New Reactors Programme

GDA close-out for the AP1000 reactor

GI-AP1000-CI-04 PMS Spurious Operation Blockers

Assessment Report: ONR-NR-AR-16-031
Revision 0
March 2017

Published 03/17

EXECUTIVE SUMMARY

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

This report is the Office for Nuclear Regulation's (ONR's) assessment of the **AP1000** reactor design in the area of control & instrumentation (C&I). Specifically, this report addresses GDA Issue GI-AP1000-CI-04 Protection and Safety Monitoring System (PMS) Spurious Operation Blockers (SOBs).

In discussions with ONR in GDA Step 4, Westinghouse identified a number of safety functions delivered by the PMS, whose potential spurious operation could have a significant safety impact on the plant, so need to be protected by spurious operation blockers (SOBs). This GDA issue arose due to the need to complete the:

- development of a design basis of safety case (BSC) for the SOBs;
- justification for the addition of SOBs to the containment recirculation squib valves;
- development of the design of the SOB and its formal introduction via the design change process; and
- C&I safety substantiation of the SOB in the form of a BSC.

The Westinghouse's GDA issue resolution plan stated that the approach to closing this GDA issue was to:

- develop the conceptual design for the UK SOB to ensure that the potential spurious actuation of the safety functions protected by the PMS SOBs are beyond design basis events;
- provide evidence via reliability calculations that the target for the reduction in PMS spurious actuation frequency is met by the UK SOB design; and
- justify that the design of the UK SOB against SAPs and relevant standards.

Following my assessment and in consultation with fault studies, mechanical and probabilistic safety assessment (PSA) ONR inspectors, I have concluded that the safety case provided by Westinghouse addressing closure of this GDA issue adequately justifies that the events resulting from spurious operation of the safety functions protected by SOBs are now beyond design basis. I have also concluded that the safety case addressing the SOB design for the UK **AP1000** plant is adequate to support closure of GI-AP1000-CI-04.

My judgement is based upon the following factors:

- assessment of the safety case provided in the **AP1000** Pre-Construction Safety Report (PCSR) covering the spurious actuation of the automatic depressurisation system (ADS) valves (both squib and motor operated valves (MOVs)), in-containment refuelling water storage tank (IRWST) injection line squib valves and containment recirculation line squib valves;
- assessment of the C&I justification in the BSC of the SOB;
- verification that the introduction of the SOBs ensures that the reliability target for the UK SOB is met.

The following matters remain, which are for a future licensee to consider and take forward in its site-specific safety submissions:

- to fully develop the safety case for the UK SOB, taking into account detailed design information.

- based on the detailed design of the UK SOB, to verify that the reliability targets set for the SOB can be adequately justified.

These matters do not undermine the generic safety submission and require licensee input / decision.

In summary, I am satisfied that GDA Issue GI-AP1000-CI-04 can be closed.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
BSL	Basic Safety Level
CAE	Claims, Arguments and Evidence
CCF	Common Cause Failure
CIM	Component Interface Module
COT	Channel Operation Test
C&I	Control and Instrumentation
DAS	Diverse Actuation System
EDCD	European Design Control Document
ESF	Engineered Safety Feature
GDA	Generic Design Assessment
IAEA	International Atomic Energy Agency
IRWST	In-containment Refuelling Water Storage Tank
LOCA	Loss of Coolant Accident
MOV	Motor Operated Valve
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
pfd	Probability of failure on demand
PMS	Protection and Safety Monitoring System
PS	Power Supply
PSA	Probabilistic Safety Assessment
RGP	Relevant Good Practice
RP	Requesting Party
RQ	Regulatory Query
SAPs	Safety Assessment Principles
SOB	Spurious Operation Blocker
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	Technical Support Contractor

TABLE OF CONTENTS

Tables

Annex(es)

1. INTRODUCTION

1.1 Background

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

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000**® reactor design in the area of control and instrumentation (C&I). Specifically, this report addresses GDA Issue GI-AP1000-CI-04 Protection and Safety Monitoring System (PMS) Spurious Operation Blockers (SOBs).

3. The related GDA Step 4 report is published on our website (Ref. 44) and this provides the assessment underpinning the GDA issue. Further information on the GDA process in general is also available on our website (Ref. 45).

1.2 Overview of GI-AP1000-CI-04

4. Westinghouse's principal safety case submission considered by ONR during GDA Steps 3 and 4 was the European Design Control Document (EDCD in Ref. 19). Chapter 15 of the EDCD provided an extensive demonstration of the robustness of the **AP1000** reactor to a wide range of design basis faults. However, it made no attempt to systematically demonstrate that control and protection system faults were protected against.

5. It is recognised that the **AP1000** reactor has some unique features compared to other pressurised water reactor (PWR) designs. As an example, when postulating a software common cause failure its PMS may spuriously actuate equipment such as the automatic depressurisation system (ADS) stage 4 squib valves, which automatically depressurise the reactor and cause a loss of primary inventory. GDA Step 4 recognised that the consequences of such an event occurring while the reactor is at full power and pressure were challenging to deal with. In addition, if the fault is initiated in the PMS, it is relevant good safety case practice (eg ESS.22 in Ref. 5) to assume that the PMS would be unavailable to provide its other engineering safety functions (ESFs). During discussions in GDA Step 4, there were also concerns about the structural integrity of the ADS stage 4 lines following spurious actuation at full power and pressure.

6. The PMS is a Class 1 computer-based safety system designed to minimise the likelihood of spurious actuation. While in other regulatory contexts the reliability claim on C&I protection systems can be as low as 10^{-5} (probability of failure on demand (pfd)), the expectation in the UK is that a pfd of 10^{-4} is the maximum claim that can be made for complex programmable system (Technical Assessment Guide (TAG) 046, Ref. 49). It is highlighted that in GDA Step 4 Westinghouse claimed 10^{-3} both for the pfd and for the annual spurious actuation frequency of the UK PMS (see Ref. 5). Since in the UK the threshold between design basis and beyond design basis events is 10^{-5} per annum (Safety Assessment Principles (SAP) FA.5, Ref. 3), the risk of a PMS-initiated spurious actuation of ESFs is not sufficiently low to consider these events as beyond design basis.

7. During **AP1000** GDA Step 4 (see Ref. 5), Westinghouse undertook a major review of credible spurious initiation faults and demonstrated that all of them were bounded by

existing design basis accident analyses, except for a selection of PMS safety functions (notably associated with the squib valve actuations).

8. To reduce the spurious actuation frequency of these ESFs beyond the design basis accident threshold, at the end of GDA Step 4 Westinghouse proposed to introduce within the PMS an instrumented interlock / blocker (spurious operation blocker (SOB)). ONR recognised the potential for the SOBs to have an important role in the safety case against spurious squib valve actuation for the **AP1000** design. However, the proposals came too late to be fully integrated and justified into a safety case submission mature enough for detailed assessment.

9. For these reasons, ONR raised GDA Issue GI-AP1000-CI-04 for Westinghouse to:

- provide a design BSC covering the spurious PMS actuation of the stages 1 to 4 ADS valves (Action 1);
- provide a design BSC covering the spurious operation of the containment recirculation squib valves (Action 2);
- formally introduce the SOB design change to the PMS design (Action 3); and
- complete the design of the SOB and substantiate its intended role (Action 4).

1.3 Scope

10. The scope of this assessment is detailed in an assessment plan (Ref. 10).

11. To de-risk future stages of the UK **AP1000** design, this assessment focused on the:

- coherence and adequacy of Westinghouse's design BSC in the close-out of this GDA issue;
- capability of the SOB design proposed for the UK **AP1000** reactor to bring the spurious actuation events beyond design basis;
- adequacy of the UK SOB design, in terms of architecture and implementation within the overall PMS; and
- diversity of the UK SOB from the PMS.

12. I have highlighted that the main concern associated with this GDA issue in Step 4 is the risk of software or systematic faults in the PMS causing spurious operation of the Class 1 system (for further context, see Refs 5 and 7). Although the focus of my assessment for this GDA issue closure was on systematic faults of the PMS (see Section 1.2 of this report and guidance in ESS.22), I also considered the contribution of the field instrumentation to the reliability calculation. However, it should be noted that should PMS spurious operation occur as a result of failures in the field instrumentation, the availability of other PMS ESFs is not necessarily compromised, provided that the other safety functions used to protect against this event are not delivered using the same sensors.

13. Also, while the spurious opening of the ADS stages 1 to 3 motor operated valves (MOVs) is bounded by other loss of coolant accident (LOCA) scenarios in the fault schedule (see Section 3), Westinghouse clarified in their resolution plan (Ref. 11) and a standard plant design change proposal (Refs 34 and 35) its intention to also protect these valves with the SOB. Although the focus of the assessment is where the risk is more significant from a nuclear safety perspective (ie on squib valves), in the close-out of this GDA issue, I considered Westinghouse's argument regarding the addition of the

SOB on these MOVs actuation with the aim of ensuring that there is no safety detriment in their incorporation for the UK **AP1000** design.

1.4 Method

14. This assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 1).

1.4.1 Sampling Strategy

15. It is rarely possible or necessary to assess a safety submission in its entirety, and therefore ONR adopts an assessment strategy of sampling.

16. The sampling strategy I adopted for this assessment was to review the safety case as presented in the BSC in Ref. 15 for adequacy against relevant good practice (RGP) and to sample key referenced supporting documents. I raised a number of Regulatory Queries (RQs) where the information provided in the safety case was not adequate or was unclear and Westinghouse provided updated documents to address my concerns. I then performed a further review of the revised documentation to confirm (or otherwise) that my queries had been addressed.

2. ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

17. ONR's GDA Guidance to Requesting Parties (Ref. 46) states that the information required for GDA may be in the form of a PCSR, and TAG 051 sets out regulatory expectations for a PCSR (Ref. 46).

18. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (Ref. 48) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence (CAE) to substantiate the adequacy of the **AP1000** design reference point.

19. A separate regulatory assessment report is provided 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, looking at the adequacy with which the key safety case claims and arguments for squib valve spurious actuation are included within the PCSR (and supporting references) is a fundamental aspect of this assessment, notably for Actions 1 and 2.

2.2 Standards and Criteria

20. The standards and criteria adopted within this assessment are principally the SAPs, internal TAGs, relevant national and international standards and RGP informed from existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles

21. The key SAPs (Ref. 3) applied within the assessment are included within Table 1.

Table 1: List of applicable Safety Assessment Principles

SAP	Title
ECS.2	Safety classification of structures, systems and components
ECS.3	Standards
EDR.1 to 4	"Design for reliability" SAP series
EQU.1	Qualification procedures
ERL.1 to 4	"Reliability claims" SAP series
ESS.1 to 26	"Safety system" SAP series

22. Note that other SAPs are relevant to the PMS as a whole (including the SOB) and were hence addressed as part of the assessment of GI-AP1000-CI-08 (Ref. 39).

2.2.2 Technical Assessment Guides

23. The TAGs (Ref. 4) that have been used as part of this assessment are set out in Table 2.

Table 2: List of applicable Technical Assessment Guides

Identification	Title	Reference in this report
TAG-003	Safety systems	Ref. 51
TAG-051	The purpose, scope and content of safety cases	Ref. 46

2.2.3 National and international standards and guidance

24. The international standards and guidance that have been used as part of this assessment are set out in Table 3.

Table 3: Key international standards used to support this assessment

Identification	Title	Reference in this report
IEC 61226:2009	Nuclear power plants. Instrumentation and control systems important to safety. Classification of instrumentation and control functions. International Electrotechnical Commission (IEC)	Ref. 49
IEC 61513:2011	Nuclear power plants. Instrumentation and control for systems important to safety. General requirements for systems. International Electrotechnical Commission (IEC)	Ref. 50
IEC 61508-2:2010	Functional safety of electrical/electronic/ programmable electronic safety related systems – Part 2: Requirements for electrical/electronic/ programmable electronic safety related systems	Ref. 51
IEC 61508-6:2010	Functional safety of electrical/electronic/ programmable electronic safety related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	Ref. 9

2.3 Use of Technical Support Contractors (TSCs)

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

26. Table 4 sets out the broad areas for which I used technical support. I required this support to provide additional capacity and enable access to independent advice and experience. The TSC support enabled ONR to address the peak load of assessment required by the Westinghouse submission programme.

Table 4: Work packages undertaken by the Technical Support Contractor

TSC	Work package
Altran UK Ltd	Review of Westinghouse submissions provided to support the resolution of GI-AP1000-CI-04.A3 and GI-AP1000-CI-04.A4, with sampling of supporting documentation
Altran UK Ltd	Review of the Westinghouse response to Regulatory Queries (RQs) raised by ONR

27. The TSC undertook the technical reviews under ONR's close direction and supervision. ONR exclusively made the regulatory judgement on the adequacy or otherwise of the **AP1000** reactor and raised all RQs and meeting actions with Westinghouse.

28. The TSC provided a report in Ref. 52 that addresses the scope of work listed above. The TSC also reviewed responses to RQs and meeting actions placed on Westinghouse. The TSC report in Ref. 12 includes a summary statement of the results of its work and findings (ie Technical Observations (TOs)). I have reviewed the TSC's TOs and, as appropriate, taken them forward under Assessment Findings (see Annex 1). The TSC TOs provide further guidance on the GDA Assessment Findings and set expectations for their resolution. Within this report, references to the TSC TOs in Ref. 12 are provided using the unique TO identifiers (eg GI-04-TO2.nn).

2.4 Integration with Other Assessment Topics

29. 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.

30. In the assessment, I consulted with the following specialist areas within ONR to clarify the adequacy of Westinghouse's design BSC for the spurious operation of squib valves:

- fault studies
- probabilistic safety assessment (PSA)
- mechanical engineering

2.5 Out of Scope Items

31. Because the UK SOB differs from the design implemented in the standard **AP1000** reactor, the expectation for the closure of this GDA issue is that the Requesting Party (RP) develops and justifies the conceptual design of the PMS blocker devices proposed for the UK. The level of maturity of the UK SOB design expected in GDA needs to allow an adequately de-risking of future phased UK SOB development, eg by suitably defining its architecture / interfaces and selecting key components. The full development of the detailed design is hence out of scope for this GDA issue closure.

32. In line with the expectations for other **AP1000** design C&I systems in Ref. 5, the selection and justification of the field instrumentation is out of scope for this GDA issue closure.

3. REQUESTING PARTY'S SAFETY CASE

33. In the early engagement with ONR regarding GI-AP1000-CI-04.A2, Westinghouse submitted a document (APP-PXS-GEC-001 Rev 0, Ref. 31) justifying the safety benefit associated with the introduction of the SOB for the in-containment refuelling water storage tank (IRWST) containment recirculation squib valve and committed to implement it for the UK **AP1000** reactor. On the basis of the conclusion of Ref. 31, the protection of the SOB for the UK **AP1000** reactor covers the ESFs supporting the actuation of:

- ADS stages 1 to 3 MOVs
- ADS stage 4 squib valves
- IRWST injection squib valves
- IRWST containment recirculation squib valves

34. To address Actions 1 and 2 of this GDA issue, Westinghouse submitted:

- Chapters 8 and 9 of the PCSR (Ref. 26), providing the fault schedule and the safety analyses for the UK **AP1000** reactor. In these chapters, Westinghouse identifies that:
  - The spurious actuation of the squib valves associated to ADS stage 4 (Fault ID 1.5.1), the IRWST injection (Fault ID 1.9.3) and the IRWST containment recirculation (Fault ID 4.2.3) are beyond design basis events with an annual frequency below 10^{-7}.
  - Although Westinghouse claims that the spurious actuation of the ADS stages 1 to 3 (Fault ID 1.5.2) is a beyond design basis event, its safety demonstration is conservatively presented in Chapter 9 of the PCSR (Ref. 26) as a design basis event.
- Chapter 10 of the PCSR (Ref. 26), providing the analyses of the beyond design basis events (including Fault IDs 1.5.1, 1.9.3 and 4.2.3) and showing how their consequences in terms of core damage frequency and large early releases are acceptable;
- Chapter 17 of the PCSR (Ref. 26), providing the safety substantiation of the squib valves from a mechanical engineering perspective; and
- Chapter 19 of the PCSR (Ref. 26), providing the safety substantiation of the PMS actuation (including the blockers) from a C&I perspective.

35. Westinghouse addressed Action 3 of this GDA issue by submitting the following design change proposals (DCPs) to introduce the SOB in the **AP1000** reactor:

- APP-GW-GEE-2411 Rev 0, ADS Diverse Actuation Block (Ref. 34)
- APP-GW-GEE-4291 Revision 0, Change to Address Spurious Actuation of the IRWST Squib Valves (Ref. 35)
- APP-GW-GEE-4823 Rev 0, ADS & IRWST Injection Blocking Device Logic Change (Ref. 36)
- APP-GW-GEE-5280 Revision 0, Design Changes to the ADS and IRWST Blocker in Support of UK GDA CI-04 BSC (Ref. 37)

36. Note that, while the first three DCPs (Refs 34 to 36) were issued before the restart of the GDA issue closure process, Westinghouse produced the last DCP (Ref. 37) during the GDA close-out phase.

37. Westinghouse addressed Action 4 of this GDA issue by submitting a BSC for the spurious operator blocker (UKP-PMS-GLR-003 Rev. 1, Ref. 13). Westinghouse submitted the following key supporting documents:

- UKP-PMS-GLR-013, Rev. 0, United Kingdom **AP1000** IEC 61508-2 Compliance Matrix for Spurious Actuation Blocking Hardware (Ref. 14)
- UKP-PMS-GL-012, Rev. 1, United Kingdom **AP1000** IEC 61513 Claims, Arguments and Evidence for the Protection and Safety Monitoring System (Ref. 55)
- UKP-PMS-GL-006, Rev 2, United Kingdom **AP1000** Failure Rate Estimation of the PMS ADS and IRWST Injection Blocking Device Assembly (Ref. 40)

38. Note that the UK SOB BSC (Ref. 13) refers out to a number of other deliverables submitted against other C&I GDA issues which substantiate claims made in Ref. 13, ie:

- Ref. 38 (PMS BSC for GI-AP1000-CI-08 closure) in relation to the integration of the SOB with the PMS;
- Ref. 27 (CIM BSC for GI-AP1000-CI-09 closure) in relation to the interface of the SOB and the CIM; and
- Ref. 42 (PMS/DAS diversity analysis for GI-AP1000-CI-03 closure) in relation with the justification of the diversity of the DAS and the PMS (including the SOB).

39. Section 4.1 of this report clarifies the scope of the assessment of Refs 27, 38 and 42.

4. ONR ASSESSMENT OF GDA ISSUE GI-AP1000-CI-04

40. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 1).

4.1 Scope of Assessment Undertaken

41. The scope of the assessment covered the Westinghouse submissions identified in the GDA issue resolution plan (Ref. 2).

42. Although the resolution of this GDA issue involved the contribution of several other specialisms (see Section 2.4 of this report) and C&I GDA issues (see Section 3 of this report), this assessment report is not meant to duplicate the assessment carried out in other areas and hence only reports the conclusions which are relevant for the close-out of GI-AP1000-CI-04, referencing out to other ONR assessments where needed.

4.2 Assessment

43. In this section, the assessment is presented against each GDA issue action. Ref. 12 presents a detailed review of the main submissions defined in Section 3 of this report.

4.2.1 Actions 1 and 2

44. Actions 1 and 2 of this GDA issue required Westinghouse to provide a design BSC for the SOBs in the UK **AP1000** reactor, justifying how the proposed devices provide adequate protection against the spurious operation of the:

- ADS valves (stages 1 to 4)
- containment recirculation squib valves

45. Note that the SOBs are also implemented in the standard plant **AP1000** design to protect against the spurious actuation of the IRWST injection squib valves. The safety benefit of implementing this blocking function was discussed in GDA Step 4 (Ref. 5) and its justification is included in Ref. 13 (see assessment in Section 4.2.3 of this report).

46. While the blocking devices to protect against the spurious actuation of ADS stages 1 to 4 and IRWST injection valves are implemented in the standard **AP1000** design, Action 2 of this GDA issue requested Westinghouse to justify the need for SOBs for the containment recirculation squib valves. In the early stages of this GDA issue resolution, Westinghouse issued a document (APP-PXS-GEC-001, Rev. 0 (Ref. 31)) to determine the safety impact of this modification. In the assessment of Ref. 31, I verified that this revision of the document addresses the request for clarifications in RQ-AP1000-1368 (Ref. 20) raised on a draft of this document. Based on the assessment of Ref. 31 and the as low as reasonably practicable (ALARP) argument in Ref. 13, I am content with Westinghouse’s proposal to introduce the protection of the containment recirculation squib actuation through the SOBs.

47. The wording of Actions 1 and 2 of this GDA issue specifically mentions a design BSC. However, the basis of Westinghouse’s approach to GI-AP1000-CI-04.A1 and GI-AP1000-CI-04.A2 resolution is that the introduction of the SOBs means that spurious initiation events of concern qualify as beyond design basis events. This has implications for how and where they are discussed in the PCSR, but it does not exclude them from all consideration within the safety case. TAG-051 (Ref. 46) sets out some generic expectations for safety cases that still apply for beyond design basis:

- All references and supporting information should be identified and be easily accessible.

- There should be a clear trail from claims through the arguments to the evidence that fully supports the conclusions, together with commitments to any future actions.

- A safety case should accurately represent the current status of the facility in all physical, operational and managerial aspects.

- There should be references out from the safety case to important supporting work, such as engineering substantiation.

48. In the response to RQ-AP1000-1680 (Ref. 23), Westinghouse outlined its strategy to address GI-AP1000-CI-04.A1 and GI-AP1000-CI-04.A2, clarifying the approach to their resolution and where the substantiation is captured in the PCSR (see Section 3 of this report).

49. After internal consultation with other disciplines, I am broadly satisfied that the PCSR in Ref. 26 provides an adequate safety case for the spurious operation of the squib valve. Specifically, in line with the expectation in TAG-051 (Ref. 46), the PCSR:

- through the fault schedule in Chapter 8 of Ref. 26, provides an entry point for accessing all relevant supporting information in relation to spurious operation events;

- provides an adequate trail between the claims in the fault schedule and the engineering substantiation in the C&I and mechanical chapters (respectively Chapters 19 and 17 of Ref. 26); and

- provides the link to the safety demonstrations of these spurious operation events (ie in Chapter 9 of Ref. 26 for design basis events and in Chapter 10 of Ref. 26 for beyond design basis events).

50. Significantly, on the last point, although Westinghouse is also claiming that a spurious actuation of an ADS stages 1 to 3 valve is a beyond design basis event, to maintain a link to the original EDCD (Ref. 19) and the approach taken in other countries, it has retained a design basis treatment of the consequences of one of these valves opening in Chapter 9 of PCSR (Ref. 26). I have no objections to this and the fault schedule provides sufficient explanation for the reasoning behind it (see also Ref. 18 for the assessment of the **AP1000** fault schedule). As for the other spurious operation events, I judged that Westinghouse's approach to consider them as beyond design basis events in Chapter 10 of the PCSR (Ref. 26) is appropriate, provided that the supporting engineering substantiation (eg from a C&I and mechanical viewpoint) is adequate.

51. Note that:

- a detailed justification of the probability of non-C&I initiated spurious operation (eg due to mechanical failures or electromagnetic interference) is provided as part of the resolution of GI-AP1000-ME-01 (Ref. 15);

- the justification of the adequacy of the C&I design is part of the resolution of Action 4 of this GDA issue (see assessment in Section 4.2.3 of this report);

- detailed justification of the adequacy of the PSA modelling is provided against GI-AP1000-PSA-01 (Ref. 53);

- the full assessment of the fault schedule for the UK **AP1000** reactor is provided in the close-out of GI-AP1000-FS-08 (Ref. 18); and

- the full assessment of the PCSR is provided as part of the closure of GI-AP1000-CC-02 (Ref. 17).

52. I have also highlighted that, although in Ref. 26 Westinghouse claim that ADS stage 4 and IRWST injection spurious actuations are beyond design basis events, during GDA, closure evidence was provided in the form of an expert panel review (Ref. 32) to show that the consequences of their spurious actuation are bounded by other design basis LOCA accidents. Considering the conclusions of the detailed assessment of this report (Ref. 54), I found that Ref. 32 provided further confidence on the robustness of the design BSC for the spurious actuation of these squib valves.

53. From a C&I perspective, in order to close GI-AP1000-CI-04.A1 and GI-AP1000-CI-04.A2, I expect Westinghouse to show that the introduction of the SOBs in the UK PMS design:

- reduces the frequency of the spurious actuation of ESFs beyond design basis; and

- does not significantly affect the reliability of the actuation on demand of these ESFs (ie the claims in the PMS safety case of a probability of 10^{-3} on demand is met).

54. Westinghouse clarified in the resolution plan for GI-AP1000-CI-04 (Ref. 11) its intention to show that the initiating event frequency of spurious actuation originated by failures in the PMS after the introduction of SOBs is below to 10^{-7} per annum. This value corresponds to a typical cut-off frequency for beyond design basis fault sequences (see SAP FA.6 in Ref. 3) and is more stringent than the standard expectation for beyond design basis initiating faults (ie annual frequency below 10^{-5} as per SAP FA.5). I found Westinghouse's approach to justify the frequency of a C&I initiated actuation below FA.6 acceptable and in line with the regulatory expectation in the UK. In fact, in accordance with SAP ESS.22 (Ref. 3), for any spurious actuation associated with a common cause failure (CCF) of a complex Class 1 C&I system (such as the PMS) the safety demonstration should not rely on any of the other ESFs provided by the same C&I system. By requiring the spurious initiating event frequency to be below the threshold for fault sequences, Westinghouse conservatively ensures that the core damage frequency meets Target 8 in the SAPs (Ref. 5), without additional claims on other C&I systems (eg the DAS).

55. In the resolution of the C&I aspects covered in GI-AP1000-CI-04.A1 and GI-AP1000-CI-04.A2:

- Westinghouse justified in Ref. 13 that the C&I-initiated frequency of spurious actuation of the PMS functions protected by the SOB is below 10^{-7} per year. The full assessment of the reliability analysis supporting this claim is presented in Section 4.2.3 of this report.

- Westinghouse also provided a justification of the probability of failure on demand of the PMS (including the SOB). I verified in Refs 30 and 38 and was content that, after introduction of the UK SOB, the PMS reliability claim is met (ie 10^{-3} pfd). The full assessment of the PMS reliability is presented in Ref. 39 in the context of GI-AP1000-CI-08 close-out.

56. Although the spurious actuation of the ADS stages 1 to 3 is less critical from a nuclear safety perspective than other squib valve actuations, in the close-out of this GDA issue I also verified that the introduction of the SOB on these MOVs does not cause any safety detriment. In this regard, Ref. 13 shows that, while the effect of the application of the SOB to the ADS MOVs does not worsen significantly the probability of failure on demand of the PMS, it helps to reduce the C&I-initiated spurious operation. I found that

this justification is broadly acceptable to support the introduction of SOBs for ADS stages 1 to 3 MOVs.

57. In conclusion, with the support of fault studies, PSA and mechanical engineering ONR inspectors, I verified that the justification provided against GI-AP1000-CI-04.A1 and GI-AP1000-CI-04.A2 is in line with the expectations in their respective disciplines. When also considering the C&I conclusions in this section and the outcome of the assessment of GI-AP1000-CI-04.A4 (see Section 4.2.3 of this report), I am content that Westinghouse has provided an adequate design BSC and Actions 1 and 2 of this GDA issue can be closed.

4.2.2 Action 3

58. Action 3 of this GDA issue required Westinghouse to formally introduce the SOBs via DCP for the UK **AP1000**.

59. Before the restart of the **AP1000** GDA, Westinghouse had already issued the following DCPs to incorporate the SOB in the standard **AP1000** design:

- APP-GW-GEE-2411 Rev. 0 (Ref. 34), introducing the SOB for the ADS valves
- APP-GW-GEE-4291 Rev. 0 (Ref. 35), extending the scope of the SOB to the IRWST injection squib valves
- APP-GW-GEE-4823 Rev. 0 (Ref. 36), modifying the logic by which the ADS and IRWST injection squib valves are blocked via the SOBs

60. In the assessment of Refs 34 to 36, I verified that these DCPs are incorporated for the UK **AP1000** reactor and found confirmation for that in the design reference point for the **AP1000** GDA closure (Ref. 33).

61. In the close-out of this GDA issue, Westinghouse issued another DCP (APP-GW-GEE-5280 Rev. 0, Ref. 37) in relation to the SOB for the UK **AP1000** reactor. The purpose of this DCP is to:

- modify the design of the standard plant SOB to meet the reliability target set for the UK **AP1000** reactor (ie reducing the PMS spurious operation frequency below 10^{-7} per annum for the ESFs protected by the UK SOB); and
- add SOBs to the containment recirculation squib valves.

62. I assessed Ref. 37 and found that it is broadly consistent with the safety justification in the SOB BSC (Ref. 13), whose assessment is reported in Section 4.2.3 of this report. I also verified that the DCP in Ref. 37 is in the design reference point for the **AP1000** GDA closure (Ref. 33). As the full implementation of this DCP is only expected post GDA, the justification of the detailed design of the UK SOB will be required as part of the revision of the SOB BSC (see Assessment Finding CP-AF-AP1000-CI-006 in Annex 1).

63. In conclusion, on the basis of the assessment of Refs 34 to 37, I found that these DCPs address the expectation set in GI-AP1000-CI-04.A3 for the formal introduction of the SOB in the UK **AP1000** reactor and I am content that Action 3 of this GDA issue can be closed.

4.2.3 Action 4

64. Action 4 of this GDA issue requested Westinghouse to provide a design justification of the SOB for the UK **AP1000** reactor.

65. Westinghouse submitted the design substantiation of the UK SOB in the form of a BSC (Ref. 13). Westinghouse also separately submitted compliance documents against IEC standards (Refs 14 and 55). The BSC for the SOB in Ref. 13 provides a comparison of the standard plant SOB (introduced through the DCPs in Refs 34 to 36) and the design proposed for the UK **AP1000** reactor (introduced via the DCP in Ref. 37). I found that Westinghouse's approach taken in Ref. 13 (ie comparison of standard and UK SOB designs) provides the evidence of an optioneering exercise used to determine the ALARP solution proposed for the UK **AP1000**. However, in my assessment I focused my attention on the design of the SOB proposed for the UK **AP1000** and its safety demonstration.

66. In the following, the section is subdivided into three main areas of focus for this GDA closure, ie the architecture / design of the SOB, its diversity and reliability estimation. In the assessment of Ref. 13, I raised RQ-AP1000-1723 (Ref. 25) to seek clarification regarding Westinghouse safety case for the UK SOB.

Architecture and design of the SOB

67. Westinghouse clarified in Ref. 13 that, through the DCP in Ref. 37, the SOB for the UK **AP1000** reactor will utilise an interface device that is simpler than the current CIM interface. As described in Ref. 37, the modification is needed to ensure that the spurious actuation of signals protected by the blockers meets the expectation for a beyond design basis event in the UK. According to Ref. 37, the UK SOB prevents actuation signals from reaching the squib valves and ADS MOVs. I found that this modification enhances the design of the SOB in that it mitigates the risk of spurious actuations initiated by failures in the CIM.

68. In Ref. 13, Westinghouse explained that from a functional viewpoint the UK SOB (Ref. 37) duplicates the function of the standard plant SOB (Refs 34 to 36), eg utilising the same inputs. Note that, as in the standard **AP1000** plant design, there are four UK SOBs, one per PMS safety division.

69. Ref. 13 provides a justification of the architecture of the UK SOB, which is designed to minimise the impact on the overall PMS pfd and to meet the spurious actuation target. I reviewed the architecture of the UK SOB in Ref. 13 and found that:

- redundancy is provided in the UK SOB design to improve its overall availability;
- the UK SOB shares the power supply (PS) with the PMS in the same division, hence ensuring that a loss of PS feeding each PMS division minimises the risk of spurious actuations and the impact on the actuation on demand;
- the energise-to-block design of the UK SOB ensures that the block is removed in case of internal PS failures (eg converter fault); and
- the UK SOB architecture allows a manual unblocking both from the MCR and from the MCR / RSR transfer switch.

70. Note that Assessment Finding CP-AF-AP1000-CI-004 (raised as part of GI-AP1000-CI-10 closure) requests the licensee to justify the scope of the functions performed by the Class 1 switches in the UK RSR. As part of its resolution, the licensee should give consideration to providing the UK SOB manual input from the UK RSR rather than from the MCR / RSR transfer switch, considering the overall safety impact in an ALARP argument (see Ref. 29 for context).

71. I judged that the DCP in Ref. 37 and the BSC in Ref. 13 provide adequate confidence for the closure of this GDA issue, because they adequately de-risk future phases in the **AP1000** development by defining the overall architecture of the UK SOB and its

interface with the rest of the PMS. The key components in the UK SOB design (eg the comparators) are also identified in Ref. 13, providing confidence that the reliability target can be met on the basis of the specific failure rates. During detailed design, the licensee shall ensure that the implementation of the UK SOB meets the expectations for a Class 1 system and its justification is updated accordingly (see Assessment Finding CP-AF-AP1000-CI-006 in Annex 1).

72. As part of the justification of the UK SOB in Ref. 38, I was content that Westinghouse considered the expectations in IEC 61508-2 (Ref. 51) and IEC 61513 (Ref. 50). In Ref. 55, Westinghouse shows conformance against the expectation in IEC 61513 considering the UK SOB as part of the PMS system (see assessment in Ref. 39). Ref. 14 provides Westinghouse's demonstration of the UK SOB design conformance against the clauses in IEC 61508-2. Ref. 14 identifies compensating activities where the maturity of the design expected for this GDA issue closure does not allow completing the exercise. I am content that the safety plan of Ref. 38 provides a commitment to address these points as part of the future development of the UK SOB design. The licensee shall ensure that evidence of the completion of the compensating activities in Ref. 14 is captured as part of safety justification of the UK SOB detailed design (see Assessment Finding CP-AF-AP1000-CI-006 in Annex 1). More specifically, I raised an assessment finding for the licensee to provide a full justification of the techniques and measures proposed for the UK SOB, considering the expectation in IEC 61508-2 for its safety classification and its reliability claim (see Assessment Finding CP-AF-AP1000-CI-006 bullet (a) in Annex 1).

73. In my assessment of Ref. 14, I found that that only "shall" statements of IEC 61508-2 are provided with a full CAE trail with gaps and compensating measures identified where necessary; "may" and "should" statements are either not addressed or do not have gaps or compensating measures identified. It is considered necessary for these informative aspects of the standard to be considered in the development of the detailed design for the UK SOB, to determine whether adequate measures have been taken to reduce risks as low as is reasonably practicable. For this reason, in line with the expectations raised in RQ-AP1000-1707 (Ref. 45) for other AP1000 C&I systems, I raised an assessment finding for the licensee to address "may" and "should" clauses and sub-clauses in IEC 61508-2 conformance assessment, or, if this is not considered reasonably practicable, to provide a full justification for the position taken (see Assessment Finding CP-AF-AP1000-CI-006 bullet (d) in Annex 1).

74. On this basis, I found the design of the UK SOB and its justification in Ref. 13 adequate to address the key applicable SAPs and the regulatory expectation for this GDA issue closure.

Diversity of the SOB

75. In the assessment of Ref. 13, I verified that the Westinghouse's proposed design for the UK SOB provides an adequate protection against CCFs with the PMS (see EDR.3). Because the SOBs are introduced to cope with failure in the PMS, the expectation is that the design of the SOB provides sufficient diversity from the PMS. Ref. 13 highlights that protection against CCF is sought in the design of the UK SOB, eg avoiding use of software in the SOB and using different technology / development processes for the SOBs from the PMS AC160.

76. At high level, I was content that the substantiation for the diversity claim in Ref. 13 provides adequate confidence of the resilience of the SOB against CCF with the PMS. However, I raised queries in RQ-AP1000-1659 (Ref. 22) and RQ-AP1000-1704 (Ref. 24) to clarify the impact of shared components between the PMS and the SOB (eg field instrumentation). The responses to these RQs (Refs 23 and 24) showed that when considering the field instrumentation the UK SOB design still ensures that the

spurious actuation events are beyond design basis (see discussion on reliability later in this section of the assessment report).

77. As the detailed design of the UK SOB is expected to be completed post GDA and other aspects of its operation will need input from the licensee (eg regarding its maintenance strategy), I raised an assessment finding for the licensee to verify that the final design and operation of the UK SOB provide adequate diversity from the PMS (see Assessment Finding CP-AF-AP1000-CI-006 bullet (b) in Annex 1).

78. I also verified that the introduction of the SOB as part of the PMS does not compromise the overall diversity of the Class 1 primary protection system from the secondary protection system (ie the DAS), which is also based on discrete electronics. I was content that the PMS / DAS diversity analysis (Ref. 42) provided in GI-AP1000-CI-03 closure accounts for the UK SOB as part of the PMS. Note that the detailed assessment of Ref. 42 is out of scope for this report and is provided in Ref. 43.

79. In conclusion, I found that the diversity justification provided in Ref. 13 was adequate for this GDA resolution (eg in line with the expectation in SAP EDR.2). As part of the resolution of CP-AF-AP1000-CI-03 (see Ref. 43) the licensee shall verify that the detailed design of the SOB ensures adequate diversity between the UK SOB (part of the PMS) and the UK DAS. Also note that the demonstration of diversity between the UK SOB and the PLS / DDS is expected in the resolution of AF-AP1000-CI-36 (See Ref. 5 for context).

Reliability of the SOB

80. The reliability estimation of the UK SOB in Ref. 13 was supported by a failure rate calculation in Ref. 40. In the assessment of Ref. 40, I verified that it addresses previous concerns raised in RQ-AP1000-1371 (Ref. 21) on the reliability approach, eg regarding the:

- consideration of common mode failures between redundant components in the UK SOB (eg redundant comparators);
- coverage of all of the active and passive components of the UK SOB design; and
- source of reliability data.

81. I found that the reliability estimation provided in Refs 13 and 40 is adequate for this GDA issue closure because:

- By using the methodology in Ref. 28 for the UK SOB reliability calculations, Westinghouse's approach in Refs 13 and 40 is in line with the PSA for the UK **AP1000** reactor.
- Ref. 13 shows that the frequency of spurious operation initiated by a C&I failure in the PMS (including SOBs) is below 10^{-7} per annum.
- Refs 30 and 41 provide confirmation that, considering CCF between SOBs in different PMS divisions, the ESFs protected by the blockers meet the PMS reliability target (ie pfd 10^{-3}).

82. Although the focus of this GDA issue is about software / systematic faults causing a PMS spurious actuation (see Section 1.3 of this report), in GI-AP1000-CI-04 closure I also verified that the contribution of the field instrumentation to the reliability calculation is acceptable. As discussed in Section 1.3 of this report, the guidance in ESS.22 (paragraph 418 in Ref. 5) does not apply when the spurious actuation is due to faults in the field instrumentation and hence other PMS ESFs can be credited, provided that

they are not relying on the same failed sensors. For this reason, SAP FA.5 can be considered as design basis limit for these initiating events. In the assessment of Ref. 13, I sought confirmation that, when considering the field instrumentation, the spurious actuation frequency of the PMS still meets the expectation for beyond design basis initiating events. In the responses to RQ-AP1000-1659 (Ref. 22) and RQ-AP1000-1704 (Ref. 24), Westinghouse provided adequate confidence that the proposed architecture of the UK SOB meets the reliability target. I expect that these reliability figures will be confirmed once the field instrumentation is selected for the UK **AP1000** reactor (see Assessment Finding CP-AF-AP1000-CI-006 bullet (c) in Annex 1). The verification that the PSA targets for these scenarios are met is expected as part of the PSA evaluation as "normal business" during licensing/site-specific phases.

83. The calculations in Refs 13, 40 and 41 are based on a number of assumptions which should be verified when the detailed selection of components (including the field instrumentation) is finalised and the PMS technical specification is completed for the UK **AP1000** reactor. For example, on the basis of the standard **AP1000** plant, Ref. 13 makes certain assumptions on the channel operation test (COT). The expectation is that the test procedures for the UK SOB will be finalised post GDA as it should consider the licensee's decision on the maintenance strategy for the UK **AP1000** reactor. As part of this activity, I expect verification of the consistency with the assumption in the reliability assessment, eg:

- ensuring that the COT proposed for the UK SOB qualifies as a proof test (eg separately testing both core makeup tank levels and undervoltage relays) rather than being a functional test (eg testing the function as a whole); and

- confirming the frequency of the COT (92 days in the standard plant **AP1000** reactor as required in the US regulatory context).

84. Additionally, I expect a refinement of reliability estimation post GDA, to provide more meaningful risk-informed information for the operation and maintenance of the UK SOB, eg:

- considering a more realistic probability of fault detection based on detailed design choices;

- including only the dangerous failures in the reliability block estimation; and

- using a value for the CCF (ie beta factor) accounting for the specific features of the design and installation of the UK SOB, eg considering guidance in IEC 61508-6 Annex D (Ref. 9).

85. In response to RQ-AP1000-1704, Westinghouse included in Ref. 13 a number of sensitivity analyses on the most critical components and parameters, which I found adequate to de-risk future phases of the UK **AP1000** development. On this basis, I judged that the reliability estimation provided against GI-AP1000-CI-04 is adequate to address this GDA issue and I raised an Assessment Finding for the licensee to revise the reliability analysis for the UK SOB taking into consideration detailed design information as it becomes available post GDA (see Assessment Finding CP-AF-AP1000-CI-006 bullet (c) in Annex 1).

4.3 Comparison with Standards, Guidance and Relevant Good Practice

86. The key standards that informed my assessment, and which I considered to represent RGP for the SOB, are provided in Table 3 above. In my assessment, I am content that Westinghouse adequately addressed these standards to meet the expectation for GDA closure.

4.4 Assessment Findings

87. During the close-out of this GDA issue, I identified an assessment finding for a future licensee to take forward in its site-specific safety submissions. I have provided details in Annex 1.

88. This finding does not undermine the generic safety submission (ie the GDA safety case) and is primarily concerned with the provision of detailed safety case evidence, which should become available as the project progresses through the detailed design, construction and commissioning stages.

5. CONCLUSIONS

89. This report presents the findings of the assessment of GDA Issue GI-AP1000-CI-04 PMS Spurious Operation relating to the **AP1000** GDA closure phase.

90. In conclusion, I am satisfied that the submissions have been addressed in this GDA issue because:

- Westinghouse has provided an adequate safety case in the PCSR for the spurious actuation of ADS valves (both squib and MOVs);
- Westinghouse has provided an adequate safety case in the PCSR for the spurious actuation of IRWST injection line and containment recirculation line squib valves;
- Westinghouse carried out a reliability assessment demonstrating that the addition of the UK SOB to the PMS ensures that the spurious actuation events protected by the blockers are beyond design basis;
- Westinghouse showed that the addition of the blockers is not detrimental in meeting the pfd for the related PMS ESFs;
- Westinghouse issued a DCP (APP-GW-GEE-5280, Ref. 37) to implement the UK SOB design;
- Westinghouse provided a demonstration of the adequacy of the UK SOB in a BSC and also justified compliance with relevant ONR SAPs (Table 1) and standards (eg IEC 61508-2 and IEC 61513); and
- Westinghouse de-risked future phases of the UK SOB design by identifying compensating activities to be addressed post GDA, during its detailed design.

91. In the close-out of this GDA issue, I raised an Assessment Finding to capture a number of technical issues that are expected to be addressed post GDA, when the detailed design information becomes available.

92. Overall, on the basis of my assessment, I am satisfied that GDA Issue GI-AP1000-CI-04 can be closed."

6. REFERENCES

1. ONR HOW2 Guide NS-PER-GD-014, Purpose and Scope of Permissioning. http://www.onr.org.uk/operational/assessment/index.htm
2. ONR Assessment Rating Guide, TRIM 2016/118638
3. Safety Assessment Principles (SAPs), (www.onr.org.uk/saps/saps2014.pdf)
4. Office for Nuclear Regulation (ONR) Permissioning inspection, Technical Assessment Guides (www.onr.org.uk/operational/tech_asst_guides/index.htm)
5. Step 4 Control and Instrumentation Assessment of the Westinghouse **AP1000** Reactor, Assessment Report: ONR-GDA-AR-11-006 Revision 0 www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf
6. Not used.
7. GDA Issue Close-out phase – Control and Instrumentation Assessment of the Westinghouse **AP1000** Reactor, Control and Instrumentation GDA Issues Closure Guidance Document February 2015, TRIM 2015/84414
8. IEC 61508-2:2010, Nuclear power plants. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
9. IEC 61508-6:2010, Nuclear power plants. Functional safety of electrical/ electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
10. ONR-GDA-AP-14-001, **AP1000** GDA C&I Assessment Plan, TRIM 2015/149263
11. Resolution Plan for GI-AP1000-C&I-04, TRIM 2016/92077
12. Altran S.P1641.40.TSC267.3 – ONR/T27 Review of Submissions for the closure of GDA Issue 04 PMS Spurious Operation – Issue 2.0, TRIM 2017/80901
13. UKP-PMS-GLR-003 Revision 1, United Kingdom **AP1000**® PMS Spurious Operation Basis of Safety Case, TRIM 2016/492565
14. UKP-PMS-GLR-013 Revision 0, United Kingdom **AP1000** IEC 61508-2 Compliance Matrix for PMS Spurious Actuation Blocking Hardware – TRIM 2016/312938
15. ONR-NR-AR-16-014, **AP1000** Assessment Report – GI-AP1000-ME-01, TRIM 2016/275007
16. Not used.
17. ONR-NR-AR-16-038, **AP1000** Assessment Report – GI-AP1000-CC-02, TRIM 2016/274964
18. ONR-NR-AR-16-028, **AP1000** Assessment Report – GI-AP1000-CC-FS-08, TRIM 2016/274926
19. **AP1000** European Design Control Document, EPS-GW-GL-700 Revision 1, March 2011, TRIM 2011/81804
20. RQ-AP1000-1368 – **AP1000** Comments on APP-PXS-GEC-001 Rev A, 13 November 2015, Full Response – TRIM 2015/429123
21. RQ-AP1000-1371 – Comments on UKP-PMS-GL-006 Rev. 0, 10 December 2015, Full Response, TRIM 2015/468047
22. RQ-AP1000-1659 – Clarifications on Blocker Reliability Estimation (CI-04), 13 September 2016, Full Response, TRIM 2016/360473
23. RQ-AP1000-1680 – Clarification on GI-AP1000-CI-04, 29 September 2016, Full Response, TRIM 2016/381093

24. RQ-AP1000-1704 – Further Clarification on CI-04, 19 October 2016, Full Response, TRIM 2016/407612
25. RQ-AP1000-1723 – Comments on the PSO BSC (UKP-PMS-GLR-003 Rev 0) 21 November 2016, Full Response – TRIM 2016/452936
26. WEC-REG-1552N – Enclosure 1 – UKP-GW-GL-793 Revision 1, **AP1000** Pre-Construction Safety Report, 31 January 2017, TRIM 2017/43700
27. WEC-REG-1426N – Enclosure 1 – UKP-PMS-GLR-002 Revision 2, United Kingdom **AP1000** Component Interface Module Safety Case Basis, 29 November 2016
28. WNA-IG-00064-GEN Rev. 2, "Reliability and Availability Analysis Methods", Westinghouse Electric Company LLC, TRIM 2016/227310
29. ONR-NR-AR-16-036 GDA close-out for the **AP1000** reactor, GDA Issue GI-AP1000-CI-10, TRIM 2016/274949
30. UKP-PMS-GLR-001 Revision 2 – UK **AP1000** Protection and Safety Monitoring System Safety Case Basis, December 2016, TRIM 2016/502555
31. APP-PXS-GEC-001 Rev 0, Consequences of Spurious Actuation of the PXS Recirculation Squib Valves, October 2016, TRIM 2015/444148
32. WNS-DCP-002234 Revision 0, **AP1000** Plant Spurious ADS Stage 4 and IRWST Injection Expert Panel Assessment, Westinghouse Electric Company LLC, TRIM 2016/306425
33. UKP-GW-GL-060 - Revision 10 – United Kingdom **AP1000** Design Reference Point for UK GDA - 31st January 2017, TRIM 2017/18158
34. APP-GW-GEE-2411 Rev 0, ADS Diverse Actuation Block, 28 March 2016, TRIM 2016/132667
35. APP-GW-GEE-4291 Revision 0, Change to Address Spurious Actuation of the IRWST Squib Valves, 5 August 2016, TRIM 2016/312971
36. APP-GW-GEE-4823 Rev 0, ADS & IRWST Injection Blocking Device Logic Change, 15 September 2015, TRIM 2015/346346
37. APP-GW-GEE-5280 Revision 0, Design Changes to the ADS and IRWST Blocker in Support of UK GDA CI-04 BSC, 6 September 2016, TRIM 2016/389109
38. UKP-PMS-GLR-001 Revision 2 – United Kingdom **AP1000** Protection and Safety Monitoring System Safety Case Basis, 22 December 2016, TRIM 2016/502555
39. ONR-NR-AR-16-034 GDA close-out for the **AP1000** reactor, GDA Issue GI-AP1000-CI-08, TRIM 2016/274946
40. UKP-PMS-GL-006 Rev 2, Failure Rate Estimation of the PMS ADS and IRWST Injection Blocking Device Assembly, TRIM 2016/243558
41. RQ-AP1000-1737 PMS Reliability Claims, 22 November 2016, Full Response, TRIM 2016/455058
42. UKP-GW-GLR-023 Revision 2, United Kingdom **AP1000** Diversity Analysis of the Protection and Safety Monitoring System (PMS) and the Diverse Actuation System (DAS), December 2016, TRIM 2016/502495
43. ONR-NR-AR-16-030 GDA close-out for the **AP1000** reactor, GDA Issue GI-AP1000-CI-03, TRIM 2016/274940
44. UK **AP1000** – GDA Step 4 report and publications, ONR, www.onr.org.uk/new-reactors/ap1000/reports.htm
45. RQ-AP1000-1707 - Treatment of Should and May Clauses in Standards Compliance Reviews - Stephen Wardle - 18th October 2016 - Acknowledgement and Full Response TRIM 2016/404986.

46. NS-TAST-GD-051 Revision 4, The purpose, scope and content of safety cases – www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf
47. Westinghouse UK **AP1000** Generic Design Assessment Resolution Plan for GI-AP1000-CC-02 PCSR Rev. 3 www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf
48. NS-TAST-GD-046 Revision 3, Computer Based Safety Systems, April 2013 www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf
49. IEC 61226:2009 Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions
50. IEC 61513:2011 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems
51. IEC 61508-2:2010 Nuclear power plants – Functional safety of electrical/ electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
52. ONR/T2723: Support for **AP1000** C&I GDA Issues Resolution Work Package Description for SMART Device Justification for Use, Altran, S.P1641.27.3, Issue 1, TRIM 2017/47237
53. ONR-NR-AR-16-017 GDA close-out for the **AP1000** reactor – GDA Issue GI-AP1000-PSA-01, TRIM 2016/275018
54. ONR-NR-AN-16-026 Westinghouse **AP1000** Assessment Note – Structural Integrity of Squib Valves, TRIM 2017/45708
55. UKP-PMS-GL-012 Rev. 1, United Kingdom **AP1000** IEC 61513 Claims, Arguments and Evidence for the Protection and Safety Monitoring System, TRIM 2016/482514

Annex 1

Assessment Finding to be addressed during the Forward Programme – Control and Instrumentation

Assessment Finding Number	Assessment Finding	Report Section Reference
CP-AF-AP1000-CI-006	The licensee shall develop the safety case for the UK spurious operation blocker (SOB) and implement the safety plan given in UKP-PMS-GLR-003 Rev. 1. This should include, but not be limited to: a. providing a full justification of the techniques and measures proposed for the UK SOB safety lifecycle development against the expectations in IEC 61508-2; b. substantiating any claims of diversity between the design of the UK SOB and the PMS, based on detailed design information; and c. updating the reliability analyses of the PMS (including the UK SOB), using detailed design information d. addressing “should” and “may” statements in IEC 61508-2 conformance assessments for the UK SOB. For further guidance on this assessment finding, see Section 4.2 in this report and see TOs GI-04.TO2-2.1.2.1.2-1, GI-04.TO2-2.1.2.1.2-2, GI-04.TO2-2.1.2.2.2.1-1 and GI-04.TO2-2.1.2.2.2.1-2 as listed in Table 3.3 of Ref. 12.	Sections 4.2.2 and 4.2.3