Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-C&I-09
CIM – Adequacy of safety case

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

GDA ISSUE:	Shortfalls have been identified in the provision of a claims - argument - evidence structure in the CIM safety case. The CIM is a critical component of the primary protection system. It is based on Field Programmable gate array (FPGA) technology and is supplied by a company with little experience in the nuclear sector. In response to our concerns Westinghouse has produced a Basis of Safety Case (BSC) for the CIM. Assessment of the BSC has identified a number of areas for improvement. The key areas for improvement are: • demonstration that the development process is compliant or equivalent to IEC standards; and • identification of the evidence to support the demonstration. The BSC should document the standards compliance and address issues related to use of tools and test coverage. The rigour of the safety demonstration provided in the BSC should reflect the reliability claim on the CIM. The CIM safety case needs to incorporate the responses to the CIM related Assessment Findings identified in ONR C&I Assessment Report GDA-AR-11-006 Revision 0 and to reflect CIM development progress as the design is completed. For further guidance, see T15.TO1.05, T15.TO1.06, T15.TO1.07, T15.TO1.08, T15.TO1.10 and their associated TO2s in Annex 5 of ONR C&I Assessment Report GDA-AR-11-006 Revision 0.
ACTION: GI-AP1000-C&I-09.A1	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the CIM. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-C&I-09.A2	Westinghouse to provide the basis of safety case for the completed design of the CIM. The expectation is that the observations already provided will be taken into account along with those in the ONR GDA Step 4 report and in particular account will be taken of the remedial action including IV&V undertaken by

	Westinghouse. The detailed evidence above will be assessed as part of the CIM BSC review. The expectations of the form and a basis of safety case for the CIM are set down 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 design 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; and • 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-09 Revision 0 Step 4 C&I Division 6 Assessment Report, No. GDA-AR-11-006 Revision 0
Technical Queries	TQ-**AP1000**-752, TQ-**AP1000**-787, TQ-**AP1000**-1108 & TQ-**AP1000**-1121
Regulatory Observations	RO-**AP1000**-100

Other Documentation	UKP-PMS-GLR-002

Scope of work:

Westinghouse has provided the version of UKP-PMS-GLR-002, “Component Interface Module Safety Case Basis” to ONR on 19th November 2010. The CIM 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. CIM documentation, used to support the basis of safety case for the CIM.

Deliverables/description of work:

This resolution plan will provide the following deliverables for ONR assessment:

1. Westinghouse shall make available in the UK, all supporting documentation used to support the basis of safety case, including:
    a. CIM-SRNC requirement specifications
        i. WNA-DS-02331-GEN
        ii. WNA-DS-01271-GEN
        iii. WNA-DS-01272-GEN
    b. Design Documentation
        i. CIM Software Requirement Specification – 6105-20004
        ii. SRNC Software Requirement Specification – 6105-10004
        iii. CIM Software Design Description – 6105-20014
        iv. SRNC Software Design Description – 6105-10014
        v. Hardware Design Documentation - Multiple
    c. Requirements Tracing
        i. CIM RTM – 6105-20010
        ii. SRNC RTM – 6105-10010
    d. Test Process
        i. Test Plan – 6105-00005
        ii. Test Documentation - Multiple
    e. Configuration Control
        i. CIM-SRNC CM Plan – 6105-00002
        ii. CIM-SRNC Status Accounting – 6105-00053
        iii. CIM-SRNC CM Report – 6105-00070
    f. Independent Verification and Validation
        i. IVV Plan – 6105-00013
        ii. IVV Phase Summary Report – 6105-00092

2. A revision to the CIM BSC

    The revision will include:
    a. Update Section 5.4 with the results of the execution of the action plan. This includes the following areas:
        i. Design Documentation
        ii. Requirements Tracing
        iii. Test Process
        iv. Configuration Control

v. Independent Verification and Validation

b. The relevant TSC TOs identified in of the Step 4 C&I Division 6 Assessment Report, No. GDA-AR-11-006 Revision 0 will be evaluated early in the resolution plan execution cycle for inclusion in the revision of the CIM BSC as appropriate.
c. Clause by clause compliance to IEC 62566 and IEC 60987
d. Westinghouse will elaborate on additional compensating measures for any deviations identified in the self assessments.

As identified in T/AST/051, Issue 001, “Guidance on the Purpose, Scope and Content of Nuclear Safety Cases,” the purpose of a BSC document is to establish and demonstrate in written form that the plant, process, activity, modification, etc. being proposed:

- are soundly assessed and meet required safety principles;
- conform to good nuclear engineering practice and to appropriate criteria, standards and codes of practice;
- are adequately safe during both normal operation and fault conditions;
- are, and will remain, fit for purpose;
- give rise to a level of nuclear risk to both public and workers which is ALARP; and
- have a defined and acceptable operating envelope, with defined limits and conditions, and the means to keep within it.

The basis of safety case (BSC) document will be revised take into account the observations and information in the TQs referenced above.

As the CIM design completes (e.g., equipment qualification, reliability analyses, factory integration testing, and site acceptance testing) the BSC will be updated to include the items.

Schedule/ programme milestones:

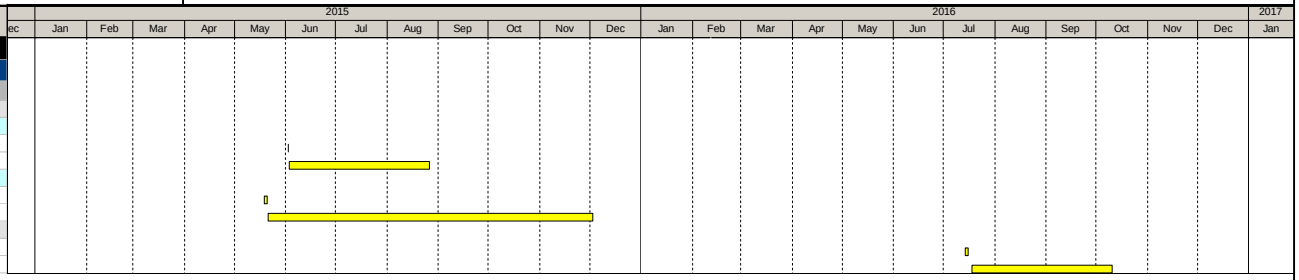
Periodic status meetings will be conducted between Westinghouse and ONR personnel to ensure that C&I GDA open issues are being resolved in timely and quality manner.

A self-assessment of process and procedures will be completed by Westinghouse to ensure that the CIM is adequately produced as safety Class 1 equipment. The documentation will be updated as needed, and the updated documents will be made available for ONR audit.

The CIM BSC will be revised, internally reviewed and transmitted to the ONR. 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.
If needed based on ONR comments, a subsequent revision to the CIM BSC will be developed and issued.

Please see the following page for the schedule.

#	Activity Name
1	**UK Generic Design Assessment (GDA) Resolution Plans (51)**
2	**CONTROL & INSTRUMENTATION**
3	**CI.09 CIM Adequacy of Safety Case-Resolution Plan**
4	**CI.09 IEC Standards Compliance Effort**
5	**CI.09 IEC 62566**
6	IEC 62566 Rev 0-Submit to ONR
7	IEC 62566 Rev 0-ONR Review of Submittal
8	**CI.09 IEC 60987**
9	IEC 60987-Submit to ONR
10	IEC 60987-ONR Review of Submittal
11	**CI.09 CIM Basis of Safety Case (BSC) Revision 1**
12	CIM Basis of Safety Case (BSC) Rev.1-Submit to ONR
13	CIM Basis of Safety Case (BSC) Rev.1-ONR Review of Submittal



Methodology:

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, Westinghouse 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.

<u>Policy and Procedures Self Assessment</u>

Westinghouse is undertaking a self assessment of CIM-related processes and procedures to ensure the CIM’s supplier can adequately produce safety-related equipment.

Review teams comprised of both Westinghouse and Supplier technical and project management personnel will perform formal gap analysis to identify deficiencies with existing processes and procedures as related to appropriate SAPs and other regulatory guidance provided by the ONR. Compensating measure to correct deficiencies will be developed, verified and implemented. The resulting documentation will be made available for ONR audit.

CIM BSC Development

The CIM BSC shall be revised to:

1. The BSC will provide further substantiation to the claims, arguments and evidence related to IEC standard compliance and key SAPs identified in the initial issuance of the BSC.

2. The relevant TSC TOs identified in of the Step 4 C&I Division 6 Assessment Report, No. GDA-AR-11-006 Revision 0 will be evaluated early in the resolution plan execution cycle for inclusion in the revision of the CIM BSC as appropriate.

3. Update of BSC Section 5.4 with the results of the execution of the self assessment of policies and procedures. This includes the following areas:
   - Design Documentation
   - Requirements Tracing
   - Test Process
   - Configuration Control
   - Independent Verification and Validation

   Westinghouse will elaborate on additional compensating measures for any deviations identified in the self assessments.

4. The BSC will identify any further available supporting analysis such as hazards analysis; FMEAs, reliability analysis, MTBF values, environmental qualification, etc. and link them to claims made and for the demonstration of fitness for purpose of the system.

5. The BSC will provide further evidence on how the CIM meets the UK position with respect to ALARP.

6. The BSC will describe the mathematically-based formal method of static analysis for verifying CIM determinism as an Independent Confidence Building Measure.

7. An impact assessment on GDA changes to the plant fault studies and PSA on the Class 1 systems that use the CIM will be conducted to determine if there is an impact on the CIM BSC.

Justification of adequacy:
The above formal methodology based on the Westinghouse QMS will address issues that ONR has raised in regards to the adequacy of the CIM BSC. This will include appropriate technical and licensing reviews to ensure that the final version of the BSC will demonstrate compliance to the appropriate SAP's and guidance provided by ONR. Westinghouse considers the aforementioned areas where the CIM BSC will be revised, in accordance to T/AST/051and per this Resolution Plan, will demonstrate that the CIM BSC will be sufficiently robust to substantiate the claim that the **AP1000** CIM 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-002, "United Kingdom **AP1000** Component Interface Module Safety Case Basis" • UKP-GW-GL-793, Chapter 19, "**AP1000** Pre-Construction Safety Report" Westinghouse notes that other Chapters of the PCSR may require revision in addition to Chapter 19 as a result of the final version of the CIM BSC. If required, changes will be provided to other Chapters will be provided to the PCSR author. However as the BSC is a separate stand alone document which is referenced from the PCSR, Westinghouse does not envisage a significant impact on PCSR revisions.