New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-CI-10 - Provision of Class 1 Displays and Controls in an Alternate Location

Assessment Report: ONR-NR-AR-16-036
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 (Westinghouse) is the reactor design company for the **AP1000**® reactor. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues require resolution prior to award of a Design Acceptance Confirmation (DAC) and before any nuclear safety-related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the areas of control and instrumentation. Specifically, this report addresses GDA Issue GI-AP1000-CI-10 regarding the provision of Class 1 displays and controls in an alternate location.

This GDA issue arose in Step 4 due to the absence of Class 1 display and control equipment outside the main control room (MCR) in the standard **AP1000** plant. In the resolution of this GDA issue, ONR requested Westinghouse to consider providing:

- Class 1 display and control provisions in an alternate location; or
- a strong justification as to why the standard **AP1000** reactor arrangements (that is, Class 1 displays and controls in the MCR and lower classes elsewhere) is acceptable in the UK and why it is not reasonably practicable to provide the Class 1 provisions in an alternative location.

The Westinghouse GDA Issue Resolution Plan stated that their approach to closing this issue was to:

- assess the feasibility of upgrading the displays and controls to Class 1 (either in the remote shutdown room (RSR) or in an alternate location); and
- develop a justification for the solution retained for the UK **AP1000** plant and clarify how this meets the ONR expectations.

My assessment conclusion is that:

- the optioneering exercise carried out by Westinghouse allowed to adequately explore different design options in the context of the GI-AP1000-CI-10 resolution and to determine the As Low as Reasonably Practicable (ALARP) solution for the alternate location display and control provisions in the UK **AP1000** design;
- Westinghouse's decision to provide Class 1 displays and controls in the RSR for the UK **AP1000** is in line with the ONR expectation for new reactors in the UK; and
- the justification provided for the retained design solution is adequately developed for GDA close-out.

My judgement is based on the following factors:

- review of the safety justifications submitted against this GDA issue and sampling of the supporting evidence;
- Westinghouse's adoption of modern standards to define the requirements for the alternate control location and consideration of the guidance in key ONR Safety Assessment Principles (SAPs); and
- Westinghouse's issuing of the design change proposal to modify the UK **AP1000** plant RSR, providing Class 1 displays and controls.

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

- fully develop the safety case outlined in the submission against this GDA issue, justifying the detailed design of the additional displays and controls provided in the RSR for the UK **AP1000** design; and
- justify the habitability of the RSR for the UK **AP1000** design.

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

In summary, I am satisfied that GDA Issue GI-AP1000-CI-10 can be closed.

LIST OF ABBREVIATIONS

ADS	automatic depressurisation system
ALARP	As Low As Reasonably Practicable
C&I	control and instrumentation
DAC	Design Acceptance Confirmation
DAS	diverse actuation system
DDS	data display and processing system
GDA	Generic Design Assessment
HVAC	heating, ventilation & air conditioning
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
MCR	main control room
ONR	Office for Nuclear Regulation
PCSR	Pre-construction Safety Report
PDSP	primary dedicated safety panel
PIE	postulated initiating event
PMS	protection and safety monitoring system
PSA	probabilistic safety assessment
RQ	Regulatory Query
RSR	remote shutdown room
RSP	remote shutdown panel
SAP	Safety Assessment Principle
SCP	supplementary control point
SDSP	secondary dedicated safety panel
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
WENRA	Western European Nuclear Regulators Association

TABLE OF CONTENTS

1 INTRODUCTION 7
1.1 Background 7
1.2 Overview of GI-AP1000-CI-10 7
1.3 Scope 7
1.4 Method 7
2 ASSESSMENT STRATEGY 9
2.1 Pre-construction Safety Report (PCSR) 9
2.2 Standards and Criteria 9
Table 1: List of applicable SAPs 9
2.3 Use of Technical Support Contractors (TSCs) 10
2.4 Integration with Other Assessment Topics 10
2.5 Out-of-scope Items 10
3 REQUESTING PARTY'S SAFETY CASE 11
4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-CI-10 12
4.1 Scope of Assessment Undertaken 12
4.2 Assessment 12
4.3 Comparison with Standards, Guidance and Relevant Good Practice 19
4.4 Assessment Findings 19
5 CONCLUSIONS 20
6 REFERENCES 21

Tables

Table 1: List of applicable SAPs
Table 2: List of applicable TAGs
Table 3: List of applicable standards

Annexes

Annex 1: Assessment Findings to be addressed during the Forward Programme – GI-AP1000-CI-10

1 INTRODUCTION

1.1 Background

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

2. This report is the ONR's assessment of the Westinghouse **AP1000** reactor design in the areas of control and instrumentation. Specifically, this report addresses GDA Issue GI-AP1000-CI-10: Provision of Class 1 Displays and Controls with one action.

3. The related GDA Step 4 report is published on the ONR website (Ref. 40), and this provides the assessment underpinning the GDA issue. Further information on the GDA process in general is also available on the ONR website (Ref. 41).

1.2 Overview of GI-AP1000-CI-10

4. This GDA issue was raised in Step 4 of the **AP1000** reactor GDA because the standard **AP1000** design is not equipped with Class 1 display and control provisions in an alternate emergency control location outside the MCR.

5. During Step 4 (Ref. 1), ONR highlighted that the alternate monitoring and control provisions for the standard **AP1000** design (ie Class 2 controls and Class 3 displays in the RSR) fell short of the UK regulatory expectation for new reactors.

6. ONR highlighted in Ref. 1 and in the additional guidance (Ref. 13) that, if the requesting party proposed not to provide Class 1 display and control provisions in an alternate location, a strong justification of the adequacy of the solution was expected, including a review of the requirements in the relevant national and international standards and an ALARP argument as to why the provision of Class 1 facilities was not reasonably practicable.

1.3 Scope

7. The scope of this assessment is detailed in the assessment plan in Ref. 2.

8. The assessment focused on the adequacy of the safety justification for the display and control provisions proposed for an alternate control location (ie other than the MCR) in the UK **AP1000** design.

9. In the initial discussions regarding the close-out of this GDA issue, Westinghouse clarified that the RSR was considered for the **AP1000** design as the main alternate location in case of MCR unavailability (for example, see Ref. 39). Therefore, the focus of the assessment for this GDA issue close-out was on the justification of the adequacy of the displays and controls proposed for the RSR in the UK **AP1000** design.

10. The scope of this assessment is appropriate for GDA because it allows for determining whether the conceptual design of the display and control provisions in the RSR meet the expectation in the UK, hence de-risking future phases of the development of the **AP1000** design.

1.4 Method

11. This assessment complies with the ONR internal guidance on the mechanics of assessment within ONR in Ref. 3.

1.4.1 Sampling Strategy

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

13. In this GDA issue close-out, I assessed the main submissions (see Section 3 of this report) and sampled a number of evidentiary documents supporting the claims in the safety justification. The detail of the sampling strategy is reported in Ref. 23.

2 ASSESSMENT STRATEGY

2.1 Pre-construction Safety Report (PCSR)

14. ONR's GDA Guidance to Requesting Parties (Ref. 43) states that the information required for GDA may be in the form of a PCSR, and Technical Assessment Guide (TAG) no. 051 sets out regulatory expectations for a PCSR (Ref. 42).

15. At the end of Step 4, ONR and the Environment Agency raised GDA Issue CC-02 (Ref. 44) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the **AP1000** design reference point.

16. A separate regulatory assessment report is provided to consider the adequacy of the PCSR and closure of GDA Issue CC-02, and therefore this report does not discuss the control and instrumentation (C&I) aspects of the PCSR. This assessment focused on the supporting documents and evidence specific to GDA Issue GI-AP1000-CI-10.

2.2 Standards and Criteria

17. The standards and criteria adopted within this assessment are principally the SAPs, relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles

18. The key SAPs (Ref. 5) applied in the assessment are included in Table 1.

Table 1: List of applicable SAPs

SAP	Title	Reference
ESS.3	Monitoring of plant safety	Ref. 5
ESS.8	Automatic initiation	
ESS.13	Confirmation of operating personnel	
ECS.3	Safety categorisation	

2.2.2 Technical Assessment Guides

19. The TAGs that have been used as part of this assessment are set out in Table 2.

Table 2: List of applicable TAGs

Identification	Title	Reference in this report
TAG-015	Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)	Ref. 6

2.2.3 National and International Standards and Guidance

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

Table 3: List of applicable standards

Identification	Title	Reference in this report
IAEA SSR-2/1	Safety of Nuclear Power Plants: Design	Ref. 7
WENRA Safety Reference Level	Safety Reference Levels for Existing Reactors	Ref. 8
IEC 60965	Nuclear Power Plants: Control Rooms – Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room	Ref. 9
IEC 61226	Nuclear Power Plants: Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions	Ref. 10
IEC 61513	Nuclear Power Plants: Instrumentation and Control Important to Safety – General Requirement for Systems	Ref. 11
IEC 60709	Nuclear Power Plants: Instrumentation and Control Systems – Important to Safety – Separation	Ref. 37

2.3 Use of Technical Support Contractors (TSCs)

21. The assessment of the submissions against GI-AP1000-CI-10 was carried out internally by ONR, without support from TSCs.

2.4 Integration with Other Assessment Topics

22. 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.

23. This assessment of the GDA issue considered the connection with CC-02, in relation to the PCSR chapters whereby claims were associated to the RSR display and control provisions (Chapter 19) and the operation from the RSR (Chapter 13).

24. In the assessment, I consulted with the following specialist areas within ONR to clarify the adequacy of Westinghouse's justification:

- Probabilistic safety assessment (PSA)
- Internal Hazard
- Fault Studies
- Human Factors

2.5 Out-of-scope Items

25. It is noted that, although to some extent AF-AP1000-CI-026, AF-AP1000-CI-027 and AF-AP1000-CI-028 are related to GI-AP1000-CI-10 (see Ref. 1 for context), it is the responsibility of the licensee to demonstrate their closure and so are not addressed as part of this GDA issue close-out.

3 REQUESTING PARTY'S SAFETY CASE

26. The safety case for GDA Issue GI-AP1000-CI-10 is documented in RSR Control Strategy for Class 1 Displays and Controls - ALARP Justification (UKP-OCS-GLR-002 "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls – ALARP Justification" Revs. 0 and 1 respectively in Refs. 27 and 28). This document was issued in accordance with the GI-AP1000-CI-10 Resolution Plan (Ref. 4). The purpose of the document is to:

- describe the standard plant RSR and clarify the context of the modification proposed for the UK **AP1000** design;
- provide the design basis for the design change introducing Class 1 display and control in the UK RSR;
- provide the result of the optioneering exercise carried out for GI-AP1000-CI-10 resolution; and
- substantiate the ALARP argument for the solution proposed for the UK **AP1000** design.

27. Although not identified in the GI-AP1000-CI-10 Resolution Plan (Ref. 4), Westinghouse also submitted RSR Control Strategy for Class 1 Displays and Controls - SAPs Compliance (UKP-OCS-GLR-001 "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls – SAPs Compliance" Revs. 0 and 1 respectively in Refs. 22 and 26), documenting Westinghouse's position as to how the solution proposed for the displays and controls in the UK RSR meets guidance in relevant ONR SAPs. The purpose of the document is to:

- identify the key SAPs relevant for the design of the RSR displays and controls;
- provide a compliance statement against each of the selected SAPs; and
- provide an overall justification of the compliance of the proposed design change against IEC 60965 (Ref. 9).

28. A design change proposal was also issued by Westinghouse to introduce the Class 1 display and control provisions in the RSR for the UK **AP1000** design (APP-GW-GEE-5383 Revs. A and 0 respectively in Refs. 29 and 30).

29. In PCSR Chapters 13 and 19, Westinghouse respectively defined the human factor and C&I equipment requirements associated with the additional Class 1 displays and controls proposed for the UK RSR.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-CI-10

30. This assessment has been carried out in accordance with ONR Guide NS-PER-GD-014, Purpose and Scope of Permissioning (Ref. 12).

4.1 Scope of Assessment Undertaken

31. The scope of the assessment undertaken is to determine whether GDA Issue GI-AP1000-CI-10 can be closed based on Westinghouse's documents submitted as part of the GDA issue close-out.

4.2 Assessment

32. In early engagement on this GDA issue closure, Westinghouse clarified the options available for the **AP1000** design to monitor and control the plant in case of MCR unavailability (see Refs. 14 and 36), which comprises:

    1. The RSR;

    2. The protection and safety monitoring system (PMS) maintenance and test panels in the four PMS cabinet rooms (one per safety division); and

    3. The remote diverse actuation system (DAS) cabinets in the auxiliary building.

33. In the context of this GDA issue resolution, options 2. and 3. above were discounted by Westinghouse, mainly because of human factor considerations (for example, see response to action 151 in Ref. 15). Westinghouse clarified that the alternate control location to be considered for the purpose of this GDA issue is the RSR (option 1 above), which provides extensive monitoring and control capabilities in a single location and is already considered in the standard **AP1000** design as the alternate control location in case of MCR evacuation (Ref. 39). I found Westinghouse's argument acceptable and in line with SAP ESS.3 (Ref. 5), which suggests that, for a nuclear reactor facility, a single emergency location is preferable over multiple control points with limited capabilities scattered around the plant.

34. In the standard **AP1000** design, Class 1 displays, ie PMS safety displays, and controls, ie primary dedicated safety panel (PDSP) and secondary dedicated safety panel (SDSP), are available in the MCR. The MCR is also equipped with Class 2 DAS and Class 3 data display and processing system (DDS) provisions. In the standard **AP1000** design, hardwired Class 2 manual control panel – remote shutdown panel (RSP) – and Class 3 computer-based controls and displays (via the DDS) are available in the RSR. It is noted that the Class 2 switches in the RSR are an input to the PMS and the justification of the adequacy on the non-Class 1 inputs to the PMS is covered via AF-AP1000-CI-027 (see Ref. 1 for context), hence out of scope for this GDA issue close-out. The control of the RSR is enabled from the MCR/RSR transfer panel, whose justification to Class 1 standard is expected post GDA as part of the resolution of AF-AP1000-CI-028 (see Ref. 1 for context).

35. The requesting party's initial position for the close-out of this GDA issue was to justify the displays and control provisions available in the standard plant design (Refs. 14 and 36). The main argument proposed by Westinghouse in Refs. 14 and 36 is that:

    - the MCR evacuation event is extremely unlikely, with an annual frequency below 10^{-7} (1 in 10 million years); and

    - the Class 1 primary protection system (that is, the PMS) is delivering automatic Cat A safety functions in all plant conditions and for any initiating events.

36. While Westinghouse's argument in Refs. 14 and 36 is mainly based on a time at risk argument and on presumption of success of the Class 1 automatic features, ONR expectation (for example, see SAP ESS.3 and ECS.3) is that provisions with adequate safety classification are available in a supplementary control point (SCP) for the operators to monitor the status of the plant and, if required, take any remedial actions. Because of the safety classification of certain safety functions that need to be monitored and/or actuated outside the MCR (Cat A), the expectation in IEC 61513 (Ref. 11) is that Class 1 provisions are also available in an alternate location outside the MCR.

37. From a safety classification perspective, I also found that the provisions proposed in the standard plant RSR (ie Class 3 information available to operators operating Class 1 components through Class 2 switches via the Class 1 PMS) fell short of the UK expectations for the delivery of a Cat A safety function (full Class 1 actuation chain). For example, this proposal introduces a potential risk for an unnecessary manual actuation of onerous safety functions – for example, Cat A automatic depressurisation system (ADS) squib valves – based on lower integrity information (ie the Class 3 DDS displays).

38. More specifically, in Ref. 38 I highlighted that Westinghouse's strategy to address this GDA issue in Refs. 14 and 36 was not compelling because:

- no detailed evidence was provided to support the probabilistic claim of the frequency of the MCR evacuation;
- there was no consideration of the potential for coincident events, such as an event triggering at the same time as the MCR evacuation and a postulated initiating event (PIE) on the plant (for example, an uncontrolled fire in the MCR causing a spurious actuation of the plant and control system, or a seismic event simultaneously causing a fire in the MCR and a PIE on the plant);
- there was no documentation of a full-scale screening of hazards and scenarios potentially necessitating an MCR evacuation;
- Westinghouse's argument was purely probabilistic and there was no consideration of deterministic aspects such as conformance with standards or consideration of relevant good practice in the UK; and
- no compelling argument was provided as to why the upgrade of the displays and controls in the RSR was grossly disproportionate (ALARP demonstration).

39. ONR expectations (Refs. 23 and 38) regarding relevant standards applicable for this GDA issue included, among others:

- International Atomic Energy Agency (IAEA) Specific Safety Requirements/SSR 2/1 (such as requirement no. 66 in Ref. 7) and Western European Nuclear Regulators Association (WENRA) (such as E10.6 in Ref. 8), requiring the essential plant parameters to be available even after the reactor is placed in a shutdown state;
- Section 5.2 in IEC 60965 standard (Ref. 9) on SCPs, requiring:
    - the SCPs to provide a sufficient control over safety functions to reach and maintain a safe shutdown state for the defined set of relevant PIE; and
    - the design basis of the SCP to consider potential coincident events, for example, plant faults after the plant is placed in a shutdown state.

- IEC 61226 (Section 5.4.2 in Ref. 10) and IEC 61513 (Table 2 in Ref. 11), requiring Class 1 systems to provide information and control capabilities to reach the non-hazardous stable state, if any Cat A manual actuations were required; and

- ONR's SAPs (Ref. 5), requiring:

    - an emergency location capable to deal with a wide range of events, including accident conditions (ESS.3);

    - the categorisation of the safety function on the basis of the fault schedule (ECS.3);

    - the need to confirm the correct operation of automatic safety systems (ESS.13); and

    - consideration of the potential risk to manually negate the correct automatic safety system actuation (ESS.8), for example, based on lower integrity information (Class 3 DDS displays available in the standard **AP1000** design RSR).

40. I also pointed Westinghouse to the relevant good practice for the nuclear new build in the UK to have Class 1 displays and controls available in a location outside the MCR (for example, see Ref. 16).

41. In response to Ref. 38, Westinghouse revised their strategy for this GDA issue closure and clarified their intention to provide Class 1 displays in the RSR for the UK **AP1000** design (Ref 17). According to Ref.17, four Class 1 safety displays with soft blocks/resets were proposed for the UK RSR that effectively duplicates the Class 1 PMS safety displays available in the MCR. However, Westinghouse's position in Ref. 17 was that the RSR control provisions (ie Class 2 switches in the RSP and the Class 3 DDS control interface) were acceptable for the UK **AP1000** design.

42. I raised Regulatory Query (RQ) RQ-AP1000-1526 (Ref 18) to determine the acceptability of this proposal (Ref. 17), requesting clarifications on the need to actuate Cat A manual safety functions from the RSR (for example, in shutdown states whereby maintenance activities on the PMS could reduce the availability of its automatic actuations) and on the justification of the probabilistic claims proposed in Ref. 17 (for example, on the quantification of PSA scenarios with loss of the automatic actuation and on the assumptions made on the MCR availability after its evacuation). RQ-AP1000-1526 (Ref 18) also requested Westinghouse to justify the reasonable practicability to provide Class 1 controls in the RSR, comparing the safety benefit and the effort associated with the modification on a grossly disproportionate scale. Although not in the scope of this GDA issue (see AF-AP1000-CI-027, Ref. 1 for context), I highlighted in Ref. 18 that the justification of the Class 2 to Class 1 interface in the standard **AP1000** design (ie input of Class 2 switches from the RSP to the Class 1 PMS) remained a significant risk in licensing space, considering the expectations for safety class segregation (for example, see EDR.2 and ESS.18, Ref. 5).

43. In response to Ref. 18, Westinghouse revised their position on the RSR control safety classification and committed to provide both Class 1 displays and controls in the RSR for the UK **AP1000** design. In Refs. 18 and 19, Westinghouse clarified that the UK RSR will be equipped with hardwired control panels similar to the PDSP available in the MCR.

44. The commitment to provide Class 1 displays and controls in the RSR was formalised by Westinghouse in a letter (Ref. 20), to which ONR responded (letter in Ref. 21) providing high-level positive feedback on the decision. Westinghouse explained that

the full justification of the design solution is included in the main submissions for GI-AP1000-CI-10 (see assessments in Sections 4.2.1 and 4.2.2 of this report).

4.2.1 ALARP Justification in UKP-OCS-GLR-002 "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls – ALARP Justification"

45. Westinghouse submitted Rev. 0 of UKP-OCS-GLR-002 (Ref. 27) containing the safety justification of the RSR display and control solution proposed in the close-out of this GDA issue. The full assessment of this document submitted is recorded in Ref. 23.

46. At high level, Ref. 27 confirmed the proposal in the letter in Ref. 20 (ie provision of both Class 1 displays and controls in the RSR for the UK **AP1000** design). In Ref. 27, Westinghouse explained that, with this modification, the RSR for the UK **AP1000** design includes:

- four divisions of the Class 1 PMS safety displays, of the same type as those available in the MCR; and
- Class 1 dedicated system-level controls to replace existing Class 2 dedicated system-level controls (similar to the PDSP in the MCR but not fully redundant).

47. Westinghouse also clarified in Ref. 27 that, while the Class 1 switches replace the Class 2 RSP controls in the standard plant design, the Class 1 displays are provided in addition to the Class 3 DDS monitors and soft controls (already available in the standard plant RSR).

48. The justification in Ref. 27 was broadly in line with my expectations because:

- Westinghouse carried out an extensive optioneering exercise to determine which is the ALARP solution for the RSR in the UK **AP1000** design;
- Westinghouse presented a structured ALARP justification for the option retained for the UK **AP1000** design, defining high-level claims and substantiating them with argument and evidence; and
- Westinghouse committed to provide in the RSR the same Class 1 display and control capabilities available in the MCR (ie PMS safety displays).

49. With regard to the additional Class 1 display provisions in the RSR, I noted that the complete demonstration of their adequacy (both in the MCR and in the RSR) will need to account for the upgrade to Cat A/Class 1 of the PMS AF100 bus (supporting the operation of the PMS safety displays). This justification is expected as part of the resolution of AF-AP1000-CI-026 and so is out of scope for this GDA issue resolution.

50. A number of technical review points were raised in the review of Ref. 27 in RQ-AP1000-1698 (Ref. 24), for example, regarding:

- the justification of the not fully redundant Class 1 provisions proposed for the RSR;
- the substantiation of the design basis and the operational philosophy of the RSR, justifying its design; and
- the outstanding activities (both design and justifications) associated with this design change proposal to be completed post-GDA during detailed design.

51. The other clarifications requested through RQ-AP1000-1698 were addressed in the RQ full response (Ref. 24) and in the next revision of the document (UKP-OCS-GLR-002, Rev. 1 in Ref. 28), whereby:

- Westinghouse restricted the claims of the justification in Ref. 28 to the displays and controls in the RSR, as opposed to the overall RSR adequacy;
- Westinghouse provided an adequate definition of the design basis of the RSR, both in terms of initiating events and internal or external hazards;
- Westinghouse improved the clarity of the risk assessment section of Ref. 28; and
- Westinghouse confirmed that this modification did not introduce any new significant hazards to the **AP1000** design.

52. With regard to the additional Class 1 control provisions, in Refs. 24 and 28 Westinghouse provided a justification of the solution proposed for the UK RSR, clarifying that:

- the wired connection from the RSR Class 1 controls to the PMS allows for improving the reliability of the design, for example, by eliminating the transmitter/receivers needed for fibre-optic communication in the standard plant design;
- the solution retained for the UK **AP1000** design minimises the risk of a spurious actuation of onerous safety functions by utilising redundant contacts connected to individual switches rather than utilising redundant switches;
- the full duplication of the MCR Class 1 control provisions in the RSR is grossly disproportionate, for example, because of significant impacts (such as the PMS cabinets and to the RSR layout) and the limited safety benefit; and
- any further improvement in the RSR Class 1 controls results in a marginal safety benefit because of the preponderance of the human error probability over the equipment reliability.

53. I judged that Westinghouse's argument in Refs. 24 and 28 for the non-redundant Class 1 controls was broadly acceptable, also considering that additional Class 1 soft controls are available in the UK RSR through the PMS safety displays enabling actuation at component level (as opposed to a system-level actuation through the proposed Class 1 RSR switches).

54. In Ref. 28, Westinghouse included a safety plan section to address the concerns raised in Ref. 24 regarding the expectation post-GDA closure. In Ref. 28, after GDA, Westinghouse committed to:

- verify the detailed design of the solution proposed for the UK RSR against the segregation and separation requirements in IEC 60709 (Ref. 37);
- determine, based on the modified electrical loads in the RSR, the optimum design for the electrical power configuration and transition from MCR to RSR in the event of a MCR evacuation; and
- provide evidence supporting the RSR habitability claim in a loss of RSR heating, ventilation & air conditioning (HVAC) scenario (both in terms of temperature and CO_2 concentration evolution).

55. I verified that the activities in the safety plan in Ref. 26 were out of scope for this GDA issue. Also, because of their reliance on detailed design information or site-specific input, they did not prevent the close-out of this GDA issue. I raised an assessment finding for the licensee to revise UKP-OCS-GLR-002 Rev. 1 (Ref. 28) implementing

the safety plan defined in Ref. 28 (see bullet a) in the assessment finding in Annex 1 in this report).

56. In Ref. 28, Westinghouse also identified as an open point the justification of the radiological protection of the UK RSR considering site-specific hazards (for example, close proximity to Sellafield site for the **AP1000** design proposed for Moorside). The ONR expectation is that the justification should provide an ALARP statement as to why, when considering the site-specific hazards, it is not reasonably practicable to increase the robustness of the UK RSR habitability (for example, carrying out an optioneering exercise). I raised an assessment finding for the licensee to provide a justification of the adequacy of the RSR arrangements in case of an external radiological event (see bullet d) in the assessment finding in Annex 1 in this report).

57. In response to RQ-AP1000-1698 (Ref. 24) and RQ-AP1000-1723 raised on GI-AP1000-CI-04 (Ref. 25), Westinghouse provided a qualitative justification as to why a limited number of switches available in the MCR are not replicated in the RSR (for example, the manual auxiliary spray isolation and the unblocking of the spurious operation blockers of the PMS). The final justification of the scope of the Class 1 RSR switches should take into consideration detailed design aspects (for example, space available in the RSR panel proposed for the UK **AP1000** design) and refined safety analysis (for example, updated fault schedule addressing outstanding fault studies assessment findings and probabilistic calculations based on the UK **AP1000** plant PSA model to estimate the safety benefit). I raised an assessment finding for the licensee to justify the scope of the functions available through the Class 1 switches in the RSR, (see bullet b) in the assessment finding in Annex 1 of this report).

58. In Ref. 28, Westinghouse stated that the use of the RSR is required only after a reactor trip. Although the operational procedure requires tripping the reactor before abandoning the MCR (Ref. 39), the potential for the operation at full or partial power from the RSR could be further reduced by tying the reactor trip to the MCR/RSR transfer panel (hence excluding the scenario by design). In response to RQ-AP1000-1698 (Ref. 24), Westinghouse stated that it did not believe that such a change would improve safety. However the argument in Ref. 24 is high level and the detailed design of the MCR/RSR transfer panel needs to consider the resolution of AF-AP1000-CI-028 (see Ref. 1 for context). I raised an assessment finding for the licensee to substantiate this position providing a rigorous ALARP justification (see bullet c) in the assessment finding Annex 1 in this report).

59. Because of the cross-cutting nature of this GDA issue, many claims in Ref. 26 are associated with PSA, internal/external hazards, fault studies and human factor analyses. As the overall design and safety cases for the **AP1000** design are expected to develop post-GDA, an assessment finding was raised for the licensee to ensure consistency of the claims in the justification in UKP-OCS-GLR-002 (Ref. 28), and in future revisions of UKP-OCS-GLR-001 (Ref. 26) with relevant safety analyses (see bullet e) in the assessment finding in Annex 1 in this report).

60. In conclusion, I found that Ref. 28 provides an adequate clarification of the design modification proposed for the UK RSR and, by providing a justification for the conceptual design solution for the RSR displays and controls, meets the expectations set for a GDA (that is, to de-risk future phases of the UK **AP1000** plant development). On this basis, I judged that the safety justification in Ref. 28 is adequate for the resolution of this GDA issue.

4.2.2 SAP Compliance in UKP-OCS-GLR-001 "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls – SAPs Compliance"

61. In UKP-OCS-GLR-001 Rev. 0 (Ref. 22), Westinghouse provided an explicit compliance assessment against the SAPs considered by Westinghouse relevant for this GDA

issue close-out. This SAP compliance assessment exercise was recorded in a claims, arguments and evidence format in the submission. The full assessment of this document submitted during the close-out of GI-AP1000-CI-10 was recorded in Ref. 23.

62. In the review of Rev. 0 of UKP-OCS-GLR-001 (Ref. 22), I verified that the SAPs considered by Westinghouse included the key principles identified in Section. 2.2.1 of this report.

63. I assessed Ref. 22 and was broadly content with the approach, which provided confidence that the justification for the retained design solution considered ONR's expectations set out in the SAPs (Ref. 5). In addition to the SAP compliance assessment, Ref. 22 also provided an explicit comparison against clauses in IEC 60965 (Ref. 9).

64. I raised queries in RQ-AP1000-1698 (Ref. 24) on Ref. 22, mainly regarding the clarity of the arguments and evidence proposed in this document against specific claims.

65. Westinghouse responded to the RQ (Ref. 24) and submitted Rev. 1 of UKP-OCS-GLR-001 (Ref. 26). I assessed Ref. 26 and found the document was broadly acceptable for this GDA issue closure. I raised an assessment finding for the licensee to revise the document to ensure consistency with the detailed design documentation and safety analysis when finalised post-GDA (see bullet e) in the assessment finding in Annex 1 of this report).

4.2.3 Design Change Proposal in APP-GW-GEE-5383

66. Westinghouse issued a draft design change proposal (APP-GW-GEE-5383, Rev. A in Ref. 29) recording the commitment to provide Class 1 displays and controls in the UK RSR. Westinghouse also explained that its implementation is tracked using a standard dedicated tool used for the **AP1000** design (that is, Westinghouse's SmartPlant® Foundation).

67. I assessed this design change proposal and confirmed that it was in line with the main submissions against GI-AP1000-CI-10 (UKP-OCS-GLR-001 Rev. 1 – Ref. 26 – and UKP-OCS-GLR-002 Rev. 1 – Ref. 27).

68. Westinghouse subsequently issued APP-GW-GEE-5383 in Rev. 0 (Ref. 30) and included the design change in the latest revision of the design reference point for the GDA close-out (Ref. 31). Rev. 0 of APP-GW-GEE-5383 (Ref. 30) confirmed the expectation in Rev. A (Ref. 29), previously assessed.

69. As a full impact assessment of this design change on the UK **AP1000** design is expected only post-GDA, I raised an assessment finding for the licensee to provide a full justification of the adequacy of the detailed design solution retained for the UK RSR (see bullet a) in the assessment finding in Annex 1 of this report).

4.2.4 Chapters 13 and 19 of the PCSR

70. In Ref. 32, Westinghouse explained that the PCSR is used for the UK **AP1000** design to record the licensing commitments that will be incorporated in the C&I system specifications post-GDA. On this basis, I sought confirmation that the information related to the RSR in the PCSR was in line with the submissions provided against GI-AP1000-CI-10 (Refs. 26, 28 and 30).

71. I assessed Section 19.3.5 of the C&I PCSR chapter (Ref. 33) and found that it considered the design change proposal in Ref. 30 and was in line with the expectations in Refs. 26 and 30.

72. I also assessed Section 13.6.9 of the Human Factor Chapter of the PCSR (Ref. 33), describing the claims on the displays and controls in the UK RSR. My review confirmed that Section 13.6.9 aligned with the main human factor claims in Refs. 26, 28 and 30.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

73. I verified that the requesting party considered suitable standards and good practice in the design modification proposed against GI-AP1000-CI-10 and concluded that:

- Westinghouse considered the relevant ONR SAPs in the design and provided an explicit compliance assessment against the key safety principles;
- Westinghouse considered the guidance in relevant international standards for supplementary control points (particularly IEC 60965, Ref. 9);
- Westinghouse's design change proposal considered the safety classification expectations in international standards applicable in the UK (IEC 61226 – Ref. 10 – and IEC 61513 - Ref. 11); and
- Westinghouse's proposal was in line with the relevant good practice for new power plants proposed for the UK (see for example Ref. 16).

74. On this basis, I was satisfied that the Westinghouse approach was in line with ONR expectations and that the design solution proposed for the UK RSR was acceptable.

4.4 Assessment Findings

75. During my assessment of GI-AP1000-CI-10, an assessment finding was identified for a future licensee to take forward in their site-specific safety submissions. Details of the assessment finding are contained in Annex 1 of this report.

76. These matters do not undermine the generic safety submission and are primarily concerned with the provision of site-specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages. These items are included in the assessment finding in Annex 1.

5 CONCLUSIONS

77. This report presents the findings of the assessment of GDA Issue GI-AP1000-CI-10 relating to the **AP1000** reactor GDA closure phase.

78. In conclusion, I am satisfied that the submissions addressed this GDA issue because:

- Westinghouse committed to providing Class 1 displays and controls in the RSR;
- Westinghouse has demonstrated an adequate application of the key standards for the alternate control location (ONR SAPs (see Table 1) and IEC 60965 (Ref. 9));
- Westinghouse has engaged in an extensive optioneering exercise, considering various technical solutions in order to determine the ALARP option for the UK RSR;
- Westinghouse raised a design change proposal in APP-GW-GEE-5383 (Ref. 30) to implement the change for the UK **AP1000** design; and
- Westinghouse has adequately de-risked post-GDA activities related to this design change proposal, with justification provided against GI-AP1000-CI-10.

79. In the close-out of this GDA issue, I raised an assessment finding to detail a number of technical issues to be addressed post-GDA, when the detailed design of the RSR Class 1 displays and controls is completed and site-specific issues are considered.

80. Overall, on the basis of my assessment, I am satisfied that GDA Issue GI-AP1000-CI-10 can be closed.

6 REFERENCES

1. Office for Nuclear Regulation (ONR) ONR-GDA-AR-11-006, Rev. 0, Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000 Reactor, November 2011.
2. ONR, ONR-GDA-AP-14-001 Rev 0, AP1000 GDA C&I Assessment Plan, April 2015 – TRIM 2015/149263.
3. ONR, ONR Guidance on Mechanics of Assessment, TRIM 2013/204124.
4. Westinghouse Electric Company LLC, Westinghouse UK AP1000® Generic Design Assessment Resolution Plan for GI-AP1000-C&I-10 Class 1 Displays and Controls, Rev. 4 (revised) www.onr.org.uk/new-reactors/reports/step-four/westinghouse-final-res-plans/resolution-plan-gi-ap1000-ci-10.pdf
5. ONR, Safety Assessment Principles for Nuclear Facilities, Revision 0, 2014, www.onr.org.uk/saps/saps2014.pdf
6. ONR, NS-TAST-GD-005 Revision 7 Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), December 2015 www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf
7. International Atomic Energy Agency (IAEA), IAEA SSR-2/1, Rev.1, Safety of Nuclear Power Plants: Design, 2016, www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf
8. Western European Nuclear Regulators Association (WENRA), Safety Reference Levels for Existing Reactors, 2014, www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf
9. British Standards Institution (BSI), IEC 60965:2009, Nuclear Power Plants: Control Rooms – Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room.
10. BSI, IEC 61226:2009, Nuclear Power Plants: Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions
11. BSI, IEC 61513:2011, Nuclear Power Plants: Instrumentation and Control Important to Safety – General Requirements for Systems
12. ONR, NS-PER-GD-014, Purpose and Scope of Permissioning, www.onr.org.uk/operational/assessment/ns-per-gd-014.pdf
13. ONR, 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
14. Westinghouse Electric Company LLC, WEC-REG-0333N (NPP_JNE_000333) – Enclosure 1 – AP1000 GDA Issue CI-10 ONR Final – 23 September 2015 – TRIM 2015/356059.
15. ONR, AP1000 - C&I Level 4 Action Tracker for C&I GDA Issue Resolution.xlsx – TRIM 2015/72603
16. ONR, ONR-GDA-AR-11-022 Rev. 1, GDA Step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor, March 2013, www.onr.org.uk/new-reactors/reports/step-four/close-out/gi-ukepr-ci-01-close-out.pdf
17. Westinghouse Electric Company LLC, WEC-REG-0729N (NPP_JNE_000729) – Enclosure 1 – Status Update on CI-10 – Class 1 Displays and Controls in the Remote Shutdown Room – Level 4 meeting presentation – March 2016 – TRIM 2016/92381.
18. RQ-AP1000-1526 – Safety Classification of Displays and Controls in the Remote Shutdown Room (GI-AP1000-CI-10) – April 2016 – Full Response – TRIM 2016/180947.
19. Westinghouse Electric Company LLC, WEC-REG-0828N (NPP_JNE_000828) – Enclosure 1 – GI-AP1000-CI-10 – Class 1 Displays and Controls in RSR Optioneering Definition and Evaluation Update – Level 4 meeting presentation – March 2016 – TRIM 2016/132537.

20. Westinghouse Electric Company LLC, WEC-REG-0875R (NPP_JNE_000875) – Letter from Westinghouse – Confirmation of RSR Class 1 Displays and Controls – ALARP Optioneering Choice – April 2016 TRIM 2016/156669
21. ONR, REG-WEC-0034N (JNE_NPP_000034) – Letter to Westinghouse – Progress on GDA Issue GI-AP1000-CI-010 – July 2016 – TRIM 2016/278175.
22. Westinghouse Electric Company LLC, UKP-OCS-GLR-001 – Revision 0 – UK AP1000 RSR Control Strategy for Class 1 Displays and Controls – SAPs Compliance – July 2016 TRIM 2016/289606
23. ONR, AP1000 – GI-AP1000-CI-10 Close-out – Note for the record – TRIM 2016/331231.
24. RQ-AP1000-1698 – Clarification Regarding the Safety Justification Provided Against GI-AP1000-CI-10 – October 2016 – Full Response.
25. RQ-AP1000-1723 – Comments on the PSO BSC (UKP-PMS-GLR-003 Rev 0) November 2016 – Full Response – TRIM 2016/452936
26. Westinghouse Electric Company LLC, UKP-OCS-GLR-001 – Revision 1 – UK AP1000 RSR Control Strategy for Class 1 Displays and Controls – SAPs Compliance –TRIM 2016/484878
27. Westinghouse Electric Company LLC, UKP-OCS-GLR-002 – Revision 0 – UK AP1000 RSR Control Strategy for Class 1 Displays and Controls – ALARP Justification – 19 July 2016 – TRIM 2016/289612
28. Westinghouse Electric Company LLC, UKP-OCS-GLR-002 – Revision 1 – UK AP1000 RSR Control Strategy for Class 1 Displays and Controls – ALARP Justification – TRIM 2016/475161
29. Westinghouse Electric Company LLC, APP-GW-GEE-5383 – Revision A – AP1000 DCP UK Addition of Class 1 Displays and Controls to the Remote Shutdown Room – September 2016 – TRIM 2016/353389.
30. Westinghouse Electric Company LLC, APP-GW-GEE-5383 – Revision 0 – UK Addition of Class 1 Displays and Controls to the Remote Shutdown Room – November 2016 – TRIM 2016/450542.
31. Westinghouse Electric Company LLC, UKP-GW-GL-060, AP1000 Design Reference Point for UK GDA Revision 10 – January 2017 – TRIM 2016/446324
32. Westinghouse Electric Company LLC, UKP-GW-GLR-116 – Revision 0 – UK AP1000 Design C&I Requirements Management Overview – November 2016 – TRIM 2016/449029.
33. Westinghouse Electric Company LLC, WEC-REG-1552N – Enclosure 1 – UKP-GW-GL-793 – Revision 1 – AP1000 Pre-Construction Safety Report – 31 January 2017 – TRIM 2017/43700
34. Not used.
35. Westinghouse Electric Company LLC, WEC-REG-1483N – Enclosure 1 – UKP-PMS-GLR-003 Rev 1 – United Kingdom AP1000 PMS Spurious Operation Basis of Safety Case – December 2016 – TRIM 2016/492565.
36. WEC-REG-0341N - Letter from Westinghouse - Transmittal of C&I Supporting Material Provided to ONR - 30th September 2015 – TRIM 2015/366183.
37. BSI, IEC 60709:2004 – Nuclear Power Plants: Instrumentation and Control Systems – Important to Safety – Separation.
38. ONR, ONR-GDA-CR-15-367 – AP1000 Control and Instrumentation GDA Issues Resolution Technical Meeting on GI-AP1000-CI-10 Class 1 Displays and Controls in the RSR – January 2016 – TRIM 2016/38551.
39. Westinghouse Electric Company LLC, APP-GW-GJP-306 – Revision 2 – AOP-306 – Evacuation of Main Control Room – TRIM 2016/310792.
40. ONR, UK AP1000 – GDA Step 4 Reports and Publications – www.onr.org.uk/new-reactors/ap1000/reports.htm
41. ONR, Generic Design Assessment (GDA) of New Nuclear Power Stations – www.onr.org.uk/new-reactors/index.htm

42. ONR, 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
43. ONR, ONR-GDA-GD-001 Revision 3 – New Nuclear Reactors: Generic Design Assessment – Guidance to Requesting Parties – www.onr.org.uk/new-reactors/ngn03.pdf
44. ONR, Westinghouse AP1000® Generic Design Assessment – GDA Issue: PCSR to Support GDA GI-AP1000-CC-02 PCSR, Revision 3 – www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf

Annex 1

Assessment Findings to be addressed during the Forward Programme – GI-AP1000-CI-10

Assessment finding number	Assessment finding	Report section reference
CP-AF-AP1000-CI-004	The licensee shall: a) implement APP-GW-GEE-5383 in the UK **AP1000** design, providing a justification of the adequacy of its detailed design and implementing the safety plan in UKP-OCS-GLR-002; b) justify of the scope of the functions performed by the Class 1 switches provided in the RSR through APP-GW-GEE-5383; c) provide an ALARP justification for the integration of reactor trip with the transfer of control from the MCR to the RSR; d) substantiate the RSR habitability claims in UKP-OCS-GLR-002; and e) ensure consistency of the claims in the justification of the displays and controls in the RSR with relevant safety analyses (including PSA, internal/external hazards, fault studies, human factors) and operational procedures as the overall design of the **AP1000** design develops post-GDA. For further guidance on this assessment finding, see Section 4.2 of this report, and recommendations CI-10-R-01 to CI-10-R-07 in Ref. 23.	Sect. 4.2.1, 4.2.2, 4.2.3 and 4.4