited spatial data available.

2.3 Use of Technical Support Contractors

22. It is usual in GDA for ONR to use Technical Support Contractors (TSCs), for example to provide additional capacity to optimise the assessment process, to enable access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision-making.

23. For this project technical support was required to share the detailed technical review workload, to provide high-quality expertise for the broad range of specialised and diverse technical subjects needed for a fire PSA, to 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 consultants Jacobsen-Analytics was chosen based on a competitive tendering process. Jacobsen-Analytics was supported by the US based consultants Engineering Planning and Management (EPM) for very specialised tasks.

2.4 Integration with Other Assessment Topics

24. 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. I have considered the following cross-cutting areas within my assessment:

- the performance of the plant operators during a fire - advice from the ONR human factors inspector was incorporated into my assessment; and
- the withstand to fire of compartment barriers and penetrations - advice from the ONR internal hazards inspector was incorporated into my assessment.

2.5 Out of Scope Items

25. The Step 4 GDA assessment report (Ref. 1) programmed the resolution of the assessment findings from Step 4 into the programme for the PSA as part of normal regulatory business. The resolution of these assessment findings was not included in

the resolution plan for this GDA issue and is therefore outside the scope of this assessment.

3 REQUESTING PARTY'S SAFETY CASE

26. Westinghouse has provided a fire PSA developed to meet the requirements of NUREG/CR-6850 (Ref. 4), ASME/ANS RA-Sa-2009 (Ref. 6) and Regulatory Guide 1.200 Revision 2 (Ref. 7). The fire PSA has been developed to the extent achievable by a pre-operational plant with limited spatial data available. When compared with the GDA Step 4 fire PSA, the submission for the close-out phase is essentially a new fire PSA included in these documents Refs 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43 and 44).

27. Westinghouse states that the scope of the fire PSA includes all credible fire sources and unscreened fire compartments within the global plant analysis boundary (Ref. 20). It includes initiating events that can arise due to fire-induced failures of safety equipment, random failures of safety equipment, and the operators' response to fires. The scope is limited to initiating events which occur when the reactor is operating at full power. The fire PSA includes both a Level 1 and Level 2 analysis. An ALARP analysis has been provided by Westinghouse to support the fire PSA.

28. The design reference point upon which the fire PSA is based uses the most recently approved revisions of the plant design at 1 September 2010. The cable routeing uses an electrical design freeze date of February 2015. The fire PSA also accounts for unincorporated Design Change Proposals (DCPs) approved before 1 September 2010. This provides a qualitative analysis of the design changes occurring after the internal events PSA was developed to provide a comparison with the UK GDA design reference point.

29. 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 following a fire: in particular the control of reactivity and the provision of decay heat removal. 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 a fire-induced fault sequence resulting in core damage. Failure of the containment can give rise to a release of fission products to the environment.

30. The output from the PSA is the core damage frequency, the large release frequency, and various importance measures. Analysis of the results has been performed using importance analysis and sensitivity studies, in order to understand the effectiveness of the safety systems and operator responses, and to present the dominant contributors to risk.

31. The fire PSA is modelled and quantified using CAFTA (version 6.0) and FRANX (version 4.2) software for both the Level 1 and Level 2 PSA. This suite of software has been developed by the Electric Power Research Institute (EPRI) and is a widely used method for the construction and evaluation of fire PSAs.

32. 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 fire PSA explores the defence-in-depth provided should the design basis claims fail to be met.

33. The fire PSA claims five modes of decay heat removal for the reactor plant, both passive and active depending on 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 (Ref. 33).

34. Westinghouse discusses further the overall PSA results in Chapter 10 of the PCSR (Ref. 45) 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 ALARP. The discussion in the PCSR applies to the broader-scope PSA and not just to the fire PSA. However, the fire PSA makes a contribution to the overall position stated by Westinghouse in the PCSR.

35. Westinghouse states that the core damage frequency and large release frequency are generally comparable with industry data for plants of similar design (Ref. 45: Chapter 10). However, given the scarcity of fire PSAs for advanced passive plants, no similar passive designs are available for comparison purposes. Westinghouse expects the core damage frequency and large release frequency from the fire PSA to be lower than typical Pressurised Water Reactor (PWR) plants. This is due to the unique passive safety systems and the defence-in-depth capabilities of the design. Westinghouse claims that the fire PSA demonstrates that the fire risk associated with advanced passive plants is lower than the fire risk for typical operating PWR plants.

36. In the PCSR (Ref. 45: Chapter 10) Westinghouse compared 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.*

ONR Numerical Target 8 Dose > 1000 mSv	Fire PSA Claims	
	Core Damage Frequency	Large Release Frequency
BSL 10^{-4}/year	6.7×10^{-7}/year	5.6×10^{-8}/year
BSL 10^{-6}/year		

37. Westinghouse states that the ALARP analysis provides a systematic process for reviewing the fire PSA for potential improvements to ensure that risks are ALARP (Ref. 38). Westinghouse states that given the AP1000 plant at-power fire PSA contribution to overall plant risk is less than the BSO for ONR target 8, only changes with small plant impacts where the risk benefit outweighed the cost were considered as ALARP.

38. The ALARP analysis undertaken by Westinghouse identified the following potential enhancements:

- reducing common mode failures between the Protection and Safety Monitoring System (PMS) and Plant Control System (PLS);
- using automatic actuation of the hydrogen igniters;
- additional fire detection and suppression in the division C Reactor Coolant Pump (RCP) switchgear room and security room; and
- cable routeing improvements: 1) separation of Diverse Actuation System (DAS) cables in the division C RCP switchgear room, 2) providing separation of the cable routing to reduce the consequences of a fire in the lower Automatic Depressurisation System (ADS) valve area, 3) ensure that the Offsite Retail

* *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.*

Power System (ZRS) cables which support the secondary-side heat removal systems are not located in the security room with the DAS cabinets, 4) separation of the hydrogen igniter power supplies, 5) optimising the cable design for the ADS stage 1 to 3 valves to further reduce the likelihood of spurious actuations.

39. Following the ALARP analysis, Westinghouse made the following ALARP recommendations:

- diversify the manual cue for actuating the hydrogen igniters;
- remove one DAS power supply from the RCP switchgear room; and
- ensure that the ZRS power supply is not routed through the security room.

These will be taken for further investigation during site licensing through the Westinghouse Design Change Proposal (DCP) process.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-PSA-02

40. I have carried out this assessment in accordance with the HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 46).

4.1 Scope of Assessment Undertaken

41. The primary aim of my assessment was to judge whether PSA-02 is adequately addressed and can be closed.

42. To judge this required gaining an appropriate level of confidence that:

- the internal fire risk model addresses the PSA-02 resolution plan;
- the internal fire risk model has been produced to an adequate technical standard (SAP FA.13);
- the internal fire risk model is an adequate plant specific representation of the generic AP1000 design (SAP FA.11);
- the internal fire risk model provides an adequate understanding of the risk from operating the AP1000 plant at a generic site (SAP FA.12); and
- the internal fire PSA confirms and / or adds to the insights into the plant risks highlighted at Step 4, and supports the view that risks are being managed ALARP as the AP1000 design process continues (SAPs FA.10 and FA.14).

Where I have identified shortfalls in the PSA, I have undertaken a risk gap analysis where practicable to understand the risk significance of these.

43. A further aim of my assessment was to identify assessment findings, should they be required. These will be addressed during the licensing phase.

44. When compared with the PSA assessed by ONR at GDA Step 4 the internal fire PSA is a substantially updated risk model with new supporting fire analysis and human factors analysis.

45. On receipt of the internal fire PSA documentation from Westinghouse, I undertook a preliminary high-level review to produce the following technical assessment strategy:

1) Gain confidence in the overall construction, completeness and logical modelling used in the internal fire PSA, and whether these conform to modern standards.

This will address the Step 4 deficiency regarding “use of a screening method that included various conservatisms and optimisms”, noting that the risk model represents substantially revised analysis. I considered that a sampling approach was proportionate provided that the sample included a selective review for each of the main technical areas needed to produce a fire PSA. These technical areas were chosen from the NUREG/CR-6850 guidance and the ASME/ANS RA-Sa-2009 fire PSA standard (Refs 4 and 6). This confidence would be gained by assessing the following technical areas against the ONR technical assessment guide on PSA (Ref. 10), in particular Table A1-2.7.2 of the guide which addresses the analysis of internal fire:

- the methodology guidebook used by Westinghouse for developing the fire risk model (Subsection 4.2.1);
- plant partitioning and fire equipment selection (Subsection 4.2.2);
- fire initiating event frequencies (Subsection 4.2.5);
- fire cable analysis and fire circuit failure mode likelihood analysis (Subsection 4.2.6);
- supporting fire analysis (fire scenario selection, detailed fire modelling targets, fire modelling spreadsheet, fire database) (Subsection 4.2.7);

- the Main Control Room (MCR) analysis and supporting CFAST work (Subsection 4.2.9);
- the identification and incorporation of human failure events into the PSA (Subsection 4.2.9);
- accident sequences for fire, including representation of consequential events (fire risk model notebook, FRANX file, CAFTA fault tree and database) (Subsection 4.2.11);
- the adequacy of the data used in the fire PSA (Subsections 4.2.10 and 4.2.11), and the integration of the fire PSA into the Level 2 PSA (Subsection 4.2.12).

46. Assessment of the cable analysis and fire circuit failure mode likelihood analysis was undertaken at Westinghouse's Cranberry offices in the US. This is because samples of detailed circuit design information are needed to undertake a meaningful assessment. This detailed information was readily available in Cranberry and not necessarily in the main PSA reports provided by Westinghouse.

2) Gain confidence in the dominant contributors to risk. This work addressed as a minimum the following items:

   - the risk model quantification and risk results (quantification notebook, CAFTA files, top core damage frequency and large release frequency cutsets);
   - the sensitivity studies, uncertainty analysis, the insights and conclusions presented by Westinghouse;
   - the gap analysis presented by Westinghouse to understand the risk implications of any design changes to the plant since the design reference point for the PSA.

3) Understand the contribution of the fire PSA to demonstrating that risk is ALARP. The following assessment work supported this task:

   - Review of the fire hazard analysis and fire compartments to identify the potential for redundant equipment and defence-in-depth to be compromised by a fire in a single compartment or area. I focussed on the novel areas of the AP1000 design, particularly the equipment needed to actuate the passive safety systems.
   - I then supplemented this by considering the risk-dominant compartments from the fire PSA, ONR's understanding of relevant good practice and Westinghouse's fire ALARP analysis.

47. I have co-ordinated assessment of the human failure events in the internal fire PSA with the ONR human factors specialist inspector.

48. There is an interface with the ONR internal hazards specialist inspectors regarding the claims made on the fire barriers, fire barrier penetrations, fire dampers and the fire analysis methods used.

4.2 Assessment

4.2.1 Fire PSA Guidebook

49. I assessed the fire PSA guidebook to establish the extent to which the AP1000 plant fire PSA methodology follows relevant good practices and to identify any potential methodology deficiencies which could lead to incomplete or inadequate results at the implementation stage of the PSA (Ref. 48). The following key items were reviewed:

- the completeness and adequacy of the selected methods;
- the acceptability of the assumptions;
- the assessment of the potential implementation deficiencies.

50. My assessment of the fire PSA guidebook (RQ-AP1000-1427) and the responses from Westinghouse are recorded in Refs 8 and 9 respectively.

51. The scope and purpose of the fire PSA methodology are limited to reactor based faults when the reactor is operating critical at power. It does not provide any methodology for analysis of the fire risk during other plant operational modes or for non-reactor based faults, such as fire in the spent fuel pool, fuel route or radioactive waste treatment plants. Also, the methodology for addressing the impact of high-hazard fire sources on exposed structural building steel, and seismically induced fires is not presented in the guidebook. The SAPs (EHA.16) comments on the need to consider the hazard of fire for possible consequences to the facility structures, and the PSA TAG (Table A1-2.7.4) comments on the need for the impact of seismically induced fires to be evaluated.

52. The scope of GDA Issue GI-AP1000-PSA-02 was agreed with Westinghouse to cover the reactor at power. A full-scope fire PSA covering the shutdown operating modes and other site facilities will be provided during the licensing phase. Therefore I consider the reduced scope of the fire PSA guidebook is appropriate to address the GDA issue.

53. The scope identified in the resolution plan for GDA did not include a methodology for the treatment of exposed structural building steel and seismically induced fires during critical operations. This resulted in no analysis of these phenomena being presented in the fire PSA. However, I addressed this with RQ-AP1000-1681 (Ref. 49) for which Westinghouse provided responses that are discussed below in Section 4.2.8.

54. I consider that a minor shortfall is appropriate to record the need for a broader scope of fire PSA guidebook for the site-licensing phase:

> **Minor Shortfall** (CP-MS-AP1000-PSA02-01): The licensee shall expand the scope of the fire PSA guidebook to include methodology for fire risk for all plant operational modes, and for non-reactor-based facilities on the site. This should also include the methodology for addressing the impact of high-hazard fire sources on exposed structural building steel, and seismically induced fires.

4.2.2 Plant Partitioning and Equipment Selection

55. The plant partitioning process first defines the global plant analysis boundary for the fire PSA. This is the boundary within which all the encompassing areas of the plant are assessed qualitatively or quantitatively by the fire PSA. The areas of the plant outside the global plant analysis boundary are not considered within the fire PSA.

56. The global plant analysis boundary is then subdivided into fire areas or fire compartments such that there is a high degree of confidence that fires originating within the area or compartment will remain confined within it. Fire risk is then assessed for each fire area or compartment by the fire PSA. The plant partitioning process is presented in Ref. 20.

57. The process of equipment selection identifies all the plant components and failure modes to be included in the fire PSA (Ref. 21). This includes equipment that can cause an initiating event, equipment that supports the mitigation of a fire-induced initiating event, or equipment the failure of which can compromise the response of the plant or operators.

58. My assessment of the plant partitioning and equipment selection analysis focused on the adequacy of the approach taken by Westinghouse with respect to relevant good practice within the industry PSA standards and ONR TAG030 (Ref. 10). The key topics for my assessment are listed below:

- the adequacy of the global plant analysis boundary definition;
- the justification of the selected boundaries;
- the basis and comprehensiveness of equipment selection;
- the appropriate selection of fire initiating events;
- the analysis of the potential fire-induced interfacing systems loss of coolant accidents;
- the completeness of the documentation.

59. My assessment concluded that the global plant analysis boundary was appropriately defined to avoid inadvertently screening plant areas that may contribute to the site fire risk. The selection of plant equipment for the fire PSA was also done in an adequately comprehensive manner. I raised a number of clarifications regarding more detailed aspects of the analysis presented by Westinghouse. I presented these in RQ-AP1000-1475 (Ref. 51).

60. The majority of the responses provided by Westinghouse give sufficient clarification to resolve the comments (Ref. 52). However, sufficient clarification was not provided by Westinghouse for a small number of questions. These are summarised below in Sections 4.2.3 and 4.2.4.

4.2.3 Global Plant Analysis Boundary

61. A number of the plant fire areas defined within the global plant analysis boundary have not been defined as fire compartments. Several of these, including the switchyard and the cooling tower, which I consider to be relevant to the fire risk, are described as site-specific, rather than generic equipment (Ref. 20 Appendix C, note 3). I asked Westinghouse to clarify which of the fire areas will be considered within the scope of the fire PSA.

62. Westinghouse stated that the switchyard area includes any other areas not explicitly documented as a separate fire compartment. However, Westinghouse did not provide the list of areas and compartments encompassed within the switchyard area as requested. I consider this to be an aspect of modelling completeness but judge that it is unlikely to be significant within the fire PSA. This is recorded as a minor shortfall.

> **Minor Shortfall** (CP-MS-AP1000-PSA02-02)**:** A number of the plant fire areas defined within the global plant analysis boundary have not been designated as fire compartments. Clarification of which of the fire areas identified in Table 7.1-1 (Ref. 20) should be considered within the scope of the fire PSA (RQ-AP1000-1475, comment 7).

4.2.4 Switchyard and Cable Tunnels

63. I requested Westinghouse to clarify how the Switchyard area is modelled within the fire PSA. Westinghouse clarified that the fires in the yard are assumed to damage all cables or components located in the area above the ground. The cable tunnels running underneath the yard are treated as separate fire compartments. The fire risk in the yard is driven by loss of offsite power sequences caused by fire-induced failure of the station transformers. I consider this approach to be generally acceptable but it requires additional analysis to confirm the absence of any pathways that can allow liquid combustible materials to leak to the underground tunnels. This is recorded as an

assessment finding as it could influence the frequency of a loss of offsite power or loss of site heatsink:

> **Assessment Finding** (CP-AF-AP1000-PSA02-01)**:** The licensee shall undertake analysis of the pathways for liquid combustible materials to leak into underground tunnels, and the potential implications for the fire PSA (RQ-AP1000-1475, comment 8).

4.2.5 Fire Initiating Events

Use of the Most Recent Fire Frequency Data

64. I noted that Westinghouse had not updated the fire initiating event frequencies with the latest data from plant operational experience within RQ-AP1000-1475 (Ref. 51 comment 25). Subsequently Westinghouse has updated the fire initiating event frequencies in accordance with NUREG-2169 (Ref. 75) and reissued the document (Ref.44).

65. I also requested Westinghouse to clarify whether it had carried out the update to NUREG-2169 using both the revised methodology and the revised fire frequency data. Westinghouse clarified that while it used NUREG-2169 as the source of the updated generic ignition frequency distributions, the methodology to implement the ignition frequencies was unchanged from Task 6 of NUREG/CR-6850 (Ref. 4).

66. I advised that there have been several updates concerning the implementation of the generic ignition frequencies since NUREG/CR-6850 was originally published. The topic of fire ignition frequencies had the highest number of National Fire Protection Association (NFPA) 805 frequently asked questions, and both the initiating event frequency methodology and EPRI's fire events database have been updated several times since 2005. I provided a table in RQ-AP1000-1475 (Ref. 51) which shows the list of NFPA 805 frequently asked questions for Westinghouse's consideration.

67. Changes in the fire initiating event frequencies have a directly proportional effect on the numerical evaluation of the overall plant fire risk. However, because Westinghouse has updated the fire initiating event frequency data, I am satisfied that the overall fire frequency used in the PSA is of the appropriate order of magnitude and consistent with the latest operational plant experience. Therefore I consider that improving the detailed methodology can be recorded as a minor shortfall.

> **Minor Shortfall** (CP-MS-AP1000-PSA02-03): The generic fire ignition frequencies used in the analysis are based on NUREG-2169. The relevant NFPA 805 PRA Update FAQs related to Task 6 should be followed to ensure the latest methodology is applied. For example, the counting guidance for certain bins (RQ-1652, comment 9).

Apportioning the Fire Ignition Frequency Between Areas/Compartments

68. The pre-operational design of the plant means that not all of the plant equipment has been allocated to a particular compartment. Therefore Westinghouse defined a generic fire compartment within which to include this equipment. This was compartment 2000AF01, which is in the turbine building.

69. When the fire frequency contribution from this equipment in the turbine building was summed, the fire compartment ignition frequency was comparable to the frequency of all the other fire compartments combined. I recommended that Westinghouse use generic historical data and test the hypothesis of whether or not almost half of the challenging fires in the plant will start in this compartment.

70. In its review of the fire frequency analysis Westinghouse revisited this item and stated that the equipment identified for the generic compartment will be located within the turbine building. Therefore, the process used is consistent with the pre-operational design of the plant.

71. However, I noted that there are 900 fixed ignition sources in the turbine building fire area 2000AF01. The cumulative ignition frequency from fixed ignition sources of $5.2x10^{-2}$/year is considered relatively very high for the turbine building fire area, and the fire compartment 2030AF20300 within the turbine building contains more than one-third of these sources. Westinghouse plans to incorporate detailed as-built design information into the PSA during site licensing. I consider that further review is then needed to justify that that an appropriate fire initiation frequency is used, and clarification provided of how the apportionment of the fire frequency throughout the plant has been carried out. The contribution of the turbine building to the overall plant core damage frequency is approximately 7% (Ref. 33). This is relatively small and therefore I am content for this item to be recorded as a minor shortfall.

> **Minor Shortfall (**CP-MS-AP1000-PSA02-04): The ignition frequency of the generic fire compartment 2030AF20300/2000AF01 appears relatively very high with respect to other compartments. Once as-built design information is incorporated, justification should be developed to demonstrate that an appropriate fire frequency has been used. Clarification should be presented of how apportionment of the fire frequency throughout the plant has been carried out (RQ-1475, comment 21).

4.2.6 Cable Analysis

72. This section describes my assessment of the cable analysis within the fire PSA. The cable analysis includes the following tasks:

- Construct a list of cables linked to all the plant components that are relevant to the fire PSA. This must cover the cables that could affect the proper operation of the equipment to compromise safe shutdown, or cause spurious operation of the equipment if the cables are damaged by fire - for example, power supply, control, instrumentation, interlock, and equipment status indication cables.

- Compile the information needed to identify the location on the plant of the cables and the associated equipment.

- Identify the failure modes of the equipment following cable damage by fire, and the probabilities that the failure modes occur.

- Identify the impact of multiple spurious operation scenarios, in which cables damaged by a common fire could result in two or more components being subject to spurious operations.

73. This work is presented in the fire PSA cable notebook, the fire PSA circuit analysis and cable selection notebook, the circuit failure mode likelihood analysis, and the expert panel multiple spurious operations analysis (Refs 41, 27, 30 and 53 respectively). The assessment of this work was done within the UK and also within the Westinghouse Cranberry offices in the USA. During the latter the more detailed circuit design documentation was sampled and included cable tray arrangements.

74. My assessment is contained in RQ-AP1000-1736 (Ref. 54: comments 36 to 50) and was focussed on the following key topics:

  - the appropriateness of the cable selection process;

- single and multiple spurious operations modelling;
- circuit failure mode likelihood analysis;
- the modelling of hot short duration probability;
- the implementation of the circuit failure probability in the FRANX PSA software.

75. Westinghouse addressed my comments satisfactorily and I conclude that this aspect of the analysis is generally adequate (Ref. 76). However, the following assessment comment merits further discussion.

Spurious Actuation of the Recirculation Squib Valves due to a Fire

76. The expert panel analysis considered that a fire damaging cables for the containment sump recirculation squib valves could spuriously actuate one or more of the four valves (Ref. 53). A spurious actuation would cause the water in the In-Containment Refuelling Water Storage Tank (IRWST) to drain into the containment sump resulting in an unnecessary demand on passive recirculation. Two of the four drain lines contain non-return valves which would prevent drain down, but a fire-related drain down could occur through the other two. Motor-operated isolation valves can be closed by operator action to stop the drain down following a spurious opening of these two valves.

77. The Westinghouse response to RQ-AP1000-1736 (Ref. 54: comment 42) and the multiple spurious operations expert panel report (Ref. 53) stated that the arm and fire circuitry for the squib valves are routed in low-voltage trays where short circuits cannot provide enough power to actuate them. Westinghouse also stated that multiple failures would be required to energise both the arm and fire circuits to actuate the squib valve igniter to open the valve. Westinghouse has confirmed that this potential fire-induced failure mode has been included in the fire PSA.

78. Westinghouse provided additional information which states that the design intent is to separate the squib valve igniter circuit cables from other cables which could present a sufficient fault current (Ref. 55: Table 2.1-2 note 13). Confirmation of the as build design will not be available until the location of the cable trays is decided during licensing. The PMS that actuates the squib valves has a blocker provided so that the frequency of a spurious PMS actuation signal and blocker failure is very small ($<10^{-6}$/year). Because this initiating event frequency is so low, the risk is currently assessed in the PSA as very small. However, it is possible that the likelihood of a fire induced spurious actuation may be of comparable or higher frequency, depending upon the detailed design. I consider that the technical basis of the claim needs clarification during licensing to confirm the overall contribution to risk from spurious squib valve actuation.

> **Assessment Finding** (CP-AF-AP1000-PSA02-02): The licensee shall justify the claim that a low voltage tray hot short cannot provide enough power to actuate the as-built squib valves.

4.2.7 Supporting Fire Analysis

79. My assessment of the supporting fire analysis consists of two parts. The first part is discussed in this section of my report and addresses the detailed fire modelling for which my assessment is presented in RQ-AP1000-1736 and RQ-AP1000-1718 (Refs 54 and 61). The second part addresses the impacts on any exposed structural steel, and the analysis of seismically induced fires (Subsection 4.2.8).

80. The supporting fire analysis is presented by Westinghouse in Refs 23 and 33 and includes the following topics:

- the identification and characterisation of the ignition sources;
- the identification and characterisation of the secondary combustibles;
- the fire growth and propagation analysis;
- the fire detection and suppression analysis;
- the development of the fire scenario definitions;
- the exporting of the fire scenario information to the FRANX computer code.

My assessment findings are discussed below.

The Modelling of Temperature-Sensitive Equipment

81. Relevant good practice for a fire PSA is to evaluate the upper and lower hot gas layer impact on any sensitive electronic components. Westinghouse's work is primarily focussed on cabling to fire-significant equipment. The response by Westinghouse to my questions identified the PMS cabinets as containing temperature-sensitive equipment but did not provide any information to indicate that potential fire impact was analysed. Given that the damage criterion for sensitive electronics is 65°C which is significantly lower than the damage criterion for cables at 330°C, and the high potential of such fire damage to cause spurious actuations, I consider that this omission may result in an incomplete and potentially optimistic evaluation of the plant fire risk.

82. However, the overall plant fire risk is currently demonstrated to be very small and within ONR numerical targets. In addition, the risk sensitivity to reducing the PMS reliability is understood within the assessment of GDA Issue GI-AP1000-PSA-01 (Ref. 56), and it does not compromise an adequate understanding of the plant risk for GDA. I consider that an assessment finding that can be addressed during the licensing phase is adequate for addressing this shortfall. This is recorded as assessment finding CP-AF-AP1000-PSA02-03 at the end of this subsection.

Cable Tray Fires

83. My assessment showed that fire spread along vertical sections of cable trays or vertical cable trays was not evaluated with the appropriate flame spread rate according to the tray orientation (Ref. 57). This may underestimate the heat release rate from the cable trays.

84. The response from Westinghouse to RQ-AP1000-1718 (Ref. 64) clarified that the FLASH-CAT (Flame Spread over Horizontal Cable Trays) code was used for the calculation of the cable tray heat release rate profile (NUREG/CR-7010 Ref. 58). This is an accepted industry standard method which makes use of semi-empirical estimates of lateral and vertical flame spread.

85. The FLASH-CAT model can be used for vertical cable tray sections as long as an appropriate fire spread rate is applied, but this was not the case within the Westinghouse analysis. Generally, the heat release rate from a vertical section is much higher than a horizontal section. Therefore, if the burning rate is not adjusted for the vertical sections, the total heat release rate will be underestimated.

86. Westinghouse stated in its response to RQ-AP1000-1718 (Ref. 64) that a small subset of trays for an AP1000 plant are vertically orientated, and that there are few instances where vertical trays travel a greater distance in the room than horizontal trays. I noted this mitigating argument. However, I consider that this shortfall needs to be reviewed, and the cable tray design is likely to evolve during the detailed design. This is recorded with assessment finding CP-AF-AP1000-PSA02-03 at the end of this subsection.

Fire Duration Calculations

87. The fire duration calculation for cable trays follows the relevant good practice presented in NUREG/CR-7010 (Ref. 58). I consider this to be an acceptable method. However, the input parameters selected by Westinghouse are plant average values. This simplification is likely to be conservative for the cable trays with low cable loading, but can be a significant underestimate of the heat release rate for the cable trays with high loadings. My assessment presented a list of specific discrepancies based on spot checks of plant drawings. For example, the 'T' intersections of the cable trays are modelled as fire spreading in two directions only, rather than three; the average mass per unit length and average plastic fraction used in the analysis appears to be different from the values I estimated from the drawings.

88. The response from Westinghouse agreed to improve the cable tray fire modelling methodology in further revisions of the fire PSA. Westinghouse also included some risk sensitivity studies showing an increase in core damage frequency of up to 9%. This is not large given the small overall core damage frequency from fires demonstrated by Westinghouse. I consider that this shortfall should be addressed and this recorded with assessment finding CP-AF-AP1000-PSA02-03 at the end of this subsection.

Fire Zone of Influence Definition

89. A sample review of reference drawings and the fire scenarios modelled highlighted an inconsistency between the number of vertical sections on the drawing for the maintenance floor (north) and the number developed within the detailed fire scenarios. The response from Westinghouse acknowledged that a different input data set was used for the fire ignition frequency task and the later detailed fire modelling due to the changing locations of cabinets as the design developed. I consider that the list of fire scenarios supporting the fire PSA is not demonstrably complete, but this type of design development is not unexpected at GDA. I am recording this as an assessment finding to ensure that it is tracked and addressed in later updates of the fire PSA. This is recorded with assessment finding CP-AF-AP1000-PSA02-03 at the end of this subsection.

90. The zone of influence for the maintenance floor (north) compartments 1100AF11300B-IS5 and 1100AF11300B-IS2 appears to be the same size even though a fire in the latter can spread to secondary combustibles. The response from Westinghouse stated that the zone of influence for all fixed ignition sources was calculated on the 98-th percentile of the peak heat release rate distribution, regardless of the possibility of the fire to ignite any secondary combustibles.

91. This approach does not correspond to accepted fire modelling practices and does not allow the analyst to define fire damage states based on the potential of fire damage to spread. Instead it generates generic fire damage information which does not correspond to the actual location of the fire equipment targets. This is recorded with assessment finding CP-AF-AP1000-PSA02-03 at the end of this subsection.

Conditional Core Damage Probability 'Floor' Value

92. Assessment of the fire scenario selection notebook found that a conditional core damage probability 'floor' value of 1.0×10^{-8} was used for all fire scenarios where the fire damage is limited to the ignition source itself. Applying a fixed conditional core damage probability to all 'source only' fires is optimistic in the cases where the ignition source is itself a PSA target - for example, items such as motor control centres or switchgear where relevant good practice assumes all components in the source cabinet to be considered to be failed by smoke.

93. The response from Westinghouse stated that the source-only fire scenarios will be evaluated during development of the site-licensing PSA. Westinghouse also stated that implementing this update is expected to increase the conditional core damage probabilities for ignition sources that contain risk-significant cables; however, the conditional core damage probabilities are expected to decrease for ignition sources that do not contain risk-significant cables. This is because the 1.0×10^{-8}/year floor value would no longer be used in the update.

94. Westinghouse stated that 'source only' scenarios are not currently quantified in the fire PSA (Ref. 33 assumption no 2). An estimate of the risk from source-only scenarios has been done by combining a realistic fire initiating frequency for individual components at 10^{-2}/year to 10^{-3}/year (Ref. 44) with the conditional core damage probability of 1.0×10^{-8}. The resulting core damage frequency from a single source-only scenario is very small. Many components would need to be classified as source-only scenarios for the overall core damage frequency from fires to be adversely affected. I consider the understanding of the risk to be sufficient for the purposes of GDA. However, source-only fire scenarios should be specifically assessed during licensing. This is recorded with assessment finding CP-AF-AP1000-PSA02-03 immediately below.

> **Assessment Finding for Supporting Fire Analysis** (CP-AF-AP1000-PSA02-03): The licensee shall carry out the following aspects of the supporting fire analysis in accordance with the NUREG guidance and the ASME/ANS PSA standard:
>
> 1) Include a hot gas layer impact analysis on sensitive electronics and include this within the fire scenario analysis and the fire PSA (RQ-AP1000-1736, comment 3).
> 2) Evaluate fire spread along vertical cable trays in accordance with the accepted industry practices (RQ-AP1000-1718, comment 6; and RQ-AP1000-1736, comment 10).
> 3) Revise the fire duration and heat release rate analysis for cable tray fires to meet relevant good practice, and use data from the actual plant design (RQ-AP1000-1736, comment 11).
> 4) Develop fire scenarios for the maintenance floor (north) (compartment 1100AF11300B) and review other fire compartments to ensure appropriate completeness of fire scenarios (RQ-AP1000-1736, comment 12).
> 5) Ensure that the zone of influence calculations takes into account the heat release rate contribution from secondary combustibles (RQ-AP1000-1736, comment 13).
> 6) Evaluate the 'source only' fire scenarios (RQ-AP1000-1736, comment 20).

4.2.8 Assessment of Exposed Structural Steel from Fires

95. I raised RQ-AP1000-1681 to address assessment comments on the fire scenarios selected by Westinghouse for analysis. This included a request for:

1) Westinghouse to follow the analysis steps in the ASME standard for exposed structural steel and describe the findings using the currently available design information (Ref. 6);

2) A bounding estimate of the risk for collapse of the turbine building due to fire damage to its structure; and

3) A bounding estimate of risk for collapse of the turbine building onto another adjacent building, due to fire damage to the turbine building structure.

The response from Westinghouse is presented in Ref. 47.

Potential High Hazard Site Locations

96. For item 1 above, Westinghouse has not undertaken a full review in accordance with the standard. However, Westinghouse reviewed the site buildings to identify five locations with a potentially high fire hazard. These are within the turbine building, the annex building and the diesel generator building.

97. None of these buildings contains any safety systems claimed within the design basis analysis: those that represent the minimum set of safety equipment justified to provide safe shutdown for the plant following a fire.

98. The analysis of exposed structural steel and potential fire-proofing is not yet complete. However, Westinghouse stated that its design intent is that structural steel members will be designed such that the effects of plant fires do not jeopardise structural support, and that fireproofing of structural steel is not required where a realistic fire analysis demonstrates this.

99. I consider that Westinghouse has identified the areas of the site most relevant to fire effects on exposed structural steel. However, it would enhance the justification if the standard was applied fully. This is recorded as a minor shortfall.

> **Minor Shortfall** (CP-MS-AP1000-PSA02-05): The analysis steps in the ASME standard for exposed structural steel should be followed to inform the design (RQ-AP1000-1681, question no 6).

Turbine Building Collapse

100. For item 2 above, Westinghouse has derived a frequency for an unsuppressed turbine building fire of 2.6×10^{-4}/year. This is based on NUREG-2169 (Ref. 75) data for the frequency of fires in turbine buildings at nuclear plants, and an estimate of the likelihood of automatic suppression and the fire brigade failing to control the fire. I consider this estimate to be reasonable because it is consistent with my experience of fire frequency and fire suppression data, and similar in magnitude to assessments for other nuclear power plant sites. Westinghouse presented a conditional core damage probability of 2×10^{-4} in the event of an uncontrolled turbine building fire. The resulting core damage frequency is of the order 5×10^{-8}/year. I consider this estimate to be very small and could possibly be justified as smaller with refinement.

Turbine Building Collapse onto an Adjacent Building

101. Westinghouse has not provided a bounding risk estimate for collapse of the turbine building onto an adjacent building (item 3 above). Westinghouse stated that it will be bounded by the estimate of turbine building collapse. This is based on a Westinghouse statement that the turbine building is separated from adjacent structures by a three-hour fire barrier which will maintain its structural integrity in the event of a complete collapse of the turbine building.

102. I consider that the three-hour fire rating of the adjacent structure walls is not directly relevant. This is because the structural collapse of the turbine building will generate mechanical forces on the adjacent structural walls and this would be the greater hazard, not the fire.

103. The bounding estimate of risk is the product of the frequency of the turbine building collapse (2.6×10^{-4}/year) and the conditional core damage probability for this scenario. However, Westinghouse has not presented the latter. I consider that assuming a

conditional core damage probability of 1.0 is excessively conservative for a bounding risk estimate.

104. The generic site plan shows that the turbine building is separated from the containment / shield building by the auxiliary building. It is the containment / shield building that contains the reactor plant. The upper portion of the turbine building, which is taller than the auxiliary building, could potentially affect the containment / shield building if it collapsed, but the auxiliary building provides some separation to reduce the likelihood of this.

105. The AP1000 design considers the consequences of a large commercial aircraft impact onto the containment / shield building (Ref. 45 Section 12.8). The supporting documents claim that the aircraft impact would not inhibit core cooling capability, containment integrity, spent fuel pool integrity, adequate spent fuel cooling, or exposure of systems inside containment to aviation fuel. Westinghouse stated that this work is based on best estimate analysis and is therefore appropriate for a PSA. Having considered this information, I am able to judge that the conditional core damage probability following a turbine building collapse onto the containment / shield building will be small, and when combined with the frequency of a turbine hall fire, the bounding risk will be very small.

106. I consider that this aspect of the fire hazard analysis does not prohibit closure of GDA Issue GI-AP1000-PSA-02. However, the analysis presented by Westinghouse is not adequately developed. Therefore I have raised the following assessment finding to inform the design.

> **Assessment Finding** (CP-AF-AP1000-PSA02-04): The licensee shall analyse the risk of collapse of the turbine building due to fire onto other buildings.

Seismic-Fire Interactions

107. The resolution plan did not include a methodology for seismic-fire interactions and this was therefore not included in the guidebook. This initially led to no information being presented on this topic as outlined in the PSA standard and the ONR TAG (Table A1-2.7.4). I addressed this by raising RQ-AP1000-1681 which requested that Westinghouse go through the steps of the NUREG-6850 PSA standard and present:

1) a review of the current design information to justify its claim that seismically-induced common cause failure of multiple fire suppression systems was insignificant; and

2) a review using the current design information available to identify whether there are any ignition sources or combustibles in the plant that could start seismically induced fires.

108. Westinghouse responded by presenting a review of the steps in the standard (Ref. 47). This response addressed the seismic design criteria for the list of equipment needed for safe shutdown following an earthquake, the potential sources of seismically induced fires, storage of flammable liquids and hydrogen line design requirements, inadvertent system actuation of deluge water spray systems, inadvertent actuations of fire detectors, the fire water tanks available, the pumps, piping, valves, fire hydrants, standpipes and fire suppression systems, and the redundancy available. This was followed by the assessment of potential for common cause failure of fire suppression systems, the review of the AP1000 plant seismic response procedures and the assessment of potential seismic impacts on manual fire-fighting.

109. I consider that the information presented demonstrates that seismic-fire interaction has been analysed to an adequate extent at this pre-operational stage of the design.

There is adequate evidence that common mode failure of multiple fire suppression systems is small and that no unique seismic-fire ignition sources have been identified. I have not raised any assessment findings or minor shortfalls for this topic.

4.2.9 Main Control Room Fire Analysis

110. My assessment of the main control room fire analysis is based on the analysis presented by Westinghouse in the main control room notebook (Ref. 40) and is presented in RQ-AP1000-1652 (Ref. 59) and RQ-AP1000-1736 (Ref. 54: comments 25 to 35 respectively).

111. My assessment covered the following main technical topics:

- identification and characterisation of the ignition sources and potential secondary combustibles in the main control room;
- fire growth and propagation analysis;
- fire detection and suppression analysis;
- the main control room abandonment analysis;
- the fire scenario definitions and exporting of information to the FRANX computer code.

112. My review resulted in a significant number of assessment comments within both RQ-AP1000-1652 and RQ-AP1000-1736 (Refs 59 and 54). The majority of these comments received a sufficiently detailed response from Westinghouse to provide confidence that they are resolved (Refs 60 and 76). However, there were a few comments which were not fully resolved and these are discussed immediately below.

The Detection of Fires within the Main Control Room

113. I requested Westinghouse to provide a more robust argument to support the claim that a main control room fire will be detected within the very short time period of one minute. The initial argument presented was that the main control room was continuously manned and the presence of smoke detectors would enable the operators to be alerted.

114. Westinghouse responded by stating that all ignition sources in the MCR are within the direct line of sight of the operators with the exception of the lighting panels. If a potential fire were to occur in one of the lighting panels, Westinghouse stated that the operators would quickly identify the smoke spreading throughout the main control room. This is supported by the argument that, according to historical industry data, control room fires are extinguished, on average, within three minutes (NUREG-2169, Ref. 75).

115. I did not necessarily disagree with the argument of prompt detection, but noted that Westinghouse has not presented test data or historical data to support the claim that the actual response time, in the case of a wall-mounted lighting panel located outside the line of sight of the operator, would be less than one minute.

116. The three minute historical data argument is valid for the average response time. In addition, any deep-seated fire may take longer than a minute to detect and will be harder to extinguish with the manual fire extinguishers available in the main control room.

117. The design of the remote shutdown room takes into account the abandonment of the main control room following a fire as a design basis event. This is addressed within the assessment of GDA Issue GI-AP1000-CI-10 (Ref. 69). Also, the fire PSA results show the core damage frequency for a fire in the main control room is very small and well within ONR target 8 BSO. A small delay in detecting a main control room fire may

increase the likelihood of abandoning it to the remote shutdown room. However, I am able to judge that a delayed detection of a fire in the main control room by a few minutes would not be risk significant for the AP1000 plant risk. I consider that a minor shortfall is appropriate for the licensee to improve the justification.

> **Minor Shortfall** (CP-MS-AP1000-PSA02-06): More robust evidence to support the claim that a fire in the MCR will be detected within a very short time period, typically less than one minute, should be developed (RQ-1652, comment 7).

Fire Propagation from Transient Ignition Sources to Secondary Combustibles

118. I consider that the accepted practice for modelling main control room fires, as well as fires in any other compartment, is to include fire scenarios that can propagate to transient or fixed secondary combustibles. This also includes propagation from transient ignition sources to fixed combustibles and vice versa. This modelling is not included in the main control room fire analysis. Westinghouse stated that, in its judgement, fires inside the main control room will be promptly detected and suppressed. Westinghouse also assumes that the operators would move any mobile secondary combustibles away from the fire source and then begin prompt fire suppression activities.

119. I consider that the arguments presented by Westinghouse may be valid for some isolated cases but is not considered generally applicable for all main control room fires (Ref. 76). A more complete consideration of secondary combustibles should be included within the fire PSA. This is recorded with assessment finding CP-AF-AP1000-PSA02-05 at the end of this subsection.

Smoke Propagation into the Main Control Room

120. The main control room fire modelling report stated that a fire in the auxiliary rooms adjacent to the main control room will result in smoke propagation into the main control area (Ref. 40 Section 7.1.3.5). However the report also stated that the potential for these fires to cause main control room abandonment conditions is not credible.

121. Westinghouse in its response confirms that smoke may leak into the main control area, but the one-hour fire barrier between the rooms will remain intact (Ref. 60, comment 18). The argument is therefore based on rapid operator action to detect and control the fire in the auxiliary room, therefore preventing the spread of smoke and the main control room being abandoned. I do not consider that there is a sufficient technical basis to conclude that auxiliary room fires cannot cause main control room abandonment. This is recorded with assessment finding CP-AF-AP1000-PSA02-05 immediately below.

> **Assessment Finding** (CP-AF-AP1000-PSA02-05): The licensee shall carry out the following for the main control room fire analysis:
>
> 1) Main control room fire scenarios that can cause fire propagation to secondary combustibles, and vice-versa (RQ-AP1000-1736, comment 25)
>
> 2) Justify the likelihood of a fire in the auxiliary room causing main control room abandonment due to smoke ingress (RQ-AP1000-1652, comment 18).

4.2.10 Identification and Incorporation of Human Failure Events

122. The fire-related human reliability modelling is contained in the human reliability analysis notebook (Ref. 62). My assessment focussed on the implementation of the

fire-specific human error probabilities in the fire risk model to determine whether this was done in accordance with relevant good practice. My assessment covered the following topics:

- analysis of the operator actions during a fire;
- the human error probability calculations;
- the dependency of the human error probabilities on fire damage;
- the incorporation of human failure events into the fire risk model.

123. I limited my assessment to fire-specific operator actions. Any generic operator actions which are applicable to fires as well as to internal events at-power have been included in my assessment work for GDA Issue GI-AP1000-PSA-01 (Ref. 56).

Operator Action to Prevent Fire-Induced ADS4 Valve Actuation

124. My assessment is presented in RQ-AP1000-1718 (Ref. 61) and highlights a number of operator actions assumed on the occurrence of a fire in the PMS cabinet rooms in the auxiliary building. Westinghouse claims that if a fire occurs in a cabinet an operator can remove the power supply from adjacent cabinets in the same division before the fire spreads between the cabinets. For example, these cabinets could be the arm and fire cabinets for the ADS4 valves.

125. I consider that this modelling of operator intervention is not usual in fire PSAs and requires substantiation that the operator actions are feasible. For example, how long does it take for cable damage to occur and is there adequate time for the operators to perform the relevant actions taking into account fire propagation? Westinghouse assumes that there is a 30-minutes delay before the fire propagates from the cabinet with the fire to the cabinet that could spuriously actuate ADS4, without a reference to the modelled fire scenarios.

126. Westinghouse undertook human factors qualitative analysis of the operator tasks to support its claim. This was undertaken for GDA Issue GI-AP1000-HF-01 (Ref. 63). This analysis states that it takes 23 minutes to complete the tasks. However, Westinghouse has not presented the justification for how long it will take for a fire to damage equipment and cause a spurious actuation of a squib valve(s). This does not address SAP ESS.9 adequately which states that the time needed before operator actions should be demonstrated as sufficient. I do not consider the claim on operator action to be appropriately justified at this time, and therefore the risk may be underestimated. I have therefore undertaken a sensitivity study to investigate the significance of this (Ref. 71).

127. My sensitivity study uses the spurious ADS4 initiating event within the internal events at-power PSA and replaced the initiating event frequency with that of a fire, rather than that of a spurious protection system event. I have also assumed that no operator action takes place and that a fire will always cause cable damage that gives rise to a spurious ADS4 event. I concluded that the overall core damage frequency and large release frequency for the fire PSA would increase by approximately 20%. This would still enable the fire risk from the plant to meet the ONR SAP BSOs for target 8 and target 9.

128. Westinghouse has acknowledged this as an open item in its human reliability notebook (Ref. 62, section 9 open item no 2) and is being tracked by Westinghouse using its CAPAL systems as item 100344222. I consider the risk sensitivity and absence of justification at the current time to be sufficient to record the following assessment finding.

> **Assessment Finding** (CP-AF-AP1000-PSA02-06): The licensee shall justify, using fire analysis, the time available to the operators before fire damage to

equipment causes a spurious squib valve(s) actuation. This should be reviewed against the duration of the task and the potential consequences to demonstrate that risk is ALARP. On completion of this work the fire PSA should be updated as necessary.

Incorporating Operator Error into Multi-Compartment Fires

129. My review of the operator error modelling for multi-compartment fire scenarios showed that human error probabilities were appropriately mapped to the ‘exposing’ compartment, but were not mapped to the ‘exposed’ compartment should the barrier between the two compartments fail to contain the fire. In response to this comment Westinghouse performed a sensitivity study which shows that if this multi-compartment modelling is included the core damage frequency would increase by a maximum of 14%.

130. Westinghouse states that the majority of this increase is associated with a fire compartment which has been included in the fire ALARP analysis and is identified for cable re-routeing. Therefore, not all of the 14% increase may be reflected in an updated risk model. Westinghouse states that an improvement to the PSA has been added to its risk model maintenance database for future implementation. This is recorded with assessment finding CP-AF-AP1000-PSA02-07 at the end of Subsection 4.2.11.

4.2.11 Plant Risk Model for Fire

131. My assessment addressed the structure of the AP1000 plant electronic CAFTA and FRANX fire risk models, the fault tree model structure represented in CAFTA, the fire PSA database and the auditability of the FRANX information together with its overall construction and coherence.

132. I raised RQ-AP1000-1718 to cover the following topics (Ref. 61):

- documentation of the fault tree model changes needed from the internal events at-power risk model;
- use of the fire PSA database as a tool for generating FRANX inputs;
- the modelling in the fault trees and FRANX for multiple and single spurious operations;
- the modelling of multi-compartment fire scenarios in FRANX.

Fire PSA Database Verification

133. Assessment of the FRANX computer code input table found that the process of gathering the data from the fire modelling spreadsheet and the data processing in the fire PSA database were done in a complex way. The process incudes data transfer between the fire database and the fire modelling spreadsheet which is controlled by Visual Basic Application (VBA) code for which no detailed documentation was provided. Westinghouse has provided a brief description of the process in its response to the regulatory query, however it was not sufficient to ensure full traceability. Additionally, the VBA code and the database queries were not supported by a formal verification document.

134. As a result of the insufficient quality control of the process, I found that the human error probabilities were not assign correctly to the multi compartment fire scenarios as described above.

135. This finding raises a concern about the robustness of the process Westinghouse uses to generate inputs to the FRANX computer code using its fire information database

and VBA code for which Westinghouse provided no formal verification evidence. I have raised this item as an assessment finding.

Assessment Finding on Multi-Compartment Fires (CP-AF-AP1000-PSA02-07). The licensee shall carry out the following for multi-compartment fire modelling:

1) Map the human error probabilities to the 'exposed' compartment should the barrier between the two compartments fail to contain the fire (RQ-AP1000-1718, comment 10).

2) Verify the process used, and inputs into, the FRANX computer code from the fire information database using Visual Basic Application (VBA) code.

4.2.12 Integration of the Fire PSA into Level 2 PSA

136. The AP1000 plant PSA uses an integrated top logic fault tree for quantification of both core damage frequency and large release frequency. My assessment of the fire PSA did not find any additional fire specific fault sequences that needed special Level 2 PSA treatment. The active protection systems which could be affected by a fire and are used for severe accident mitigation are modelled explicitly, and their fire-induced failures are modelled adequately. I did not identify any Level 2 PSA assessment findings or minor shortfalls to record in my report.

4.2.13 Quantification, Uncertainty and Presentation of Results

137. I carried out an assessment of the fire risk quantification and the uncertainty analysis for the overall results of the fire PSA (Ref. 33). My review focussed on the following key topics:

- the adequacy of the risk quantification methods and computer codes used (CAFTA and FRANX);
- the presentation of the fire risk results;
- the selection and evaluation of the sensitivity cases;
- the selection of the uncertainty parameters;
- the propagation of the uncertainties through the fire risk model.

138. The outcome of this assessment is presented in RQ-AP1000-1718 (Ref. 57, comments 11, 12 and 13).

139. The risk quantification methods and computer codes used are industry standard and I consider the use of these to represent relevant good practice.

140. My assessment found that the uncertainty analysis was not conducted in accordance with relevant good practice because the uncertainty for the fire initiating event frequencies and the hot short probabilities was not propagated through the risk model. The uncertainty presented in the risk model results may not represent the actual fire risk uncertainty. I accept that this does not compromise the comparison of the fire risks with ONR SAPs, as noted by Westinghouse in its response to my assessment comments (Ref. 64). My comments on the uncertainty analysis is recorded as a minor shortfall.

Minor Shortfall (CP-MS-AP1000-PSA02-07): The fire initiating event frequencies and hot short probabilities should be propagated through the risk model.

4.2.14 Design Changes and Gap Analysis

141. 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 fire PSA this corresponds to the plant design at 1 September 2010, and an electrical design freeze date of February 2015. Westinghouse agreed to provide a qualitative risk gap analysis of the Class 1 and Class 2 design changes made after 1 September 2010 to provide confidence that the PSA adequately represents the UK GDA design reference point.

142. This “gap” analysis presents a discussion of the methodology in Ref. 77 and a comprehensive listing of the design change proposals under the following headings in Ref. 78:

- 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 model for the UK PSA under assessment;
- the UK-specific design change proposals that are not incorporated at this time but will be during the licensing phase.

143. I selected the following sample of design change proposals for assessment, concentrating on those originating between the PSA design freeze date and the present time. My criteria for selecting these from the extensive list of design change proposals were 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 area associated with the fire PSA such as electrical design that may involve cable runs:

- PXS Screen Flow Limit Changes for RNS Injection to Prevent ADS Stage 4 Actuation;
- Changes to Incorporate PXS 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 Finalization;
- AP1000 Plant Electrical Package 5 Design Finalization;
- AP1000 Plant Electrical Package 6 Design Finalization;
- AP1000 Plant Electrical Package 7 Design Finalization;
- AP1000 Plant Electrical Package 8 Design Finalization;
- 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.

I requested further information from Westinghouse in Ref. 79. The further information presented by Westinghouse for this sample of design change proposals shows that the fire PSA is not affected by any of them (Ref. 80). The electrical package design changes are already incorporated into the PSA. I am content that the gap analysis does not adversely affect my understanding of the overall risks from the fire PSA.

4.2.15 ALARP Assessment for the Fire PSA

144. The resolution plan stated that the fire PSA would be accompanied by an ALARP analysis to identify options for fire risk reduction based on the risk-significant fire compartments as well as the cables, systems and components driving the risk.

145. Prior to receiving the fire PSA ALARP analysis from Westinghouse, I carried out a high-level assessment of the AP1000 design features to identify those which I

considered may benefit from a fire risk ALARP review. I did this by reviewing the fire hazard analysis together with the safe shutdown equipment associated with the passive safety systems (Ref. 65). My review considered the following principles:

- relevant good practice for fire assessment and fire engineering;
- the potential for a fire to reduce defence-in-depth (SAP EKP.3);
- the potential impact a fire in a single compartment may have on the effectiveness of redundancy, diversity, segregation, separation and barriers between safety significant equipment (SAP EDR.2);
- the impact a fire may have on initiating events or the initiation of the passive safety systems (SAP EKP.5).

146. The results of my review identified a number of design features of the plant for attention (Ref. 67). I discussed these with the ONR internal hazards specialist inspector and fire specialists from my technical support contractor (Ref. 66). I identified the following features for further consideration on receipt of Westinghouse's ALARP analysis:

1) The neutron flux detectors outside the Reactor Pressure Vessel (RPV). These detectors and associated cabling are needed to monitor neutron flux at power and when shut down. All four of the Class 1E divisions for the detectors are located in the same fire zone (1100 AF 11105 – rooms 11105 and 11205) which contains the RPV. A fire in this compartment may result in the unavailability of all neutron flux monitoring. This may not be consistent with ONR SAP ERC.4 (Monitoring of parameters important to safety): "The core should be designed so that parameters and conditions important to safety can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected."

2) The two in-containment reactor water storage tank (IRWST) gutter isolation valves (V130A/B). These two valves are located in fire zone 1100 AF 11300A (maintenance floor south) and are required to close to divert condensate from the passive containment cooling system into the IRWST to maintain the passive residual heat removal heat exchanger heat sink for the long term. These two valves are 3.6m apart horizontally and 3.05m apart vertically. A single fire could compromise both valves.

3) The two passive residual heat removal heat exchanger control valves (PXS-PL-V108A/B). These two valves are located in fire zone 1100 AF 11300B (maintenance floor north) and are located within several feet of each other. A single fire could compromise the operation of these valves. One of these two valves is required to open to permit flow through the heat exchanger to provide passive decay heat removal. This passive safety feature is used for intact circuit faults when decay heat removal via the steam generators is not available.

4) The upper and lower ADS valve area (compartments 11703/11603). There are two sets of three pairs of ADS Stage 1 to 3 motor-operated valves in these two open areas. These valves provide the first three stages of automatic primary circuit depressurisation. This process is needed, in addition to ADS Stage 4 depressurisation, to permit passive IRWST injection and passive recirculation to remove decay heat.

   The power and control cables from each of the four control and instrumentation divisions come together in this area. There is the potential for a fire to compromise all four divisions of the cabling to the two sets of ADS Stage 1 to 3 valves, and therefore reduce defence-in-depth and reliability of the depressurisation safety function.

5) The ONR internal hazards specialist inspector raised a concern regarding the security room (12554) which contains all three of the DAS cabinets (Refs 68 and 70). The DAS cabinets provide a diverse means of actuating the passive safety systems should the PMS be unavailable. A fire in this room may fail both the manual and automatic DAS actuation functions. This room and the division C reactor coolant pump switchgear room (12312) are dominant contributors to the fire core damage frequency. A fire in the latter room can spread and damage two divisions of PMS. Common cause failures of the other two divisions of PMS in other compartments would result in reliance on DAS to actuate safety systems.

Westinghouse ALARP Analysis for the Fire PSA

147. The ALARP analysis and the fire PSA risks are presented by Westinghouse in Refs 33 and 38 respectively.

148. The fire PSA presents core damage frequency and large release information for a comprehensive set of plant compartments. I consider that the ALARP analysis is based on a systematic review of the fire PSA results to identify potential risk reduction measures. This is because Westinghouse reviewed the dominant minimal cutsets from the fire PSA for those compartments that displayed the highest core damage frequency. The overall core damage frequency and large release frequency is predicted by Westinghouse to be very small at 6.7×10^{-7}/year and 5.6×10^{-8}/year respectively. This makes an 80% contribution to the overall core damage frequency for reactor operations when other faults and hazards from at-power operations are considered. The larger contribution from fires than from other faults and hazards has led me to undertake a detailed assessment of the ALARP submission presented by Westinghouse.

149. The ALARP analysis presented by Westinghouse did not contain items 1, 2 and 3 from above that I anticipated in my initial ALARP considerations, but did contain items 4 and 5 in addition to a selection of other potential enhancements as follows:

- reducing common mode failures between the PMS and PLS;
- using automatic actuation of the hydrogen igniters;
- additional fire detection and suppression in the division C RCP switchgear room and security room;
- cable routing improvements:
  1) separation of DAS cables in the division C RCP switchgear room,
  2) providing separation of the cable routing to reduce the consequences of a fire in the lower ADS valve area,
  3) ensure the offsite retail power system (ZRS) cables which support the secondary side heat removal systems are not located in the security room with the DAS cabinets,
  4) separation of the hydrogen igniter power supplies,
  5) changing the cable design for the ADS1 to 3 valves to reduce the likelihood of spurious actuations.

150. Following the ALARP analysis Westinghouse make the following ALARP recommendations:

- diversify the manual cue for actuating the hydrogen igniters;
- remove one DAS power supply from the RCP switchgear room;
- ensure the ZRS power supply is not routed through the security room.

Westinghouse will investigate these further during the licensing phase using its design change proposal staged gate process.

Assessment of Westinghouse's Fire PSA ALARP Analysis

151. 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 paragraph 5.3). I consider that Westinghouse (rather than the licensee) has done this within GDA, but I have identified a number of additional areas of the plant that need further consideration.

152. The risk measures presented by Westinghouse show that the overall fire risk from at-power operations is small and falls within ONR's target 8 BSO of 10^{-6}/year for off-site dose greater than 1000 mSv. I have taken this position into account in my assessment in addition to the guidance in the ONR SAPs (Ref. 14 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 this within the detailed technical assessment of the fire PSA reported elsewhere in my report and within this section. However, the designer or dutyholder 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 dutyholder must do so by law.

153. The ONR SAPs are written in terms of legal dutyholders and licensees. Within GDA I consider Westinghouse as fulfilling the function of 'dutyholder' for the purpose of providing the ALARP analysis, although I note that the legal duty does not apply to GDA requesting parties.

154. I have assessed the ALARP analysis presented by Westinghouse and consider that for the majority of the options addressed, those not recommended for implementation are justified. The risk benefits presented by Westinghouse are small and I judge that the arguments provided by Westinghouse support the view that the "time, cost and trouble" of implementing the options would be grossly disproportionate to the safety benefit (Ref. 72 ALARP TAG paragraph 1.3).

155. However, my assessment identified that further work on the ALARP analysis was needed to address the following topics:

- the plant features I identified that are listed as items 1, 2 and 3 above;
- assurance on how the cable enhancements and suggested operator cue will be tracked to ensure their incorporation into the design;
- additional argument regarding the application of relevant good practice for the installation of automatic fire detection and suppression within the division C RCP switchgear room and security room (items 4 and 5 above).

156. This further work was raised in RQ-AP1000-1757 supplemented by meeting discussions with Westinghouse (Refs 73 and 74 respectively).

157. Westinghouse provided the following information in its response to RQ-AP1000-1757:

- Item 1 above. In the absence of the external RPV neutron flux detectors the reactivity of the core can be monitored independently using the BEACON system, and the boron content of the primary circuit can be monitored using sampling and chemical analysis in the longer term. The passive safety systems can be used to provide safe shutdown decay heat removal which will result in automatic boron addition to the primary system via the core make-up tanks. I consider this to be an adequate response to demonstrate that ONR SAP ERC.4 is met.

- Item 2 above. The safety-related cables for each of these valves belongs to a separate division and the raceways for the trays are fully enclosed inside solid steel covers. These valves move to the position required for PRHR decay heat removal should the air supply to the valves fail due to a fire. A fire detector is located close to each valve, and low combustible inventory means that a fire on one valve is unlikely to affect the other. These valves are qualified to operate with elevated temperatures of 340°F (171°C). I consider that additional measures are not needed to safeguard these two valves for GDA.

- Item 3 above. The safety-related cables for each of these valves belongs to a separate division and the raceways for the trays are fully enclosed inside solid steel covers. These valves move to the open position to permit PRHR flow should the air supply to the valve fail due to a fire. The valves are separated from each other by a non-combustible barrier of steel or steel composite materials. Separate fire detectors are provided near each valve. There is a low combustible inventory consisting of the cables themselves. These valves are qualified to operate with elevated temperatures of 340°F (171°C). I consider that additional measures are not needed to safeguard these two valves for GDA.

158. The response by Westinghouse states that its SmartPlant® Foundation† design database can be used to track 'known issues' through to completion. Its ALARP recommendations have been given a known issue identification number for tracking purposes. This is an adequate response for this item.

159. For item 4 above, the upper and lower ADS Stage 1 to 3 valve area, Westinghouse argues that fire wrapping of the cables would introduce a potential source of fibrous debris into the containment. In the event of a loss of coolant accident in this area, fibrous debris may be generated that blocks the passive recirculation cooling screens thereby disabling passive core cooling. I acknowledge that recirculation screen blockage is a single failure mode of passive recirculation cooling, the functioning of which is very important to the passive safety of the AP1000 plant design. I judge it reasonable not to introduce a new source of fibrous debris inside containment.

160. For item 4 above the fitting of automatic fire detection and suppression was not adequately considered in the original ALARP analysis (Ref. 38). The Westinghouse response to RQ-AP1000-1757 clarifies that automatic detection and suppression are not provided in the security room where the DAS cabinets are located, and that automatic detection is provided in the reactor coolant pump switchgear room, but not automatic suppression. The response states that the security room may be continuously manned during operations. However, this will be a future licensee decision. If so, the benefit of automatic detections and suppression would be reduced.

161. For items 4 and 5 above, I consider that there is one aspect of the ALARP analysis not adequately presented. This is the information supporting the contribution of relevant good practice as applied to other nuclear reactor designs. In addition, Westinghouse states in its ALARP analysis that detection and suppression changes are considered to be low-cost options (Ref. 38, section 7.6.4).

162. The ONR ALARP TAG (Ref. 72, paragraph 6.1) states that ALARP demonstrations should consider first and foremost factors relating to engineering, operations and the management of safety. These expectations are often referred to by the general term 'relevant good practice'. An important source of relevant good practice in the nuclear industry is what is done on similar facilities (Ref. 72, paragraph 6.7).

† *http://ppm.intergraph.com/products/information-management-product-family/smartplant-foundation*

163. I consider that additional justification is needed regarding the application of relevant good practice for the installation of automatic fire detection and suppression within the division C RCP switchgear room, the security room and the upper and lower ADS Stage 1 to 3 areas.

164. In its response to RQ-AP1000-1757, Westinghouse considered it is premature to include more detailed ALARP analysis. This is because further design development and PSA refinement may demonstrate smaller risks for these items. I agree this is possible and note that the adoption of fire detection and suppression in the future is not precluded by the design at the GDA close-out phase. I consider that the option of fitting additional fire detection and suppression can be reviewed during the licensing phase and this should be recorded as an assessment finding.

> **Assessment Finding** (CP-AF-AP1000-PSA02-08): The licensee shall carry out an ALARP analysis to determine whether automatic detection and suppression should be fitted to the division C RCP switchgear room, the security room housing the DAS cabinets and the upper and lower ADS Stage 1 to 3 valve areas.

ALARP Assessment Summary

165. I consider that the ALARP analysis for the fire PSA is based on a systematic review of the fire PSA results to identify potential risk reduction measures. The justification for implementing improvements is generally adequately robust. However, I have raised an assessment finding to improve the ALARP justification during the licensing phase. My assessment supports the view that the fire risks are being managed ALARP as the AP1000 design process continues through GDA and into the licensing phase.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

166. In Section 2.2 I listed the standards and criteria I used during my assessment to judge whether the AP1000 plant fire PSA submission appropriately addresses the resolution plan and has been carried out adequately with respect to modern standards.

167. I am able to concluded that the fire PSA has been carried out adequately with respect to these standards to enable a meaningful GDA assessment to be completed and for the GDA issue to be closed.

4.4 Overseas regulatory interface

168. ONR has formal information exchange agreements with a number of international nuclear safety regulators, and collaborates through the work of the 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 help promote consistency.

169. 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.

170. 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 US NRC PSA specialist inspectors (Ref. 50) - this meeting exchanged information of mutual interest on the AP1000 plant PSA;

- technical reports from the US NRC website;
- minutes of MDEP meetings undertaken by ONR inspectors.

4.5 Assessment Findings

171. During my assessment I identified 8 assessment findings for a future licensee to take forward in their site-specific safety submissions. Details of these are contained in Annex 1.

172. 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.

173. 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 or 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 or commissioning.

4.6 Minor Shortfalls

174. During my assessment I identified 7 items as minor shortfalls in the fire PSA, which are not considered serious enough to require the future licensee to take specific action. Details of these are contained in Annex 2.

175. Residual matters are recorded as a minor shortfall if they do 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; or
   - require further substantiation to be undertaken.

5 CONCLUSIONS

176. This report presents my technical conclusions for the assessment of GDA Issue GI-AP1000-PSA-02 (Fire PSA) relating to the AP1000 plant GDA closure phase.

177. The ONR Step 4 GDA assessment of the AP1000 plant fire PSA conducted in 2011 concluded that the predicted internal fire risk was not representative of the AP1000 design (Ref. 1). Therefore ONR raised GDA Issue GI-AP1000-PSA-02 which required a modern standards fire PSA to be developed for the AP1000 plant.

178. 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 15 technical actions and an ALARP analysis to accompany the resulting fire PSA.

179. To address GDA Issue GI-AP1000-PSA-02 Westinghouse presented a new fire PSA undertaken to NUREG/CR-6850 guidance and the ASME/ANS RA Sa 2009 fire PSA standard (Refs 4 and 6). This was undertaken to the extent achievable by a pre-operational plant with an agreed design reference point. An ALARP analysis was also submitted to accompany the fire PSA.

180. My assessment addressed each of the main technical elements of a fire PSA as presented within the NUREG guidance and ASME/ANS PSA standard. In this way I covered each of the 15 technical areas in the resolution plan. I undertook this assessment by sampling from each technical area of the fire 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 fire analysis and fire PSAs.

181. I consider the NUREG guidance and the ASME fire PSA standard to be a suitable basis for developing a modern standards fire PSA. My assessment found that the fire PSA has been carried out adequately with respect to these standards, and this has enabled a meaningful GDA to be completed. I am satisfied that the fire PSA meets the majority of the guidance in the ONR TAG on PSA.

182. However, my assessment has identified a number of shortfalls with respect to the NUREG guidance, the ASME PSA standard and the ONR TAG on PSA. I have raised a number of assessment findings to address these shortfalls. The number of shortfalls is relatively few when considering the large size and complexity of the fire PSA. I have raised assessment findings in the followings areas for the licensee to address:

- analysis of the potential pathways for liquid combustible material to leak into underground tunnels;
- further assurance for the frequency of a fire damaging cables which could spurious actuate a squib valve(s);
- improving the completeness of the supporting fire analysis (for example, hot gas layers on sensitive electronics, fire spread duration within cable trays, a more complete consideration of secondary combustibles);
- additional analysis for fire-induced collapse of the turbine building onto adjacent structures;
- improving the justification for main control room fires;
- justification that operator action in the event of a fire will be successful to de-energise equipment which could spuriously actuate a squib valve;
- complete the operator error modelling for multi-compartment fires, and additional verification of the database software used.

183. I have also raised a small number of minor shortfalls for the licensee to consider.

184. The ALARP analysis presented by Westinghouse is based on a systematic review of the fire PSA results to identify potential risk reduction measures. I consider the justification presented by Westinghouse for implementing improvements, or not, to be generally adequate given the small fire risk. However, I have raised one assessment finding where I judge that further ALARP justification is needed. This is to undertake

further ALARP analysis to address the need for fire detection and suppression within a limited number of areas of the plant.

185. The ALARP options for fire detection and suppression are not precluded by the status of the design at the closure of GDA or into the licensing phase. They can be implemented by the licensee if necessary.

186. Westinghouse claims that the core damage frequency and large release frequency from fires 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. None of the shortfalls has been found to individually increase the core damage frequency by more than 20%. Following my assessment it is my judgement that these claims are supported.

187. However, I consider that the risk from fires could change upwards or downwards as additional analysis is undertaken during the licencing phase to reflect detailed design, and the assessment findings presented above are addressed.

188. I consider that Westinghouse has presented suitable and sufficient work to enable GDA Issue GI-AP1000-PSA-02 to be closed.

6 REFERENCES

1 ONR-GDA-AR-11-003. Revision 0. 10 November 2011. ONR GDA – Step 4 Report – AP1000 – Probabilistic Safety Analysis. TRIM 2011/616488. www.onr.org.uk/new-reactors/ap1000/reports.htm

2 AP1000 - PSA-02 (Fire PSA) - Resolution Plan. March 2015. TRIM 2016/423988. www.onr.org.uk/new-reactors/ap1000/gda-issues-res-plan.htm

3 Guidance on Mechanics of Assessment within the Office for Nuclear Regulation (ONR). TRIM 2013/204124.

4 NUREG/CR-6850 (EPRI TR-1011989) Fire PRA Methodology for Nuclear Power Facilities, Electric Power Research Institute and U.S. Nuclear Regulatory Commission, September 2005.

5 EPRI 1019259, Fire Probabilistic Risk Assessment Methods Enhancements Supplement 1 to NUREG/CR-6850 and EPRI 1011989, Technical Report, September 2010.

6 ASME/ANS RA-Sa-2009 (and Addenda ASME/ANS RA-S-2008), February 2009. Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications.

7 Regulatory Guide 1.200 Revision 2, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.

8 RQ-AP1000-1427 - Fire PRA Model Development Guidebook ONR Assessment Comments - 26th October 2015. TRIM 2015/395881.

9 UKP-PRA-GM-010 Revision A - AP1000 Plant Fire PRA Model Development Guidebook (Response to RQ-AP1000-1427), January 2016. TRIM 2016/1649.

10 NS-TAST-GD-030 Revision 5, June 2016. Nuclear Safety Technical Assessment Guide. Probabilistic Safety Analysis. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-030.pdf

11 ONR-GDA-GD-001 Revision 3 dated September 2016. New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties. Parties. www.onr.org.uk/new-reactors/ngn03.pdf

12 NS-TAST-GD-051 Revision 4 dated July 2016. ONR Nuclear Safety Technical Assessment Guide. The Purpose, Scope, and Content of Safety Cases. (www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf)

13 GDA Issue GI-AP1000-CC-02 Revision 3. Westinghouse AP1000® Generic Design Assessment. PCSR to Support GDA. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf

14 Office for Nuclear Regulation, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 0.

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

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

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

18 Western European Nuclear Regulators' Association, Reactor Harmonization Group, WENRA Reactor Reference Safety Levels, WENRA, September 2014. www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

19 UKP-PRA-GM-010 - Revision A - AP1000 Plant Fire PRA Model Development Guidebook. TRIM 2014/472801.

20 APP-PRA-GSC-361 - Revision D - AP1000 Plant At-Power Fire PRA Plant Partitioning Notebook. TRIM 2016/135668.

21 APP-PRA-GSC-362 - Revision C - AP1000 Plant At-Power Fire PRA Equipment Selection Notebook. TRIM 2016/135695.

22 APP-PRA-GSC-362 - Revision C - AP1000 Plant At-Power Fire PRA Equipment Selection Notebook. List of Equipment - Electronic Files. TRIM 2016/135704.

23 APP-PRA-GSC-364 - Revision A - AP1000 Plant At-Power Fire PRA Fire PRA Fire Risk Model Notebook. TRIM 2016/135389.

24 APP-PRA-GSC-364 - Revision A - AP1000 Plant At-Power Fire PRA Fire Risk Model Notebook. Risk Model Electronic Files. TRIM 2016/135397.

25 APP-PRA-GSC-365 Revision B. AP1000 Plant At-Power Fire PRA, Fire Ignition Frequencies Notebook. TRIM 2015/41396.

26 APP-PRA-GSC-365 - Revision D - AP1000 Plant At-Power Fire PRA Fire Ignition Frequencies Notebook. Compartment Frequency Calculations – Electronic File. TRIM 2016/135782.

27 APP-PRA-GSC-366 - Revision 1 - AP1000 Nuclear Power Plant Fire PRA Circuit Analysis and Cable Selection. TRIM 2016/135411.

28 APP-PRA-GSC-367 - Revision C - AP1000 Plant At-Power Fire PRA Fire Scenario Selection Notebook. TRIM 2016/135418.

29 APP-PRA-GSC-367 - Revision C - AP1000 Plant At-Power Fire PRA Fire Scenario Selection Notebook. Fire Scenario Selection Database and Fire Modelling Analysis Electronic Files. TRIM 2016/135422.

30 APP-PRA-GSC-377 - Revision 1 - AP1000 Nuclear Power Plant Fire PRA Circuit Failure Mode Likelihood Analysis (CFMLA). TRIM 2016/135436.

31 APP-PRA-GSC-369 - Revision C - AP1000 Plant At-Power Fire PRA Fire Human Reliability Analysis Notebook. TRIM 2016/135456.

32 APP-PRA-GSC-369 - Revision C - AP1000 Plant At-Power Fire PRA Fire HRA Notebook. HRA Analysis Electronic Files. TRIM 2016/135468.

33 APP-PRA-GSC-370 - Revision A - AP1000 Plant At-Power Fire PRA Quantification and Results Notebook. TRIM 2016/135475.

34 APP-PRA-GSC-370 - Revision A - AP1000 Plant At-Power Fire PRA Quantification and Results Notebook. CAFTA Electronic Files. TRIM 2016/135483.

35 APP-PRA-GSC-370 - Revision A - AP1000 Plant At-Power Fire PRA Quantification and Results Notebook. Sensitivity Studies Electronic Files. TRIM 2016/135499.

36 APP-PRA-GSC-370 - Revision A - AP1000 Plant At-Power Fire PRA Quantification and Results Notebook. Top 100 Cutset Electronic Files. TRIM 2016/135563.

37 APP-PRA-GSC-370 - Revision A - AP1000 Plant At-Power Fire PRA Quantification and Results Notebook. CAFTA Cutset Electronic Files. TRIM 2016/135572, TRIM 2016/135579, TRIM 2016/135599 and TRIM 2106/135613.

38 LTR-AP1000-PRA-16-015 - Revision A - AP1000 Plant At-Power Fire Probabilistic Safety Assessment As Low As Reasonably Practicable Assessment to Support UK GDA PSA-02. TRIM 2016/135632.

39 APP-GW-GMP-025 - Revision A - AP1000 Plant Probabilistic Risk Assessment Maintenance and Update Procedure. TRIM 2016/135657.

40 APP-PRA-GSC-368 - Revision C – AP1000 Plant At-Power Fire PRA Main Control Room Notebook. TRIM 2016/118511.

41 APP-PRA-GSC-363 - Revision C - AP1000 Plant At-Power Fire PRA Cable Notebook. TRIM 2016/135716.

42 APP-PRA-GSC-363 - Revision C - AP1000 Plant At-Power Fire PRA Cable Notebook. Zone, Raceway and Cable Information – Electronic Files. TRIM 2016/135727.

43 SV0-PRA-GSC-363 - Revision C - AP1000 Plant At-Power Fire PRA Cable Notebook (Site Specific) Plus Cable Property List – Electronic Files. TRIM 2016/135735 and TRIM 2016/135746.

44 APP-PRA-GSC-365 - Revision D - AP1000 Plant At-Power Fire PRA Fire Ignition Frequencies Notebook. TRIM 2016/135762.

45 UKP-GW-GL-793 - Revision 1 (Chapter 10) - AP1000 Pre-Construction Safety Report - January 2017. TRIM 2017/43700.

46 NS-PER-GD-014 Revision 6. Purpose and Scope of Permissioning. November 2016. TRIM 2016/448079.

47 LTR-AP1000-PRA-16-043 - Fire Action Items from Generic Design Assessment (GDA) Meeting with Office for Nuclear Regulation (ONR) and Probabilistic Safety Assessment (PSA) for 4 October 2016. TRIM 2016/409326.

48 RQ-AP1000-1427 - Fire PRA Model Development Guidebook ONR Assessment Comments. October 2015. TRIM 2015/395881.

49 RQ-AP1000-1681 - AP1000 Plant At-Power Fire PRA Fire Scenario Selection Notebook ONR Assessment Comments. August 2016. TRIM 2016/343942.

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

51 RQ-AP1000-1475 - Fire PRA Model Development Documents. 25 January 2016. TRIM 2016/33260.

52 NPP-JNE-000842 - Document Review and Comment Resolution Form (Response to RQ-AP1000-1475) - 1st April 2016. TRIM 2016/139549.

53 Westinghouse Letter LTR-RAM-I-15-001 Revision 0. Summary of Expert Panel Activities Related to the Review of Multiple Spurious Operations for the AP1000® Plant Fire PRA. TRIM 2015/132181.

54 RQ-AP1000-1736 - Assessment of Details Fire Analysis CFAST Analysis and Cable Analysis for the Fire PSA - 24 October 2016. TRIM 2016/411533.

55 WEC-REG-1480N - Enclosure 2 - APP-EW21-E1-001 Rev 3 - AP1000 Standard Raceway and Cable Separation and Segregation. TRIM 2016/489984.

56 ONR-NR-AR-16-017 March 2017 - GDA Close-Out for the AP1000 Reactor - Probabilistic Safety Analysis for the Westinghouse AP1000 Reactor. GDA Issue GI-AP1000-PSA-01 (Success Criteria). TRIM 2016/275018.

57 RQ-AP1000-1718. AP1000 Plant At-Power Fire PRA Fire Risk Model Assessment. 12th October 2016. TRIM 2016/396433.

58 NUREG/CR-7010, Volume 1, July 2012. Cable Heat Release, Ignition, and Spread in Tray Installations During Fire (CHRISTIFIRE), Volume 1: Horizontal Trays. Volume 2: Vertical Shafts and Corridors.

59 RQ-AP1000-1652 - AP1000 Plant At-Power Fire RRA. Main Control Room Notebook. ONR Assessment Comments. 28 July 2016. TRIM 2016/301858.

60 APP-PRA-GSC-368 - Revision C - AP1000 Plant At-Power Fire PRA Main Control Room Notes (Response to RQ-AP1000-1652). September 2016. TRIM 2016/354311.

61 RQ-AP1000-1718 - AP1000 Plant At-Power Fire PRA Fire Risk Model Assessment - October 2016. TRIM 2016/396433.

62 APP-PRA-GSC-369 - Revision C - AP1000 Plant At-Power Fire PRA Fire Human Reliability Analysis Notebook. March 2016. TRIM 2016/135456.

63 NNP-JNE-001477 - Revised Human Error Analyses Revised Human Error Analyses - 14th December 2016. TRIM 2016/489290.

64 APP-PRA-GSC-364 Revision A and APP-PRA-GSC-370 Revision A. AP1000 Plant At-Power Fire PRA Fire Risk Model Notebook and Qualification and Results Notebook Comments Resolution Form. NPP_JNE_001369 (Enclosure 02) Response to RQ-AP1000-1718. November 2016. TRIM 2016/426892.

65 APP-GW-N4R-003 - Revision H - Fire Protection Analysis Report. TRIM 2015/147436.

66 AP1000 - TSC Advice on ALARP Options for the Fire PSA - Gutter Isolation Valves and ADS1 to 3 Valve Area, 28 October 2016. TRIM 2016/419416.

67 AP1000 PSA-02 - Early ALARP Considerations for the Fire PSA - 18 February 2016. TRIM 2016/74196.

68 RQ-AP1000-1431 - Internal Hazards Impacts on the Diverse Actuation System - 15 January 2016. TRIM 2016/21245.

69 AP1000 Assessment Report - Control and Instrumentation - GI-AP1000-CI-10. TRIM 2016/274949.

70 RQ-AP1000-1641 - Internal Fire - Comments from the Internal Hazards July 2016 Workshop. TRIM 2016/347047.

71 AP1000 - Fire PSA - Sensitivity Study - Failure to Prevent Spurious ADS4 During a Fire by Successfully Isolating the Power Supplies to the ADS4 Valves, 5 January 2017. TRIM 2017/6153.

72 NS-TAST-GD-005 Revision 7. December 2015. Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). TRIM 2015/457433.

73 RQ-AP1000-1757 - AP1000 Fire PSA ALARP Analysis - 16th November 2016. TRIM 2016/446055.

74 ONR-NR-CR-16-745 - AP1000 Westinghouse - Discussion of AP1000 PSA Work for PSA-01 & PSA-02 (No 37), 29 November 2016. TRIM 2016/469793.

75 NUREG-2169 (EPRI 3002002936) January 2015. Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database United States Fire Event Experience Through 2009.

76 RQ-AP1000-1736 Full Comment Resolution Form (Response to RQ-AP1000-1736) – November 2016. TRIM 2016/454853.

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

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

79 ONR Email to Westinghouse. Clarifications Requested from Westinghouse on Gap Analysis DCPs, 24 January 2017. TRIM 2017/40128. (Westinghouse reference: LTR-AP1000-PRA-17-005 Revision 0 “Westinghouse Response to Gap Analysis Questions – Clarification on Incorporated DCPs Post PSA Design Freeze Date 2010”).

80 AP1000 – Westinghouse Response to Gap Analysis Questions – Clarification on Incorporated DCPs Post PSA Design Freeze Date 2010, 26 January 2016. TRIM 2016/36079. (Westinghouse reference: LTR-AP1000-PRA-17-005 Revision 0 “Westinghouse Response to Gap Analysis Questions – Clarification on Incorporated DCPs Post PSA Design Freeze Date 2010”).

Table 1

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-PSA02 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 1.2 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 the GI-AP1000-PSA02 project is by agreement with ONR limited to critical operations 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. 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 4.2.15 of this report. The fire 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: 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 Section 4.2.12 where the numerical risks are used to support the ALARP analysis. Section 2.2 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 fire PSA.

SAP Number and Title	Description	Interpretation	Comment
EHA.16 Fire Detection and Fighting	"Fire detection and fire-fighting systems of a capacity and capability commensurate with the worst-case design basis scenarios should be provided"	This SAP provides advice that fire hazard analysis should be carried out understand the consequences of fire initiation and growth on the facilities structures, systems and components. The outcome from this needs to be understood with respect to the fire protection features provided in the design.	I have considered this SAP within Sections 4.2.1 and 4.2.8 when assessing the potential consequences of fires on the building structures where there may be exposed structural steel.
EKP.5 Safety Measures	"Safety measures should be identified to deliver the required safety function(s)"	This SAP describes a hierarchy of various types of safety measures of which passive safety systems are listed at the top.	I have considered this SAP within my ALARP assessment when considering the effect of a fire on the successful initiation of the passive residual heat removal system (see Section 4.2.15).
EKP.3 Defence-in-Depth	"Nuclear facilities should be designed and operated so that defence-in-depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression"	This SAP is relevant when the availability or reliability of standby safety systems can be compromised by a hazards such as fire.	I have considered this SAP within my ALARP assessment when the effect of a fire could adversely affect the availability or reliability of redundant safety equipment within the same fire area or the same fire compartment. (See Section 4.2.12).
EDR.2 Redundancy, Diversity and Segregation	"Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components"	This SAP is relevant to my fire assessment when there is redundant safety equipment within a single fire area or a single fire compartment.	I have considered this SAP within my ALARP assessment when the effect of a fire could adversely impact the availability or reliability of redundant components within the same fire area or the same fire compartment - for example the passive residual heat removal isolation valves. (see Section 4.2.15).

SAP Number and Title	Description	Interpretation	Comment
ERC.4 Monitoring of Parameters Important to Safety	"The core should be designed so that parameters and conditions important to safety can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected"	This SAP is relevant to the potential for a single fire to damage all of the external neutron flux detectors which are located within the same fire compartment in the vicinity of the RPV. Failure of all the neutron flux detectors could compromise the ability of the operators to monitor the reactivity of the core.	I have considered this SAP within my ALARP assessment when judging whether improvements to the fire mitigation are needed for the external neutron flux detectors. (see Section 4.2.15).
ESS.9 Time for Human Intervention	"Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided, before intervention, should be demonstrated to be sufficient"	This SAP is relevant to the time it takes for fire damage to occur and actuate a squib valve(s). This should be sufficient for the operators to undertake the required tasks.	Considered for the claim that the operators can prevent squib valve(s) actuation by isolating power supplies before fire growth causes this failure mode, (see Section 4.2.10)

Annex 1

Assessment Findings to be addressed during the Forward Programme – PSA-02 (Fire PSA)

Assessment Finding Number	Assessment Finding	References
CP-AF-AP1000-PSA02-01	The licensee shall undertake analysis of the potential pathways for liquid combustible materials to leak into underground tunnels, and the potential implications for the fire PSA (RQ-AP1000-1475, comment 8).	4.2.4 Switch Yard and Cable Tunnels
CP-AF-AP1000-PSA01-02	The licensee shall justify the claim that a low-voltage tray hot short cannot provide enough power to actuate the as-built squib valves.	4.2.6 Cable Analysis (RQ-AP1000-1736, comment 42)
CP-AF-AP1000-PSA02-03	Assessment Finding for the Supporting Fire Analysis The licensee shall carry out the following aspects of the supporting fire analysis in accordance with the NUREG/CR-6850 guidance and the ASME/ANS RA-Sa-2009 (and 2013 Addenda) PSA standard: 1) Include a hot gas layer impact analysis on sensitive electronics and include this within the fire scenario analysis and the fire PSA. 2) Evaluate fire spread along vertical cable trays in accordance with the accepted industry practices. 3) Revise the fire duration and heat release rate analysis for cable tray fires to meet relevant good practice, and use data from the actual plant design. 4) Develop fire scenarios for the maintenance floor (north) (compartment 1100AF11300B) and review other fire compartments to ensure appropriate completeness of fire scenarios. 5) Ensure that the zone of influence calculations takes into account the heat release rate contribution from secondary combustibles.	4.2.7 Supporting Fire Analysis 1) RQ-AP1000-1736, comment 3 2) RQ-AP1000-1718, comment 6 and RQ-AP1000-1736, comment 10 3) RQ-AP1000-1736, comment 11 4) RQ-AP1000-1736, comment 12 5) RQ-AP1000-1736, comment 13 6) RQ-AP1000-1736, comment 20

Assessment Finding Number	Assessment Finding	References
	6) Evaluate the “source only” fire scenarios.	
CP-AF-AP1000-PSA02-04	The licensee shall analyse the risk of collapse of the turbine building due to fire onto other buildings.	4.2.8 Assessment of Exposed Structural Steel from Fires
CP-AF-AP1000-PSA02-05	The licensee shall carry out the following for the main control room fire analysis: 1) Main control room fire scenarios that can cause fire propagation to secondary combustibles, and vice-versa. 2) Justify the likelihood of a fire in the auxiliary room causing main control room abandonment due to smoke ingress.	4.2.9 Main Control Room Fire Analysis 1) RQ-AP1000-1736, comment 25 2) RQ-AP1000-1652, comment 18
CP-AF-AP1000-PSA02-06	The licensee shall justify, using fire analysis, the time available to the operators before fire damage to equipment causes a spurious squib valve(s) actuation. This should be reviewed against the duration of the task and the potential consequences to demonstrate that risk is ALARP. On completion of this work the fire PSA should be updated as necessary.	4.2.10 Identification and Incorporation of Human Failure Events
CP-AF-AP1000-PSA02-07	Multi-Compartment Fires The licensee shall carry out the following for multi-compartment fire modelling: 1) Map the human error probabilities to the ‘exposed’ compartment should the barrier between the two compartments fail to contain the fire. 2) Verify the process used, and inputs into, the FRANX computer code from the fire information database using Visual Basic Application (VBA) code.	4.2.11 Plant Risk Model for Fire RQ-AP1000-1718, comment 10.

Assessment Finding Number	Assessment Finding	References
AF-AP1000-PSA02-08	The licensee shall carry out an ALARP analysis to determine whether automatic detection and suppression should be fitted to the division C RCP switchgear room, the security room housing the DAS cabinets and the upper and lower ADS Stages 1 to 3 valve areas.	4.2.15 ALARP Assessment for the Fire PSA

Annex 2

Minor Shortfalls to be addressed during the Forward Programme – PSA-02 (Fire PSA)

Minor Shortfall Number	Minor Shortfall	Report Section Reference
CP-MS-AP1000-PSA02-01	The scope of the fire PSA guidebook should be expanded to include methodology for fire risk for all plant operational modes, and for non-reactor based facilities on the site. This should also include the methodology for addressing the impact of high hazard fire sources on exposed structural building steel, and seismically induced fires. See RQ-AP1000-1427.	Section 4.2.1 Fire PSA Guidebook
CP-MS-AP1000-PSA02-02	A number of the plant fire areas defined within the global plant analysis boundary have not been designated as fire compartments. Clarification of which of the fire areas identified in Table 7.1-1 (Ref. 20) should be considered within the scope of the fire PSA (RQ-AP1000-1475, comment 7).	Section 4.2.2 Plant Partitioning and Equipment Selection
CP-MS-AP1000-PSA02-03	The generic fire ignition frequencies used in the analysis are based on NUREG-2169. The relevant NFPA 805 PRA Update FAQs related to Task 6 should be followed to ensure the latest methodology is applied. For example, the counting guidance for certain bins (RQ-1652, comment 9).	Section 4.2.5 Fire Initiating Events

Minor Shortfall Number	Minor Shortfall	Report Section Reference
CP-MS-AP1000-PSA02-04	The ignition frequency of the generic fire compartment 2030AF20300/2000AF01 appears relatively very high with respect to other compartments. Justification should be developed to demonstrate that an appropriate fire frequency has been used. Clarification should be presented of how apportionment of the fire frequency throughout the plant has been carried out (RQ-1475, comment 21).	Section 4.2.5 Fire Initiating Events
CP-MS-AP1000-PSA02-05	The analysis steps in the ASME standard for exposed structural steel should be followed to inform the design (RQ-AP1000-1681, question no 6).	Section 4.2.8 Assessment of Exposed Structural Steel from Fires
CP-MS-AP1000-PSA02-06	More robust evidence to support the claim that a fire in the MCR will be detected within a very short time period, typically less than one minute, should be developed, (RQ-1652, comment 7).	Section 4.2.9 Main Control Room Fire Analysis
CP-MS-AP1000-PSA02-07	The fire initiating event frequencies and hot short probabilities should be propagated through the risk model. Within the uncertainty analysis the uncertainty associated with fire ignition frequency was not propagated through the plant risk model. The uncertainty data in terms of ignition frequency distributions are provided in NUREG 2169 and can be used as an input to CAFTA database (.rr). CAFTA also allows equations to be used for frequency/probability calculation, therefore including the ignition frequency uncertainty in CAFTA/FRANX input is not considered to be of any practical difficulty.	Section 4.2.13 Quantification, Uncertainty and Presentation of Results

Minor Shortfall Number	Minor Shortfall	Report Section Reference
	The uncertainty data (probability distributions) of the hot short events were not included in the CAFTA database and not propagated through the plant risk model. A sensitivity evaluation documented in Ref. 33 Section 7.4.14.4 indicated a high importance of the hot short probabilities, therefore it was expected the associated uncertainty to affect significantly the overall plant risk uncertainty. Furthermore since hot short probabilities within the same cutset are often correlated this omission may result in an underestimate of the mean CDF and LRF predictions.	