Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-C&I-08
PMS BSC

MAIN ASSESSMENT AREA	RELATED ASSESSMENT AREA(S)	RESOLUTION PLAN REVISION	GDA ISSUE REVISION
C&I	PSA, FS, FD	3	0

GDA ISSUE:	Shortfalls have been identified in the provision of a claims - argument - evidence structure for the PMS safety demonstration. The PMS is based on non safety equipment and requires an 'added quality' demonstration to be made; this demonstration has proved difficult to understand without a logically structured safety case. In response to our concerns Westinghouse has produced a Basis of Safety Case (BSC) for the PMS covering both the platform and application development. Review of the BSC has identified a number of areas for improvement including, to the SAPs and IEC standards conformance demonstration, and justification of the scope and adequacy of the independent confidence building measures. The PMS safety case needs to incorporate the responses to the PMS related Assessment Findings identified in ONR C&I Assessment Report No. ONR-GDA-AR-11-006, Rev. 0 and to reflect PMS development progress as the design is completed. For further guidance, see T15.TO1.02, T15.TO1.03 T15.TO1.11 and their associated TO2s plus T15.TO2.36 and T15.TO2.43 in Annex 5, and also T16.TO1.01 and its associated TO2s, and T16.TO1.02, T16.TO2.07, T16.TO2.08, T16.TO2.09, T16.TO2.38, T16.TO2.42 and T16.TO2.45 in Annex 6 of ONR C&I Assessment Report No. ONR-GDA-AR-11-006, Rev. 0.
ACTION: GI-AP1000-C&I-08.A1	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the PMS. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-C&I-08.A2	Westinghouse to provide a basis of safety case for the PMS that takes into account the expectations expressed below: The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that Westinghouse has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the

	equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the **AP1000**® C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques. The BSC should identify the pedigree of any COTS and pre-developed components and provide a demonstration of the adequacy of the development arrangements. For older components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety demonstration. The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant Westinghouse safety principles and standards. Given the programmable nature of such complex devices, SAP ESS.27 a special case procedure

	for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design1 should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; • prototype equipment has been produced and subject to performance and qualification testing; With agreement from the Regulator this action may be completed by alternative means.
RELEVANT REFERENCE DOCUMENTATION RELATED TO GDA ISSUE	
GDA Open Issues Documents	GI-**AP1000**-C&I-08, Revision 0 Step 4 C&I Division 6 Assessment Report, No. ONR-GDA-AR-11-006 Revision 0
Technical Queries	TQ-**AP1000**-770, TQ-**AP1000**-787, TQ-**AP1000**-788, TQ-**AP1000**-975, TQ-**AP1000**-1033, TQ-**AP1000**-1034, TQ-**AP1000**-1086, TQ-**AP1000**-1109, TQ-**AP1000**-1116, TQ-**AP1000**-1118 & TQ-**AP1000**-1138
Regulatory Observations	RO-**AP1000**-101
Other Documentation	UKP-PMS-GLR-001

Scope of work:
Westinghouse will continue to provide ABB documentation for review by the ONR in the UK. The PMS BSC shall be revised to address observations identified in the GDA final report and facilitate ONR access in the UK to the detailed evidence, e.g. ABB documentation, used to support the basis of safety case for the PMS.

Deliverables/description of work:

The following deliverables will be provided according to the schedule below:

1. PMS BSC - UKP-PMS-GLR-001, Revision 1
   The revision 0 submission will be revised to address the following observations by ONR:
   a. The relevant TSC TOs identified in the Step 4 C&I Division 6 Assessment Report, ONR-GDA-AR-11-006 Revision 0 will be evaluated early in the resolution plan execution cycle for inclusion in the revision of the PMS BSC as appropriate.
   b. Reference IEC compliance matrices by document number
   c. Provide a map of impact analyses for each AC160 software module
   d. Provide a configuration baseline for the current AC160 software
   e. Identify any errors uncovered in the O1-MOD qualification test reports that did not get assigned a tracker
   f. Confirm that FCB test software has been put under configuration control
   g. Disposition all comments from the TSC and Westinghouse independent reviewers
   h. Address the open issues identified in the ONR deviation matrix
   i. Update the safety plan (UKP-GW-GL-078) to reflect the PMS completion plan. Reference the Safety Plan defining the time schedule for PMS design life cycle documentation
   j. Add a complete Partitions/Claims/Documentation matrix
   k. Reference the PMS RTM through the design phase
   l. Reference the PMS Design Requirements (if completed within GDA, otherwise it will remain an open item)
   m. Reference the PMS EQ Test Procedures and Reports
   n. Reference the DP620 Qualification Documentation (if completed within GDA, otherwise it will remain an open item)
   o. Reference the AI687/688 Qualification Documentation
   p. Reference the CI631/CI527 Category A AF100 Qualification Documentation (will remain an open item)
   q. Reference the **AP1000** PMS Reliability Analysis
   r. Reference the **AP1000** PMS Statistical Test Plan
   s. Update the MALPAS verification process description
2. Standards Compliance Matrices:
   a. IEC 60880 for the PMS Application (UKP-PMS-GL-002)
   b. IEC 61513 for the PMS Application (UKP-PMS-GL-003)
   c. IEC 60987 for the PMS Application (UKP-PMS-GL-004)

Schedule/ programme milestones:

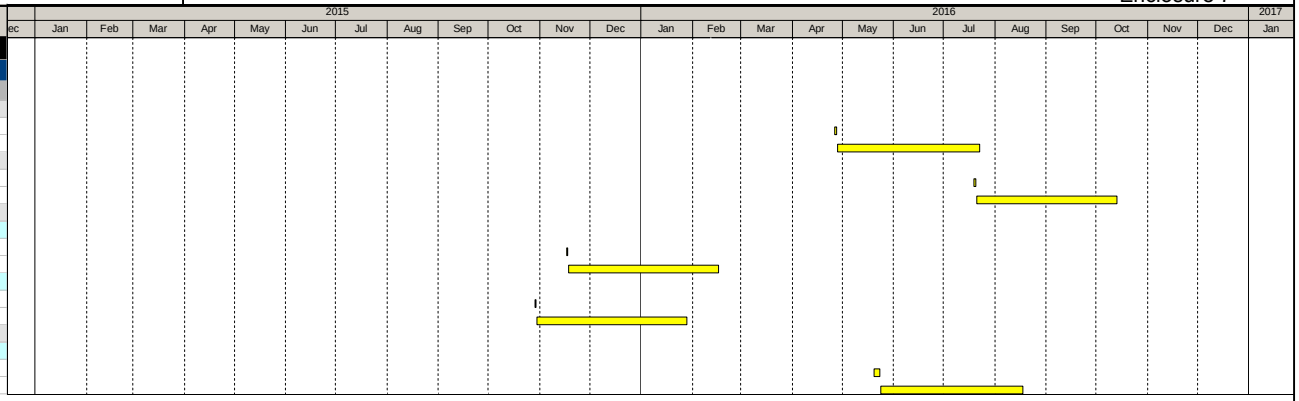
Periodic status meetings will be conducted between Westinghouse and ONR personnel to ensure that C&I GDA open issues are being resolved in a timely and quality manner.

Schedule Overview

The following schedule identifies major work efforts and associated milestones for GI-**AP1000**-C&I-08. The PMS BSC will be revised, internally reviewed and transmitted to

the ONR. If needed based on ONR comments, a subsequent revision to the PMS BSC will be developed and issued.

#	Activity Name
1	**UK Generic Design Assessment (GDA) Resolution Plans (51)**
2	**CONTROL & INSTRUMENTATION**
3	**CI.08 PMS Adequacy of Safety Case-Resolution Plan**
4	**CI.08 SAPs Assessments**
5	SAPs Assessment Rev 1 - Submit to ONR
6	SAPS Assessments Rev. 1 - ONR Review of Submittal
7	**CI.08 PMS BSC Revision 1**
8	PMS BSC Rev.1-Submit to ONR
9	PMS BSC Rev.1-ONR Review of Submittal
10	**CI.08 IEC Standards Compliance Updates**
11	**CI.08 IEC 60880 (UKP-PMS-GL-002) Revision**
12	IEC 60880 Assessment - Submit to ONR
13	UKP-PMS-GL-002-ONR Review of Submittal
14	**CI.08 IEC 60987 (UKP-PMS-GL-004)**
15	IEC 60987 - Submit to ONR
16	UKP-PMS-GL-004-ONR Review of Submittal
17	**CI.08 Supporting Deliverables**
18	**CI.08 AC160 Suitability Analysis (T15.TO2.37)**
19	AC160 Suitability Analysis-Submit to ONR w/ PMS BSC Rev. 1
20	AC160 Suitability Analysis-ONR Review of Submittal w/ PMS BSC Rev. 1



Methodology:

ABB documentation will be provided for review by the ONR in the UK when requested.

The PMS BSC shall be revised to:

1. Reference the PMS compliance documents for the safety assessment principles stored in the Westinghouse document control system.
2. Reference the IEC standards compliance matrices that will be documents in the Westinghouse document control system.
3. Westinghouse will elaborate on additional compensating measures for deviations. These measures include;
    a. For each impact analysis for changed software in the AC160, the software modules impacted will be documented.
    b. A configuration baseline for the AC160 software will be defined that represents the current configuration of the AC160 software.
    c. Review all the test records identified in Appendix: AQD Results For All Partitions in MOD 97-7771, “Final Quality Assessment and Justification Report,” and verify there are no exceptions without a tracking mechanism for closure.
    d. Put test FCB files referenced in test procedures into configuration control.
    e. Reference the Deviation Matrix in the ONR GDA Step 4 report and address the deviations identified in that table.
    f. Describe the error tracking and impact analysis process used by ABB.
    g. Describe where Add Quality Demonstration measures for the original qualification of the AC160 ends and when Westinghouse is claiming production excellence for the maintenance of the product.
    h. Address the TSC TOs associated with GDA Issue 08 in the GDA Step 4 report.
4. An impact assessment on GDA changes to the plant fault studies and PSA on the PMS design will be conducted.
5. PMS BSC to be independently reviewed according the Westinghouse QMS Level 2 Procedure WEC 3.3.3
6. PMS BSC to Identify and justify any data entry facilities and that data integrity is assured (e.g. data from BEACON).

The PMS BSC will reference equipment qualification, reliability analyses, factory integration testing, and site acceptance testing that are applicable to the UK **AP1000** design.

Westinghouse and ONR personnel will conduct periodic review meetings during the course of the Resolution Plan execution to resolve in a timely manner any emergent issue that may impact Resolution Plan schedule and ensure ONR expectations are being met.

All Westinghouse system designs and associated documentation, like the BSC, follow the Westinghouse Quality Management System (QMS) procedures as the methodology.

Specifically, quality and standardisation of technical documents generated as part of this resolution plan are governed under the following procedures:

- Westinghouse QMS, “Westinghouse Electric Company Quality Management System”
  - Section 1.2, “Document and Data Control”
  - Section 2.1, “Quality Policy”
- Westinghouse Level II Procedure WEC 6.1, “Document Control”

Documents that are customer deliverables are subject to the Customer Satisfaction Process, discussed in Westinghouse Level II Procedure WEC 16.8, “Customer Satisfaction”

In addition, the following Westinghouse Level II Procedures provide important rules for creating and handling quality records, and electronic document management:

- WEC 17.1, “Records”
- WEC 17.2, “Electronic Approval”
- WEC 17.3, “Electronic Document Management”

The continued use of use of Claims, Arguments and Evidence (CAE) structure for BSC documents will be employed as identified in T/AST/051, Issue 001, “Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.”

Appropriate technical and licensing reviews will be conducted to ensure that the final version of the BSC will demonstrate compliance to the appropriate SAP’s and guidance provided by ONR. Technical reviews are independent Westinghouse reviews that will focus on CAE being technically correct and producible. Whereas, licensing reviews concentrate on ensuring regulatory requirements are properly addressed and substantiated.

Standards and practices, technology selection and justification, design tools and techniques, and verification and validation techniques will be identified and substantiated in the BSC, as appropriate.

Justification of adequacy:

The above methodology will address issues that ONR has raised in regards to the adequacy of the PMS BSC. This will include appropriate technical and licensing reviews to ensure that the final version of the BSC demonstrates compliance to the appropriate SAP’s and guidance provided by ONR.

Westinghouse considers the aforementioned areas where the PMS BSC will be revised, in accordance with T/AST/051 and per this Resolution Plan, will demonstrate that the PMS BSC will be sufficiently robust to substantiate the claim that the **AP1000** PMS is fit for purpose as described in the BSC.

Impact assessment:

The safety submission document impacted by the implementation of the resolution plan:

- UKP-PMS-GLR-001, “United Kingdom **AP1000** Protection and Safety Monitoring

System Safety Case Basis." as described in the work scope and methodology
- UKP-GW-GL-793, Chapter 19, "**AP1000** Pre-Construction Safety Report," Updating reference to PMS BSC

The diversity analysis developed through the resolution of GDA Issue GI-**AP1000**-CI-03 will need to be addressed by the PMS BSC. In addition, the resolution of GDA Issue GI-**AP1000**-FD-03 on the use of BEACON may impact work on this GDA Issue. Lastly, the BSC developed through the resolution of GDA Issue GI-**AP1000**-CI-04 on PMS spurious operation will need to be addressed by the PMS BSC.

It is expected that the PCSR Chapter 19 will be updated to provide stronger links between the BSC and PCSR. Information from the BSC will be included as appropriate.