New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-FS-07 Safety Case for Shutdown Faults

Assessment Report: ONR-NR-AR-16-027
Revision 0
March 2017

Published 03/17

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

Westinghouse Electric Company LLC (Westinghouse) is the reactor design company for the **AP1000**® reactor. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC), which had 51 GDA Issues attached to it. These issues require resolution prior to 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 GDA Issues.

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fault studies. Specifically, this report addresses GDA Issue GI-AP1000-FS-07 Safety Case for Shutdown Faults.

Safety cases are required to consider faults occurring in all the configurations and plant states that a nuclear facility is permitted to be in as part of normal operations. Intuitively, faults occurring when a nuclear reactor is operating at full power will be more onerous than similar faults occurring when the reactor is operating at a fraction of full power or is shut down. However, pressurised water reactors (PWRs) such as the **AP1000** reactor are extensively reconfigured during a routine outage. This means that a fault transient experienced by the plant during shutdown operations can progress differently from the way it would if a similar initiating event occurred while the reactor was configured for power operations. It also means that new faults, unique to shutdown operations, can be introduced because of the changes in configuration or the maintenance / inspection tasks being undertaken.

In submissions assessed by ONR in GDA Step 4, Westinghouse did describe in detail the many features included within the **AP1000** design to ensure that shutdown operations are undertaken safely. It also analysed several fault sequences that are unique to shutdown operational modes. However, this treatment was not integrated into the wider design basis safety case and was missing some of the components of a modern UK safety case. As a result, GDA Issue GI-AP1000-FS-07 was raised, requiring Westinghouse to provide a fully integrated design basis safety case as part of the Pre-Construction Safety Report (PCSR) and the accompanying fault schedule.

In response, Westinghouse has updated its PCSR (specifically Chapters 8 and 9) to address the requirements of the GDA Issue.

My assessment conclusions, following a review of the updated PCSR, are:

- Shutdown faults have now been considered and integrated into the **AP1000** design basis safety case (including the fault schedule), as required by the GDA Issue.
- Faults have been systematically identified, initiating event frequencies have been estimated, the Structures, Systems and Components (SSCs) claimed in the safety case have been clearly identified and classified, Technical Specification assumptions have been substantiated, radiological consequences have been calculated where appropriate and have been shown to be As Low As Reasonably Practicable (ALARP), consistent with the expectations set out in ONR's Safety Assessment Principles (SAPs) for a design basis safety case.
- Faults not considered in previous safety case submissions, notably pipe breaks outside the containment involving the Normal Residual Heat Removal System (RNS), have now been addressed.
- The adequacy of the **AP1000** reactor's low temperature over-pressure protection has been demonstrated.
- Faults restricted to refuelling operations have been described sufficiently for the purposes of GDA (although the future site-specific safety case will need to be updated as additional design and safety case information becomes available).

One Assessment Finding has been raised for a future licensee to address once a modern, full-scope Probabilistic Safety Analysis (PSA) model for shutdown modes has been developed in response to the GDA Step 4 Assessment Finding GI-AP1000-PSA-050.

- CP-AF-AP1000-FS-03: The licensee shall ensure that the initiating event frequencies assumed in the design basis safety case for shutdown faults are consistent the frequencies derived for the shutdown PSA as part of work to address AF-AP1000-PSA-050. If necessary, safety case arguments shall be modified as appropriate.

Ultimately, I am satisfied that Westinghouse has addressed all the requirements of GDA Issue GI-AP1000-FS-07 and that it can be closed.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
BSL	Basic Safety Level
BSO	Basic Safety Objective
C&I	Control and Instrumentation
CMT	Core Make-up Tank
CVS	Chemical and Volume Control System
DAC	Design Acceptance Confirmation
DiD	Defence-in-Depth
EDCD	European Design Control Document
EPRI	Electric Power Research Institute
GDA	Generic Design Assessment
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
IRWST	In-containment Refuelling Water Storage Tank
LOCA	Loss of Coolant Accident
NRC	[United States] Nuclear Regulatory Commission
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PMS	Protection and Safety Monitoring System
POSRV	Pilot-Operated Safety Relief Valve
PPS	Primary Protection System
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System
SAPs	Safety Assessment Principles
SSC	Structure, System and Component
TSC	Technical Support Contractor
VES	Main Control Room Emergency Habitability Systems
WENRA	Western European Regulators' Nuclear Association

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

1. Westinghouse Electric Company LLC (Westinghouse) is the reactor design company for the **AP1000**® reactor. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC), which had 51 GDA Issues attached to it. These issues require resolution prior to 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 GDA Issues.

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fault studies. Specifically, this report addresses GDA Issue GI-AP1000-FS-07 Safety Case for Shutdown Faults.

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 Overview of GI-AP1000-FS-07

4. ONR's Safety Assessment Principles (SAPs) (Ref. 2) define a safety case as a logical and hierarchical set of documents that describes risk in terms of the hazards presented by the facility, site and the modes of operation, including potential faults and accidents, and those reasonably practicable measures that need to be implemented to prevent or minimise harm.

5. Intuitively, faults occurring when a nuclear reactor is operating at full power will be more onerous than similar faults occurring when the reactor is operating at a fraction of full power or is shut down. Therefore, if the safety case can provide analysis showing the effectiveness of safety measures to deal with full power faults, in many cases it can be confidently assumed that the same measures can deal with the same faults occurring during shutdown. However, this simplistic approach is insufficient for modern safety case standards.

6. Pressurised Water Reactors (PWRs) such as the **AP1000** reactor are extensively reconfigured during a routine outage (compared to when they are at power); for example, the primary containment is opened, the head of the reactor pressure vessel is removed, the water level in the steam generators is lowered, etc. This means that a fault transient experienced by the plant during shutdown operations can progress differently from the way it would if a similar initiating event occurred while the reactor was configured for power operations. It also means that new faults, unique to shutdown operations, can be introduced because of the changes in configuration or the maintenance / inspection tasks being undertaken. In addition, many of the safety measures that protect the reactor at power are not available when the reactor is shut down. This could be because they need to be disabled to get to a cold, depressurised state (eg accumulators), they are not effective in shutdown conditions (eg power-range neutron flux detectors) or because maintenance activities result in them being taken out of service.

7. During GDA Step 4, ONR's fault studies assessment (Ref. 1) found that Westinghouse had extensively considered shutdown operations in both its design work for the **AP1000** reactor and its principal submission to ONR, the European Design Control Document (EDCD) (Ref. 3). However, but for a few exceptions, this information was not integrated into its main deterministic design basis safety case. While the documentation demonstrated that the designers of the **AP1000** reactor had included

many welcome features for shutdown operations that benefit both operations and safety, their importance within the safety case (through a graded approach to safety categorisation and classification) was not clear. Ref. 3 demonstrated that Westinghouse had reviewed the at-power design basis fault analyses to check their continuing applicability in shutdown modes, and had performed some new analyses for faults that were unique to shutdown, but crucially these analyses were not explicitly linked to safety case claims, the radiological consequences had not been evaluated, and there was no discussion as to why the risks from shutdown operations had been reduced to be As Low As Reasonably Practicable (ALARP).

8. For these reasons, at the end of GDA Step 4, ONR's fault studies assessment (Ref. 1) raised GDA Issue GI-AP1000-FS-07 (Ref. 4), requiring Westinghouse to provide a fully integrated design basis safety case for the Pre-Construction Safety Report (PCSR) and the fault schedule.

1.3 Scope

9. The assessment plan (Ref. 5) details the scope of this assessment. Consistent with this plan, the assessment is restricted to considering whether the Westinghouse submissions to ONR for GI-AP1000-FS-07 provide a response sufficient to justify closure of the GDA Issue. As such, this report only presents the assessment undertaken as part of the resolution of this GDA Issue and it is recommended that this report be read in conjunction with the Step 4 fault studies assessment of the Westinghouse **AP1000** reactor (Ref. 1) to appreciate the totality of the assessment of the evidence in the fault studies safety case undertaken as part of the GDA process.

10. As stated in the previous subsection, the EDCD (Ref. 3) assessed during GDA Step 4 highlighted many significant features in the **AP1000** design that benefit the shutdown safety case. These features remain in the design following the GDA pause, and a lot of text in the EDCD describing shutdown operations and reviews of the bounding nature of at-power transient analysis has been carried over unchanged into the latest version of the PCSR. This assessment for GI-AP1000-FS-07 has not attempted to repeat the ONR fault studies review done during GDA Step 4 (Ref. 1), and it should be assumed that the multiple positive conclusions reached about the **AP1000** design for shutdown modes still apply.

11. The scope of this assessment has therefore been limited to looking for clear demonstrations in updated safety case documentation that the shortfalls against ONR's expectations for design basis safety cases (which apply in all modes of operation) that were specifically identified in the text of GI-AP1000-FS-07 (Ref. 5) and the GDA Step 4 fault studies assessment report (Subsection 4.2.12 of Ref. 1) have been addressed.

12. The **AP1000** reactor safety case defines six discrete 'modes', which cover all the states that the reactor plant can be in during normal operation (ie non-fault conditions). These modes are shown in table 1 below. For the purposes of this assessment report, it is assumed that shutdown faults are design basis events occurring from Modes 3, 4, 5 or 6.

Table 1: Definition of **AP1000** reactor operational modes

Modes	Title	Reactivity condition (Keff)	% Rated thermal power(1)	Average reactor coolant temperature (°C) (°F)
1	Power operation	≥ 0.99	> 5	N/A
2	Startup	≥ 0.99	≤ 5	N/A
3	Hot standby	< 0.99	N/A	> 215.6 (420)
4	Safe shutdown(2)	< 0.99	N/A	215.6 (420) ≥ Tavg > 93.3 (200)
5	Cold shutdown(2)	< 0.99	N/A	≤ 93.3 (200)
6	Refuelling(3)	N/A	N/A	N/A

Notes:
1. Excluding decay heat
2. All reactor vessel head closure bolts fully tensioned
3. One or more reactor vessel head closure bolts less than fully tensioned

1.4 Method

13. This assessment has been undertaken in line with internal guidance on the mechanics of assessment within ONR (Ref. 6).

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report

14. ONR's GDA Guidance to Requesting Parties (Ref. 7) states that the information required for GDA may be in the form of a PCSR, and Technical Assessment Guide NS-TAST-GD-051 sets out regulatory expectations for a PCSR (Ref. 8).

15. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (Ref. 9), requiring Westinghouse to submit a consolidated PCSR and associated references to supply the claims, arguments and evidence to substantiate the adequacy of the **AP1000** design reference point.

16. A separate regulatory assessment report has been written to consider the adequacy of the PCSR and closure of GDA Issue GI-AP1000-CC-02, and therefore this report does not attempt to assess the totality of the **AP1000** PCSR. However, Westinghouse's response to GI-AP1000-FS-07 has been to capture its design basis safety case for shutdown faults within the PCSR, specifically in Chapters 8 and 9. As a result, this assessment report is effectively providing a commentary on the adequacy of the PCSR as it pertains to shutdown faults, and it is looking for many of the same expectations for a safety case as will considered in the broader GI-AP1000-CC-02. Its conclusion will be among the factors considered by ONR in its GI-AP1000-CC-02 assessment.

2.2 Standards and Criteria

17. The assessment has been undertaken in line with the requirements of the HOW2 BMS document NS-PER-GD-014 (Ref. 10). In addition, the SAPs (Ref. 2) constitute the regulatory principles against which dutyholders' safety cases are judged, and, therefore, they are the basis for ONR's nuclear safety assessment. I used the SAPs 2014 Edition (Revision 0) when performing the assessment described in this report (the original Step 4 fault studies assessment used the 2006 Edition).

2.2.1 Safety Assessment Principles and Technical Assessment Guides

18. The following SAPs (Ref. 2) were identified in the assessment plan (Ref. 5) as being appropriate to judge the adequacy of the arguments in the area of fault studies for the UK **AP1000** reactor.

- Fault Analysis SAPs FA.1 to FA.9
- Severe Accidents SAPs FA.15 and FA.16
- Engineering SAPs EKP.2 to EKP.5, ECS.1, ECS.2, EDR.1 to EDR.4, ESS.2, ESS.4, ESS.6 to ESS.9, ESS.11, ERC.1 to ERC.3, EHT.1 to EHT.4
- Computer Codes and Calculation Methods SAPs AV.1 to AV.8
- Numerical Target for DBA Consequences Target 4.

19. It is important to note, however, that the scope of the assessment to close the GDA Issue is narrowly defined and is less than that of a typical ONR assessment, such as that undertaken in GDA Step 4. The original fault studies assessment (Ref. 1), which resulted in GI-AP1000-FS-07, considered the SAPs identified above and identified gaps against expectations as they arose. By fully addressing the requirements of the GDA Issue, the assumption is that the resulting safety case for shutdown faults should meet the SAPs' expectations for fault studies.

2.2.2 National and International Standards and Guidance

20. There are both International Atomic Energy Agency (IAEA) standards (Ref. 11) and Western European Regulators' Nuclear Association (WENRA) Reference Levels (Ref. 12) that are relevant to the fault studies assessment of the **AP1000** reactor. The original GDA fault studies assessment undertaken during Steps 3 and 4 took

cognisance of the international standards published at the time. The GDA Issues that emerged from that original assessment can generally be characterised as having their origins in the application of the SAPs and UK relevant good practice, rather than through comparison with international guidance. Therefore, the SAPs (and not the international references) will be the foremost standards considered. It should be noted that the latest version of the SAPs (Ref. 2) were benchmarked against the extant IAEA and WENRA guidance in 2014.

21. Both IAEA and WENRA guidance is clear that the safety case for new nuclear power plant needs to consider all operational modes. Requirement 14 of IAEA's "Specific Safety Requirements 2-1" (Ref. 11) states:

> *Design basis for items important to safety - The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.*

22. Position 1 of WENRA's report on "Safety of new NPP designs" states:

> *The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents is the application of the concept of Defence-in-Depth (DiD). This concept should be applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states.*

23. The objectives of GI-AP1000-FS-07, which arose from an assessment against ONR's SAPs, are consistent with these high-level expectations defined in international guidance.

2.3 Use of Technical Support Contractors

24. No Technical Support Contractors (TSCs) were used in this assessment.

2.4 Integration with Other Assessment Topics

25. This GDA Issue focuses on ensuring that the features of the **AP1000** design for shutdown faults are fully integrated and accounted for in the design basis safety case. Therefore, this GDA Issue has required little input from outside the fault studies topic area for a conclusion to be reached on the adequacy of Westinghouse's submissions.

26. A modern safety case for a nuclear power plant should complement its deterministic design basis considerations with a comprehensive Probabilistic Safety Analysis (PSA). The expectation that faults during shutdown operational modes will be considered applies just as much to PSA as it does to the design basis safety case.

27. In GDA Step 4, ONR specialist inspectors assessed the treatment of low-power and shutdown events in the **AP1000** PSA (Ref. 13). They found that extensive use had been made of AP600 data (an earlier passive PWR plant design developed by Westinghouse before the **AP1000** reactor) and there was very limited documentation provided to justify their appropriateness for the **AP1000** reactor. Ultimately Ref. 13 concluded that the **AP1000** reactor's PSA treatment of shutdown faults was sufficient for GDA, but fell far short of the requirements for a site-specific safety case. Assessment Finding AF-AP1000-PSA-050 was raised, requiring the future licensee to provide a full-scope, modern and well-documented low-power and shutdown PSA specific to the **AP1000** reactor. Because this significant shortfall against ONR's expectations was raised as an Assessment Finding, it has not been Westinghouse's responsibility to address it within the same GDA timescales as GI-AP1000-FS-07.

Therefore, my assessment reported here has not needed to take account of a large volume of contemporaneous work being undertaken in the PSA area. However, in future, any licensee addressing AF-AP1000-PSA-050 will need to ensure that its PSA work is consistent with the design basis safety case developed for this GDA Issue.

2.5 Out of Scope Items

28. As I stated previously, this assessment has not sought to repeat the review undertaken during GDA Step 4 (Ref. 1). Notably, Westinghouse's analytical methods for modelling shutdown faults have not been assessed against the requirements of SAPs AV.1 to AV.8. It is assumed that the conclusions reached during GDA Step 4 about the adequacy of Westinghouse's methods (based on a sampling approach) remain applicable. This includes radiological consequences calculations, as well as thermal hydraulic analyses.

29. Refuelling operations (Mode 6) will be associated with many lifts of fuel, reactor internals and other heavy components. These operations have risks associated with them, potentially with radiological consequences. There is some limited consideration of Mode 6 faults in this assessment report (see Subsection 4.5), however I have not attempted to replicate the multidisciplinary assessments that were performed during GDA Step 4 (notably internal hazards, mechanical engineering and human factors), or to pre-empt future assessments that will need to be undertaken during site licensing, when the **AP1000** design and outage procedures are fully developed.

3 REQUESTING PARTY'S DELIVERABLES IN RESPONSE TO THE GDA ISSUE

31. During the GDA Step 4 review of the **AP1000** shutdown safety case, information provided in Chapter 19E of the EDCD (Ref. 3) was originally considered by ONR. In response to a Regulatory Observation, an additional (UK-specific) report (Ref. 14) was generated to complement the information in Ref. 3. The basis for raising the GDA Issue was an assessment of the information contained in these two documents. At the end of the GDA Step 4, Westinghouse consolidated the information from Ref. 14 into Revision 0 of its PCSR (Ref. 15). This was not provided in sufficient time for formal ONR assessment however, a quick review has demonstrated that this initial revision of the PCSR provided limited additional information to address the requirements of the GDA Issue.

32. Consistent with the expectations set out in ONR's wording for GI-AP1000-FS-07, Westinghouse has chosen to address the GDA Issue by making changes directly to the **AP1000** PCSR. Westinghouse had decided no longer to maintain Ref. 3 in addition to the PCSR, and it has reduced the scope of Ref. 14 to just spent fuel pool faults (ie it no longer provides information that could be relevant to the closure of this GDA Issue). This means that the PCSR, specifically Chapters 8 and 9, constitutes Westinghouse's primary submission for this GDA Issue.

33. During the interactions on this GDA Issue, constructive discussions were held between Westinghouse and ONR, using a succession of draft updates to the PCSR. Westinghouse also provided a 'roadmap' report (Ref. 16) to systematically demonstrate that ONR's comments on shutdown faults in the Step 4 assessment report (Ref. 1) were being taken into account. However, the judgement on whether this GDA Issue can be closed has ultimately been reached following an assessment of the formal Revision 1 version of the PCSR, supplied in January 2017 (Ref. 17).

34. More details of the relevant sections of the PCSR considered as part of this assessment are given below.

3.1 Chapter 9 of the PCSR

35. Chapter 9 ("Internally Initiated Events") is Westinghouse's chosen location for its design basis safety case within the PCSR. The bulk of the chapter (Sections 9.1 to 9.6) is concerned with faults occurring while the reactor is at full power or in low-power modes of operation (ie Modes 1 and 2). These sections have a scope that has its origins in the contents of Chapter 15 of the EDCD (Ref. 3). It is worth noting that because of the historical link to Ref. 3, the safety case for boron dilution faults caused by Chemical and Volume Control System (CVS) malfunctions in shutdown modes is discussed in Section 9.4.

36. With the exception of the CVS fault, the design basis safety case for shutdown faults is in Section 9.8. It contains a lot of information that was originally included in Appendix 19E of the EDCD (Ref. 3), however Westinghouse has extended its scope to cover additional faults and to meet the expectation for a UK safety case.

37. Section 9.8 does the following:

- It outlines the basis of its shutdown safety case. For each design basis fault, the **AP1000** design provides multiple lines of defence through both Class 1 passive systems and Class 2 active systems. The Class 1 systems provide the primary means of ensuring that safety functions are delivered. The Class 2 systems minimise the demands on the Class 1 systems, but are not formally claimed for any design basis shutdown fault. Operator actions during shutdown modes are only credited where there is indication from Class 1 instruments and there are at least 30 minutes for the operator to take action.

- It describes the features included in the **AP1000** design that contribute to safety during shutdown operations.
- It systematically reviews all the full-power and low-power (Modes 1 and 2) faults considered in Sections 9.1 to 9.6, and discusses the applicability of their safety case arguments and transient analyses to shutdown modes. To support fault schedule entries, it provides initiating event frequency estimates for individual faults. Typically, it assumes that a fault will occur during shutdown modes with a frequency $1/20^{th}$ of that assumed for the equivalent fault in power-operation modes (based on the fraction of time for which the reactor is expected to be shut down, compared to when it is generating electricity). This approach has resulted in the majority of shutdown faults being judged 'infrequent' (initiating event frequency $< 1 \times 10^{-3}$ per year).
- In most cases, it is argued that no additional analysis is necessary for shutdown faults. The exception to this conclusion is for a double-ended cold-leg guillotine break fault. Westinghouse has determined that additional analysis is required to demonstrate that safety criteria can be met if the fault is assumed to occur in Mode 3 immediately after the accumulators have been isolated (the analysis of the equivalent at-power fault demonstrates that safety criteria are met assuming more onerous conditions; however, it credits the performance of the accumulators).
- It provides a summary of the Class 1 equipment that is claimed in the design basis safety case for shutdown faults, following the review just described.
- It identifies and provides a design basis safety case (supported by analysis, as required) for faults that are unique to shutdown modes (ie they are not variations of faults that can occur while the reactor is at power, and therefore already considered). These faults are all associated with the Normal Residual Heat Removal System (RNS), which provides closed-loop decay heat removal in Modes 4, 5 and 6:
  - Failure of RNS during Modes 4 and 5, with the Reactor Coolant System (RCS) intact
  - Failure of RNS during Modes 5 and 6 with the RCS open
  - Loss of Coolant Accidents (LOCAs) involving the RNS in Modes 4 and 5 with the RCS intact
  - LOCAs involving the RNS in Mode 5 with the RCS open
  - LOCAs involving the RNS in Mode 6 with the refuelling cavity flooded.
- For shutdown faults that are judged to be bounded by the equivalent faults occurring at power, no additional radiological consequences evaluations or ALARP discussions are provided (Westinghouse has assumed that the information provided in Sections 9.1 to 9.6 applies). For the RNS faults that are unique to shutdown operations, the mitigated radiological consequences have been evaluated and a comparison against numerical target 4 from the SAPs (Ref. 2) has been made. ALARP discussions are also provided, stating why the **AP1000** design is adequate for GDA, while also identifying some further improvements that should be considered during site licensing, in order to strengthen the safety case.

38. The main text of Section 9.8 is supplemented with tables and figures:

- A table is used to define the six **AP1000** operational modes (identical to table 1 in this report).
- A table is used to summarise the availability of Class 1 passive core cooling equipment in the different operational modes established by the extant Technical Specifications.
- Tables summarise the assumptions and results of the RNS and Mode 3 cold-leg break faults.
- Figures illustrate the configuration of the **AP1000** plant during shutdown and the results of the shutdown-specific transient analysis.

3.2 Chapter 8 of the PCSR

39. Chapter 8 of the PCSR is dominated by the fault schedule. Westinghouse has split the fault schedule into five sections:

- Section 1 – reactor internal events
- Section 2 – additional reactor internal faults
- Section 3 – non-reactor faults
- Section 4 – internal hazards
- Section 5 – external hazards.

40. Section 1 summarises the key safety case claims for the power modes (Modes 1 and 2) design basis events considered in Sections 9.1 to 9.6; but in adjacent entries, it has also included summaries for the same faults occurring in Modes 3 to 6. These entries are informed by the systematic review of the consequences of these faults occurring in shutdown modes, set out in Section 9.8. The fault schedule provides links to relevant parts of Section 9.8 where an individual fault is discussed.

41. Section 2 summarises the key safety case claims for the RNS-related faults that are unique to Modes 4, 5 and 6. It also includes reactor internal events that are specific to refuelling operations (ie Mode 6).

42. Section 3 is not directly relevant to the shutdown (reactor) safety case.

43. Sections 4 and 5 summarise the design basis safety case for a range of internal and external hazards. They state that for most hazards, the safety case claims are the same in all operational modes.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-FS-07

45. My assessment of Westinghouse's submissions for GI-AP1000-FS-07 is set out below, against the scope defined in Section 1 and the strategy discussed in Section 2.

46. I have broken my assessment into six parts:

- The general adequacy of PCSR Section 9.8 (shutdown faults) and Chapter 8 (the fault schedule)
- Loss of RNS faults
- RNS LOCAs
- Low temperature over-pressure protection
- Mode 6 faults
- Initiating event frequencies.

47. My overall conclusion on whether this GDA Issue can be closed is informed by each of these.

4.1 The general adequacy of Section 9.8 and Chapter 8 of PCSR

48. The headline requirement for GI-AP1000-FS-07 is for Westinghouse to provide a fully integrated design basis safety case for shutdown faults in the PCSR. It is my judgement that Westinghouse's updates to the PCSR achieve this.

49. In the EDCD assessed during GDA Step 4 (Ref. 3), the design basis safety case set out in Chapter 15 was almost exclusively concerned with at-power faults. The discussion of shutdown faults was disassociated to another chapter (Appendix 19E) and was primarily concerned with reporting the results of transient analyses of a small number of faults, rather than delivering the broader-ranging objectives of Chapter 15.

50. The PCSR (Ref. 17) is now much more closely aligned with UK relevant good practice for design basis safety cases, as established by the SAPs (Ref. 2):

- The objective of the information provided on shutdown faults is clearly identified as being in support of demonstrating the fault tolerance of the **AP1000** design and the effectiveness of its safety measures (SAP FA.4).
- Through the fault schedule (Chapter 8) and the systematic review of the applicability of at-power faults presented in Chapter 9 (Section 9.8), Westinghouse has set out a comprehensive list of initiating events, in all operational modes, that have been considered in the design basis safety case for the **AP1000** reactor (SAP FA.5).
- Through the fault schedule and the text included in Section 9.8, Westinghouse has clearly identified the relevant design basis fault sequences for events occurring during shutdown (SAP FA.6). Claims are only made on Class 1 systems in the design basis safety case (no assumptions are made on the correct performance on non-Class 1 systems). Table 9.8.3-1 of Ref. 18 summarises the reductions in availability of Class 1 systems that are permitted in shutdown modes by the Technical Specifications, and the fault schedule entries demonstrate how these have been taken into account for individual faults.
- The approach that Westinghouse has taken to splitting up entries on the fault schedule is consistent with the advice given in paragraph 634 of the SAPs. If a fault is crediting the same safety measures across several operational modes, then a single fault schedule entry is provided. However, if the same initiating event occurring in some specific shutdown modes will result in claims being made on different (or a reduced number of) safety measures (eg due to maintenance), then a separate fault schedule entry is given.

- The consequences of shutdown faults have been systematically discussed in Section 9.8 (SAP FA.7). In many cases, Westinghouse has argued that the consequences of a fault (thermal hydraulic and radiological) occurring in shutdown modes are bounded by those evaluated for the same fault in at-power modes. Its general approach is that if it has been able to demonstrate for the more frequent and more onerous at-power versions of fault that ONR's numerical target 4 has been met and that the design is ALARP, then the same conclusion can be reached for a less onerous and less frequent version of the fault occurring during shutdown.
- The consideration of events in all operational modes in the fault schedule provides a powerful demonstration against the expectations of SAP FA.8 for design basis safety cases (in this case, for shutdown faults) to provide a clear and auditable link between initiating events, fault sequences and safety measures.
- SAP FA.9 suggests that the design basis analysis should provide the main basis for controls on plant configurations and the availability of safety systems. In practice, the **AP1000** design and the generic Technical Specifications governing operational modes and the availability of Class 1 safety systems have evolved over time in an iterative process, taking into account experience from older Westinghouse PWR designs, requirements requested by utilities, and a long design process undertaken without explicit consideration of typical UK safety case approaches. However, by referring to the fault schedule and Section 9.8, Westinghouse has effectively demonstrated that an adequate design basis safety case does exist for its operational modes, assuming the extant Technical Specification controls on availability.

4.2 Loss of RNS faults

51. In Modes 4, 5 and 6, decay heat removal in normal operation is provided by the RNS, supported by AC power supplies and the Class 2 cooling chain. Westinghouse has always recognised the need to consider a problem resulting in the loss of the RNS as a design basis fault, and in GDA Step 4, ONR observed that the fault was discussed in detail in Appendix 19E of the EDCD (Ref. 3).

52. This discussion and the supporting transient analysis results from Ref. 3 have been included in Chapter 9 of PCSR (Ref. 17), supplemented by a UK-specific safety case discussion, which is summarised below:

- Failure of the RNS during Modes 4 and 5 with the RCS intact is designated as a 'frequent' design basis fault (initiating event frequency > 1 x 10^{-3} per year), and diverse means for protecting against the fault are identified in accordance with UK relevant good practice.
- Failure of the RNS during Modes 5 and 6 with the RCS open is designated as an 'infrequent' design basis fault.
- The radiological consequences for a member of the public off site and for workers have been calculated (0.225 mSv and 0.326 mSv, respectively), assumed to be applicable in any operating mode using the RNS), and compared to the Basic Safety Level (BSL) numerical target 4 from the SAPs (Ref. 2) for 'frequent' faults (1 mSv off site, 20 mSv for workers).
- An ALARP discussion is provided. This explains Westinghouse's view that there is conservatism in both its thermal hydraulic and radiological consequences calculations that could reasonably be removed to further lower the predicted consequences to beneath the SAPs' Basic Safety Objective (BSO) levels. It refers to all the design work that has already gone into the **AP1000** reactor's features for shutdown faults, while also identifying some additional enhancements that could be considered in site licensing to reduce the risks further. Ultimately, it concludes that the current design is ALARP and

further enhancements (beyond those identified for further consideration in site licensing) would be grossly disproportionate.

53. As a result of the inclusion of this extra information, I am satisfied with both the **AP1000** reactor's design and the safety case for loss of RNS faults during shutdown modes. The key consideration in reaching this judgement is the clarity provided on how the permissions given in the Technical Specifications for the removal of Class 1 Structures, Systems and Components (SSCs) (notably the Core Make-up Tanks (CMTs) and Stage 4 of the Automatic Depressurisation System (ADS)) from service have been taken into account, together with single failure assumptions.

54. This information already existed in Ref. 3, and I welcome its continued inclusion as part of the PCSR.

55. ONR's Step 4 assessment (Ref. 1) did discover that Westinghouse had not fully documented its calculations for loss of RNS faults in accordance with its own internal processes. I am satisfied that this matter has now been addressed. Consistent with its general approach for Chapter 9 of the PCSR (ie an approach not just restricted to shutdown faults), Westinghouse has identified Ref. 18 as the source of the technical information that supports the presented analysis results. In turn, Ref. 18 clearly identifies an appropriate calculation note for loss of RNS faults.

56. The UK-specific information included in Section 9.8 of the PCSR addresses many of the weaknesses in the original safety case presentation observed in the GDA Step 4 assessment (Ref. 1). Westinghouse has not undertaken transient analysis of its diversity cases; instead it has provided a discussion to explain why it believes future analysis will be able to demonstrate the effectiveness of the measures it has identified. For the purposes of GDA, I am satisfied with the justifications given, and the text in the PCSR is written in such a way that the requirement to 'tidy up' these open items in the safety case through 'normal business' in site licensing will not be lost (ie an Assessment Finding is not needed).

57. The inclusion of a dose evaluation to be compared against the BSOs / BSLs in the SAPs is an important UK-specific addition to the safety case, and Westinghouse has used these results in a convincing way in the subsequent ALARP discussion to argue that the design is adequate. A powerful aspect of Westinghouse's ALARP argument is the linkage to all the design work it has already put into improving the **AP1000** reactor's robustness to shutdown faults (compared to earlier PWR designs), and therefore its arguments that further improvements would be grossly disproportionate (compared to their risk benefit) have credibility.

58. I consider the justification of the initiating event frequencies attributed to loss of RNS faults to be weak. A failure of the RNS in Modes 5 and 6 with the RCS open is designated an 'infrequent' fault, but it is likely that the plant will spend just as much time in these configurations during a refuelling outage as it would in Modes 4 and 5 with the RCS intact (for which an RNS failure is assumed to be a 'frequent' fault). No explanation is given for how either of these frequencies is derived, and by classifying it as an infrequent event, Westinghouse has made no attempt to describe a diverse means of cooling the plant with the RCS open. I will return to the issue of initiating event frequencies in Subsection 4.5.

4.3 RNS LOCAs

59. Breaks in the RNS piping outside the containment during Modes 4, 5 and 6 were not considered in the EDCD (Ref. 3). Westinghouse explained to ONR that this was in accordance with US Nuclear Regulatory Commission (NRC) guidelines, which specify that pipe ruptures need only be considered in systems that operate with high-energy conditions for more than 2% of the system operating time, or 1% of plant operating

time (including shutdowns). The RNS does not have high-energy conditions for sufficient time for these US criteria to be met, and therefore pipe breaks were not considered.

60. During GDA Step 4, Westinghouse recognised that this generic rule-based approach would not be acceptable in the UK without further justification. As a result, it undertook to include RNS breaks within the design basis safety case. This commitment has demonstrably been delivered by the fault schedule and supporting Section 9.8 (Ref. 17) text submitted in response to this GDA Issue.

61. Westinghouse has categorised a break in RNS pipework as an 'infrequent' fault. Given that the RNS pipework is qualified to a standard consistent with Class 1 components, I consider this to be a reasonable assumption.

62. An RNS break could occur either inside or outside the containment. A break outside the containment is significantly more onerous because:

- There is a route for RCS radioactivity to reach the outside environment.
- Water inventory assumed to be part of the closed passive cooling system within the containment is being lost (until action is taken to isolate the break).
- Prompts for action (eg to isolate the RNS and containment) could be delayed because the containment pressure will not rise, as it would if coolant was being lost through a break inside the containment (high containment pressure being a prompt for various automatic isolation actions).

63. For these reasons, Westinghouse's analysis has focused on breaks outside the containment. The fault schedule (Chapter 8 of Ref. 17) includes a statement that the consequences of an RNS break inside the containment are bounded by outside containment faults. In effect, Westinghouse is putting forward the same safety case for the two versions of the fault, despite the differing consequences. Westinghouse could have made an RNS break inside containment its own fault, or bounded it with a 'standard' LOCA within containment. However, I have no objections and see no disadvantages to Westinghouse's chosen approach.

64. As stated in Section 3, Westinghouse has identified three versions of the fault:

- LOCAs involving the RNS in Modes 4 and 5 with the RCS intact
- LOCAs involving the RNS in Mode 5 with the RCS open
- LOCAs involving the RNS in Mode 6 with the refuelling cavity flooded.

65. Each version results in a different fault sequence as a result of the differing configurations the plant is in when the break occurs. For the Modes 4 and 5 RNS LOCA fault, the event is assumed to proceed like any other LOCA fault, with the 'standard' automatic Class 1 **AP1000** safety features responding. However, this is supplemented by a claim that the operator will identify that the break is associated with the RNS, and within 30 minutes will take the necessary action to isolate both the RNS and the containment. Westinghouse has calculated the amount of water that could be lost through the break in that time and the effect that these losses would have on the flooded-up containment water level at the end of a LOCA sequence. It has shown that the resulting water level will be above the minimum required water level to support long-term passive containment recirculation.

66. On its own, this calculation to determine the adequacy of the final water level addresses an open item discussed in Ref. 1 on RNS LOCA faults to be closed by GI-AP1000-FS-07. However, since the GDA Step 4 assessment was undertaken, Westinghouse has introduced design change APP-GW-GEE-2761 (Ref. 23) into the UK design reference (Ref. 19) to automatically initiate the Class 1 RNS isolation and containment isolation functions when ADS Stage 4 actuates in Modes 4 and 5. In

response to a Regulatory Query (Ref. 20), Westinghouse has stated that this is expected to reduce the RNS isolation time from the 30 minutes assumed for a manual action to 14 minutes. However, this reduction in isolation time has not been credited in its analysis. This is a notable conservatism that I will return to later in the context of the acceptability of the predicted radiological consequences of the event.

67. For LOCAs in Mode 5 with the RCS open, Westinghouse has conservatively assumed that the RCS water level is drained down to 'mid-loop' level prior to the break occurring (a configuration that allows steam generator draining and maintenance activities while fuel is in the core). Ref. 17 states that a break outside the containment will rapidly drain the RCS hot leg. The **AP1000** Class 1 Protection and Safety Monitoring System (PMS) includes logic to automatically initiate ADS Stage 4 and In-containment Refuelling Water Storage Tank (IRWST) injection on a low hot-leg level indication after a 25-minute time delay.[1] During this 25-minute period without active core cooling, the RCS water would heat up, but Westinghouse's analysis shows that the core would not become uncovered. After 25 minutes, IRWST injection starts. Westinghouse has assumed that IRWST inventory will be lost for 5 minutes through the break, until the operator isolates the RNS break 30 minutes after the initial event. As with the Modes 4 and 5 RCS intact case, it has calculated that even with the lost water inventory, the final containment flood level will still be above the minimum required water level to support long-term passive containment recirculation.

68. For LOCAs in Mode 6 with the refuelling cavity flooded, Westinghouse has stated that the amount of water lost through the RNS break in 30 minutes will not cause the level to drop to below the reactor vessel flange, and therefore the core will remain covered. The water in the RCS will start to boil and steam, but this will cause the containment to pressurise, which in turn initiates the **AP1000** systems for passive containment recirculation.

69. In all three cases, I am satisfied with the explanation given in the PCSR (Ref. 17) and the links to supporting analyses (via Ref. 18) for why the fuel in the core is adequately protected and will not suffer consequential damage as a result of the RNS break. However, all three versions of the fault result in RCS inventory being released outside the containment, with both on- and off-site radiological consequences.

70. Westinghouse has estimated these radiological consequences using the RADTRAD code.[2,3] The predicted doses, although below the Target 4 BSLs for 'infrequent' faults, are very high:

Off-site dose: 52 mSv Worker dose: 323 mSv.

71. By way of comparison, Westinghouse's prediction of the off-site dose from a steam generator tube rupture fault (which also bypasses containment) is 0.19 mSv, while its prediction of the off-site dose for an at-power large break LOCA (assuming 33% of the fuel pins are damaged by the event) is 10.2 mSv.

72. At an early stage of the discussions on this GDA Issue, Westinghouse presumed that simply meeting the BSLs through a conservative calculation was sufficient for the safety case. However, I advised Westinghouse that these results could only be acceptable if they were accompanied by a very robust ALARP argument. In addition, I pursued my own investigation into the assumptions within this evaluation. In response

[1] *The 25-minute delay is designed to allow any personnel inside the containment to evacuate and allows them time to close up the containment behind them.*
[2] *ONR assessed the RADTRAD code during GDA Step 4 (see Ref. 1).*
[3] *Westinghouse has evaluated the radiological consequences for the Mode 4 and 5 RNS LOCA fault on the basis that the RCS activity levels it has assumed will only be present when the RCS pressure boundary is intact. The operators would not be permitted to open the RCS if high levels of activity were detected. On that basis, the radiological consequences of an RNS break in the other modes and plant configurations are judged to be bounded by the results of the single calculation.*

to a Regulatory Query (Ref. 20), Westinghouse clarified some its key assumptions and supplied its supporting calculation (Ref. 21). Significantly:

- The calculations have assumed that all the initial water inventory of the RCS is released outside the containment, not crediting the claimed manual isolation of the RNS on 30 minutes or the automatic isolation on 14 minutes. It is my view that it would be reasonable for Westinghouse to credit either of these actions in its calculations, potentially reducing the doses to 45% (assuming a 30-minute isolation time) or 25% (assuming 14 minutes) of the original predictions.
- Westinghouse has assumed an RCS activity inventory based on a generic 1995 Electric Power Research Institute (EPRI) paper, which surveyed iodine spiking in PWR plants and included data from the 1970s and 1980s. Westinghouse or a future licensee would have scope to use less-conservative assumptions, based on the performance of modern fuel designs and any limits imposed on RCS activity levels by **AP1000** Technical Specifications.
- No credit is taken in the off-site calculations for delay, plate-out or hold-up of radioactivity within the auxiliary building prior to its being released into the environment.
- No credit is taken for the Class 2 Heating, Ventilation and Air Conditioning (HVAC) system.
- No credit is taken for the Main Control Room Emergency Habitability Systems (VES) in the worker dose calculation. This is an appropriate analysis assumption for a 'standard' single **AP1000** unit as considered in GDA, because the extant Technical Specifications do not require VES to be operable in Modes 4, 5 and 6 unless irradiated fuel is being moved. However, the provision and availability of main control room HVAC will need to be reviewed as part of a site-specific safety case, given that the current proposal is for a three-unit site in a location with a significant external radiological hazard. This opens up a potential for the predicted worker dose for an RNS LOCA to be further reduced in the site-specific safety case.

73. If some or all of these points were taken into account, the predicted doses would fall to a level more typical for a modern PWR safety case. While not updating its calculations, Westinghouse has rightly captured these conservatisms in its final PCSR submission as part of a wider ALARP discussion (Ref. 17). It is my view that without this additional discussion of the conservatism in the results, it would be impossible to have the appropriate context to form judgements on whether further risk reduction options are grossly disproportionate.

74. Westinghouse's ALARP discussion does identify several further design improvements that should be considered by a future licensee (in addition to more refined calculations), including:

- Technical Specification changes to link RNS alignment to a specific decay heat level
- Further improvement to the automatic RNS isolation functionality
- Technical Specification changes to extend the availability of the VES to include Mode 5, as well as Modes 1 to 4.

75. Given the predicted doses, there does seem to be merit in considering them further (even if they are ultimately not all taken further), and I therefore agree with Westinghouse's recommendations.

76. Westinghouse's ALARP discussion also observes that the two-train separated RNS that is already proposed for the UK **AP1000** reactor (not assumed in the analysis) would reduce the break flow loss (due to smaller pipe diameters), while also increasing the ability to maintain active cooling following a break, without reliance on passive Class 1 systems. The installation of a two-train separated RNS is a major physical

modification to the standard **AP1000** plant (ie more significant than a change to the Technical Specifications), and I agree with Westinghouse that it is a further factor to take into account in the ALARP considerations.

77. In my opinion, the most significant point raised by Westinghouse in its ALARP discussion is that **AP1000** design has set out to reduce the number of containment leak paths and to provide an ability to quickly close the containment, should a fault occur during shutdown operations. It is very difficult for a fault which results in a loss of RCS inventory outside the containment for a period of time to meet the BSO established by Target 4 in the SAPs (Ref. 2). While Westinghouse's 'headline' predictions for the radiological consequences of an RNS LOCA fault are high, further refinements of analysis methods will never be able to show that the consequences of such an event have been reduced to insignificant levels. Striving to minimise the number of events which bypass the containment is a more effective way of meeting the ALARP principle than simply focusing on mitigating the consequences of the event once it has occurred.

78. In conclusion, I welcome the detailed consideration of RNS LOCA faults within the UK **AP1000** safety case. I am satisfied that Westinghouse has demonstrated that the fuel in the core will be protected and, despite the high predicted doses, I judge that Westinghouse has adequately shown that it has reduced the risks to be ALARP.

4.4 Low Temperature Over-pressure Protection

79. ONR's GDA Step 4 assessment (Ref. 1) criticised the presentation in Westinghouse's original safety case submissions for over-pressure events in shutdown modes with the RNS in operation. During at-power operations and shutdown modes without the RNS, malfunctions that result in increases in RCS inventory are protected by the Class 1 PMS (on detection of a high pressuriser level), which isolates the source of the extra inventory. When the RNS is in operation, these signal and isolation functions are not available. Instead, low temperature over-pressure protection of the RCS pressure boundary is provided by RNS relief valves. The fault sequence for a design basis over-pressure event is therefore significantly different when the RNS is in operation to an equivalent scenario in other operational modes.

80. The inclusion of RNS relief valves in **AP1000** design to provide a low temperature over-pressure protection function was prominent in Appendix 19E of the EDCD (Ref. 3) and Ref. 14, but there was no design basis safety case justification for their adequacy. The frequency of the initiating event that they were designed to protect against was not identified, single failure and Technical Specification availability assumptions were not explained, and there was no justification of their sizing, beyond a reference to a US "Code of Federal Regulation" requirement.

81. I am satisfied that Westinghouse's updated PCSR (Ref. 17) addresses the shortfalls identified by ONR in Ref. 1:

- The relevant fault (CVS malfunction that increases RCS inventory in Mode 4 with the RNS aligned and Mode 5 with the RCS intact) is clearly identified and discussed in both the fault schedule (Chapter 8 of PCSR) and in Section 9.8.
- The initiating event frequency is identified as 'infrequent' ($<1 \times 10^{-3}$ per year).
- The sizing of the RNS relief valves is explained more clearly, with a link to PCSR chapters detailing relevant engineering substantiation.
- The availability controls which dictate how the RNS trains will be used in shutdown modes are described.
- A justification of the single failure tolerance of the relief valves is provided as part of a wide ALARP discussion.

82. The ALARP discussion and a contrast with the equivalent protection provided on Sizewell B is worthy of further discussion. The UK **AP1000** reactor has two segregated RNS trains, each of which has a relief valve. Westinghouse states that during normal operations to cool the plant down, both trains are expected to be in use, as that significantly reduces the duration of the outage. In addition, Mode 5 mid-loop operations are prohibited unless both RNS trains are available. Therefore, Westinghouse claims that in most circumstances the **AP1000** design is single failure tolerant. However, it does concede that it is permitted to enter Modes 4 and 5 with just one RNS train operable.

83. Sizewell B's primary protection for low temperature over-pressure events is provided by three pairs of Pilot-Operated Safety Relief Valves (POSRVs), which are connected to the Primary Protection System (PPS). The PPS monitors the reactor coolant temperature and calculates an acceptable RCS pressure. If the pressure exceeds the derived limit, then the valves are opened by their solenoid control valves. The POSRV protection is therefore single failure tolerant, but its reliability is limited by the PPS. To increase the overall reliability of the low temperature over-pressure protection function, Sizewell B also has a single diverse spring-loaded relief valve on the CVS let-down line connected to one of the four RCS crossover legs.

84. Westinghouse observes in Ref. 17 that the **AP1000** designers have been able to reduce the sources of low temperature over-pressure by eliminating the need for high-head safety injection pumps (Sizewell B has four). The equivalent capability on the **AP1000** reactor is provided by the CMTs, but these are not pressurised above the RCS pressure and are therefore not capable of causing a low temperature over-pressure event. It also observes that the **AP1000** design has only two CVS makeup pumps, which inject through a common cavitating venturi. This limits their combined makeup. It claims that other PWRs have three such pumps and no cavitating venturi (although Sizewell B does similarly have two CVS pumps).

85. In contrast to the relatively complex primary protection provided on Sizewell B, Westinghouse states that the RNS spring-loaded relief valves on the **AP1000** reactor are simple and reliable, requiring no control and instrumentation (C&I) initiation, valve operators or power supplies. They are Class 1, and so will undergo extensive equipment qualification and in-service testing. Similar observations could be made for Sizewell B's diverse protection; however, it only has a single valve, compared to the **AP1000** reactor's two.

86. Finally, Westinghouse observes that in the unlikely event of a spurious failure of the CVS when only one RNS train is in service, and the single RNS relief valve fails, the limiting consequences would be an RNS break outside the containment, which has now been assessed as an 'infrequent' design basis fault.

87. Taking into account all the arguments put forward in the final version of the PCSR submitted for this GDA Issue (Ref. 17), it is my judgement that Westinghouse has now provided an adequate safety case for over-pressure events in shutdown modes with the RNS in operation, and it has justified why its design is ALARP. Although the over-pressure protection is not fully single failure tolerant, I do believe the **AP1000** reactor compares favourably with UK relevant good practice (as exemplified by Sizewell B), especially when the work to reduce the causes and severity of an event are taken into account. Clearly, a consequential RNS LOCA outside the containment should be avoided if at all possible, but I accepted in the previous subsection that Westinghouse has provided an acceptable safety case for that event, on the basis that it is an 'infrequent' design basis fault. I am satisfied that considering a CVS malfunction along with a failure of the RNS relief valves as a possible initiator will not have a significant impact on the 'infrequent' classification applied to an RNS LOCA, and therefore the safety case arguments I have accepted will remain valid.

4.5 Mode 6 Faults

88. The wording of GI-AP1000-FS-07 requires Westinghouse to ensure that faults during refuelling (Mode 6) are covered by the PCSR.

89. A review of the fault schedule shows that Westinghouse has ensured that the entries for each reactor fault summarise the safety case claims in all operational modes, including Mode 6, as appropriate. In addition, the consideration of RNS faults that are unique to shutdown extends to Mode 6 (see above).

90. Westinghouse has also identified additional faults in the fault schedule that it says are restricted to Mode 6. These include:

- Fuel misloading events
- Reduction in boration events
- Dropped loads onto the reactor core (including fuel, integrated head package and core internals)
- Refuelling operations before the fuel is adequately cooled.

91. Insofar as it identifies these faults, summarises Westinghouse's basic safety case claims and points to where further information can be found, the fault schedule is fulfilling its basic task. However, for most faults, the fault schedule and the supporting text in Chapter 9 of PCSR give few details on the frequency of the initiating event, the safety classification of the equipment or procedures designed to prevent the event from happening, and what the consequences would be, should the event occur.

92. Despite these limitations, I judge that Westinghouse has addressed this requirement of the GI-AP1000-FS-07 sufficiently for GDA. In parallel to this GDA Issue, Westinghouse has undertaken a significant package of work to improve its analysis of the consequences of dropped load events in response to GI-AP1000-IH-06 (Ref. 22). However, it is unrealistic to expect this new work to be reflected in a comprehensive safety case for Mode 6 faults before two key Assessment Findings raised in GDA Step 4 have been addressed:

- AF-AP1000-CI-004 requires a future licensee to assign and justify the safety classification applied to C&I equipment used in mechanical handling equipment and cranes.
- AF-AP1000-PSA-050 requires a future licensee to develop a full-scope, modern and well-documented low-power and shutdown PSA specific to the **AP1000** plant.

93. As these Assessment Findings are addressed, I would expect impacted sections of the safety case to be updated accordingly, including the fault schedule and the deterministic safety case currently presented in Chapter 9 of the PCSR. This should be a routine task for a licensee with robust safety case arrangements. Consequently, I am content for the currently observed weaknesses in the safety case for faults in Mode 6 to be resolved as part of 'normal business' in site licensing.

4.6 Initiating Event Frequencies

94. As described in Section 3, Westinghouse's general approach to estimating initiating event frequencies has been to assume that a fault will occur during shutdown modes with a frequency $1/20^{th}$ of that assumed for the equivalent fault in power-operation modes. This approach has resulted in most shutdown faults being judged to be 'infrequent' (initiating event frequency $< 1 \times 10^{-3}$ per year) with only one means identified on the fault schedule for delivering each required safety function.

95. A PWR like the **AP1000** reactor would typically operate continuously at power for 18 months between refuelling outages (which could last about one month). Therefore, for events that are random and could occur at any time during the 60-year operating life of the plant, I consider 1/20th frequency reduction to be a reasonable assumption. In some cases, where the likelihood of the initiating event at a point in time could be influenced by the pressures and temperatures being experienced by the plant, this approach could even be conservative. The crediting of just a single means of delivering each safety function for these 'infrequent' faults is consistent with UK relevant good practice for a design basis safety case for a civil nuclear power plant.

96. It is important to recognise that during outages the containment is entered, maintenance is performed and heavy lifts are undertaken. Some faults may therefore become much more likely during outages; indeed, some may only be possible when the plant is shut down. However, the most challenging consequences from such events are likely to be a loss of active cooling to the reactor or a LOCA event. It is my judgement that the safety case for these events is largely insensitive to changes in the initiating event frequency (notably, the safety case for the 'frequent' loss RNS faults).

97. For the purposes of GDA, I am content with how Westinghouse has allocated frequencies to shutdown faults. However, it is usual for the initiating event frequencies assumed in the design basis safety case to reference PSA results. In the absence of a modern, full-scope PSA for shutdown modes (see Subsection 2.4), it has not been possible for Westinghouse to provide this level of substantiation for its assumptions. Looking ahead, though, GI-AP1000-PSA-050 requires a future licensee to produce such a PSA as part of site-specific activities. Where appropriate, I would expect the PSA to adopt a more sophisticated approach to generating initiating event frequencies than has been used in the GDA design basis safety case. It is important for the design basis and PSA safety case to be consistent and to support each other; therefore I have identified an additional Assessment Finding for a future licensee to address once it has addressed the requirements of GI-AP1000-PSA-050.

- CP-AF-AP1000-FS-03: The licensee shall ensure that the initiating event frequencies assumed in the design basis safety case for shutdown faults are consistent the frequencies derived for the shutdown PSA as part of work to address AF-AP1000-PSA-050. If necessary, safety case arguments shall be modified as appropriate.

4.7 Assessment Findings

98. Assessment Findings are matters that do not undermine the generic safety submission and that 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.

99. Residual matters are recorded as Assessment Findings if one or more of the following apply:

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

In my assessment, I have raised only one Assessment Finding, CP-AF-AP1000-FS-03, which is described in Subsection 4.6 above.

5 CONCLUSIONS

100. This report presents the findings of the assessment of GDA Issue GI-AP1000-FS-07, relating to the **AP1000** GDA closure phase.

101. As a result of my assessment of Westinghouse's submissions for this GDA Issue, notably Chapters 8 and 9 of the PCSR (Ref. 17), I am satisfied that:

- Shutdown faults have been considered and integrated into the **AP1000** design basis safety case, including the fault schedule, as required by the GDA Issue.
- Faults have been systematically identified, initiating event frequencies have been estimated, the SSCs claimed in the safety case have been clearly identified and classified, Technical Specification assumptions have been substantiated, radiological consequences have been calculated where appropriate, and ALARP demonstrations have been provided. All of this is consistent with the expectations set out in ONR's SAPs for a design basis safety case.
- Faults not considered in previous safety case submissions, notably RNS LOCAs, have now been addressed.
- The adequacy of the **AP1000** reactor's low temperature over-pressure protection has been demonstrated.
- Faults restricted to refuelling operations (Mode 6) have been described sufficiently for the purposes of GDA (although future site-specific safety cases will need to be updated, as additional design and safety case information becomes available).

102. One Assessment Finding has been raised for a future licensee to address, once a modern, full-scope PSA for shutdown modes has been developed in response to GI-AP1000-PSA-050, which was raised in GDA Step 4.

- CP-AF-AP1000-FS-03: The licensee shall ensure that the initiating event frequencies assumed in the design basis safety case for shutdown faults are consistent the frequencies derived for the shutdown PSA as part of work to address AF-AP1000-PSA-050. If necessary, safety case arguments shall be modified as appropriate.

103. Ultimately, I am satisfied that Westinghouse has addressed all the requirements of GDA Issue GI-AP1000-FS-07 and that it can be closed.

6 REFERENCES

1.	Step 4 Fault Studies – Design Basis Faults Assessment of the Westinghouse **AP1000** Reactor, ONR-GDA-AR-11-004a Revision 0, November 2011, TRIM Ref. 2010/581406.
2.	Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0, ONR, November 2014. www.onr.org.uk/saps/saps2014.pdf
3.	**AP1000** European Design Control Document, EPS-GW-GL-700 Revision 1, March 2011, TRIM Ref. 2011/81804.
4.	GDA Issue "Safety Case for Shutdown Faults", GI-AP1000-FS-07 Revision 0. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-fs-07.pdf
5.	UK **AP1000** Assessment Plan for Closure GDA Fault Studies Issues 1 to 8, ONR-GDA-AP-14-002 Revision 0, March 2015, TRIM Ref. 2015/51535.
6.	ONR Guidance on Mechanics of Assessment, TRIM Ref. 2013/204124.
7.	GDA Guidance to Requesting Parties. www.onr.org.uk/new-reactors/ngn03.pdf
8.	The Purpose, Scope, and Content of Safety Cases, NS-TAST-GD-051 Revision 4. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf
9.	GDA Issue "PCSR to Support GDA", GI-AP1000-CC-02 Revision 3. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf
10.	Purpose and Scope of Permissioning, NS-PER-GD-014 Revision 5, TRIM Ref. 2015/304735.
11.	IAEA Standards and Guidance: International Atomic Energy Agency (IAEA) Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements (SSR) 2/1 Revision 1, IAEA, 2016. International Atomic Energy Agency (IAEA) Safety Standards Series – General Safety Requirements (GSR) Part 4: Safety Assessment for Facilities and Activities, IAEA, 2007. International Atomic Energy Agency (IAEA) Safety Standards Series – Safety Guide: Safety Assessment and Verification for Nuclear Power Plants 2001. (This publication has been superseded by GSR Part 4 and SSG-2.) www.iaea.org
12.	Western European Nuclear Regulators' Association (WENRA): Reactor Safety Levels for Existing Reactors, September 2014. WENRA Statement on Safety objectives for new nuclear power plants, WENRA, November 2010. Safety of new NPP designs, WENRA, March 2013. www.wenra.org
13.	Step 4 Probabilistic Safety Analysis Assessment of the Westinghouse **AP1000** Reactor, ONR-GDA-AR-11-003 Revision 0, November 2011, TRIM Ref. 2010/581527.
14.	**AP1000** Shutdown & Spent Fuel Pool Faults, UKP-GW-GL-077 Rev 0, January 2011, TRIM Ref. 2011/91027.

15.	**AP1000** Pre-Construction Safety Report, UKP-GW-GL-793 Revision 0, March 2011, TRIM Ref. 2011/192251.
16.	**AP1000** Shutdown Faults Safety Case Roadmap, UKP-SSAR-GL-002 Revision 0, January 2016, TRIM Ref. 2016/41534.
17.	**AP1000** Pre-Construction Safety Report, UKP-GW-GL-793 Revision 1, January 2017, TRIM Ref. 2017/43700.
18.	UK Fault Studies Analysis Basis, UKP-SSAR-GLR-001 Rev 0, August 2016, TRIM Ref. 2016/333118.
19.	**AP1000** Design Reference Point for UK GDA, UKP-GW-GL-060 Revision 10, January 2017, TRIM Ref. 2017/18158.
20.	Response to Regulatory Query “Conservatism in RNS LOCA Radiological Consequences Calculation”, RQ-AP1000-1774, TRIM Ref. 2016/496204.
21.	**AP1000** Normal Residual Heat Removal System (RNS) Failure Doses and RNS Break Doses, UKP-SSAR-GSC-014 Revision 0, January 2016, TRIM Ref. 2016/496271.
22.	GDA Issue “Substantiation and Analysis of the Consequences of Dropped Loads and Impact from Lifting Equipment Included Within the **AP1000** Design”, GI-AP1000-IH-06 Revision 0. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-ih-06.pdf
23.	Addition of RNS and Containment Isolation signals on ADS Stage 4 signal in Mode 4 and 5 with RCS Pressure Boundary intact, APP-GW-GEE-2761, Rev 0, September 2010, TRIM Ref. 2017/43214.

Annex 1

Assessment Findings to be addressed during the Forward Programme

Assessment Finding No.	Assessment Finding	Report Section Reference
CP-AF-AP1000-FS-03	The licensee shall ensure that the initiating event frequencies assumed in the design basis safety case for shutdown faults are consistent the frequencies derived for the shutdown PSA as part of work to address AF-AP1000-PSA-050. If necessary, safety case arguments shall be modified as appropriate.	4.6