Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-C&I-01 & GI-AP1000-C&I-02
DAS – Adequacy of Safety Case & Adequacy of Architecture

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

GDA ISSUE:	Westinghouse has proposed design changes to the DAS secondary protection system, as a result the DAS design is not complete and this has lead to the absence of safety case argumentation and evidence to substantiate the DAS design. Westinghouse has provided an initial basis of safety case (BSC) for the DAS and ONR's assessment has shown that this broadly aligns with our expectations. However, Westinghouse needs to respond to ONR's observations on the BSC, progress the detailed design, complete the safety case, provide the evidence identified in the safety case and introduce the design change proposal. For further guidance, see T15.TO2.14, T15.TO2.16, T15.TO2.18 to 26 and T15.TO2.54 in Annex 5, and also T16.TO1.03 and its associated TO2s, T16.TO1.04, T16.TO2.17, and T16.TO2.43 in Annex 6 of ONR C&I Assessment Report No. ONR-GDA-AR-11-006, Revision 0.
ACTION: GI-AP1000-C&I-01.A1	Westinghouse to formally introduce the change to the architecture and technology of the DAS via the design change process (DCP). The revised DAS has to be formally introduced and the safety documentation amended accordingly. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-C&I-01.A2	Westinghouse to provide the basis of safety case for the completed design of the DAS. The form and content of the BSC for the completed design is indicated below, the interim BSCs should also record in principle the methodology by which the missing design information and substantiation will be included to demonstrate the adequacy of the DAS and to justify that sufficient information will be available in a timely fashion for assessment by ONR. 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.

GDA ISSUE:	ONR sought clarity regarding the adequacy of the DAS (the secondary protection system) 2 out of 2 operating philosophy. In response Westinghouse has proposed significant changes to the architecture of the DAS (i.e. from a 2 channel 2oo2 voted system to a system whose logic is a combination of 2oo3 or 1oo2 twice voting). The expectation is that this modified architecture will allow the DAS to remain in service during power operation but this needs to be substantiated as the detailed design and reliability analyses are completed. The substantiation should also demonstrate that both the automatic and manual DAS can achieve their declared reliability targets. For further guidance, see T16.TO1.04 and T16.TO2.17 in Annex 6 of C&I Assessment Report)GDA-AR-11-006, Revision 0.

ACTION: GI-AP1000-C&I-02.A1	Provide a substantiation that the automatic DAS remains in service during reactor power operation including meeting the requirements for maintenance and proof testing. The DAS forms part of the reactor protection system and Westinghouse had identified that the DAS would be a two channel system requiring a 2oo2 vote and positive actuation to trip. The DAS automatic trip function would not be available during reactor operation when test and maintenance activities are undertaken as the channel is in bypass and the 2oo2 logic retained. The DAS Engineered Safeguard Features (ESF) manual controls would also be powered down during reactor power operation. ONR identified that this architecture and mode of system operation appeared contrary to a number of the SAPs associated with protection systems, e.g. ESS 21 & EDR 1, and ESS 23 for maintenance, and for systems providing the ESF, e.g. ESS 8 & 9 and ERL 3. Westinghouse has proposed, a change to the DAS architecture changing the required automatic logic from 2oo2 logic to a combination of 2003 and 1oo2 twice logic. ONR has reviewed the change proposal noting that it in principle addresses the concerns raised and has provided comments to Westinghouse to this effect. Note: The revised DAS has to be formally introduced, its design completed, see GI-**AP1000**-CI-01.A1 & A2, to allow the necessary analysis to be completed to substantiate that the DAS is available at all times during power operation. The substantiation should be included in the basis of safety case for the DAS. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-C&I-02.A2	Provide a substantiation that the automatic and the manual DAS meets their reliability targets. The revised DAS has to be formally introduced, its design completed, see GI-**AP1000**-CI-01.A1 & A2, to allow the necessary analysis to be completed to substantiate that both the automatic and manual parts of the DAS meet their reliability targets. Note: the substantiation should be included in the basis of safety case for the DAS. With agreement from the Regulator this action may be completed by alternative means.

ACTION: GI-AP1000-C&I-02.A3	Identify and provide a description of the sources of electric power for the DAS and their physical location on the plant. This should include the safety class of the supply, the source of supply including the division providing the supply, supply voltage and capacity, and loads supplied. For battery backed supplies the battery operating time is also required. For the DAS dedicated battery supplies the location of the equipment (batteries and chargers) is required along with their safety class, loads supplied and battery operating time. The primary source of power should be described as part of the response above. Other sources of power required by the DAS to operate should be described, for example for firing the squib valves or hydrogen igniters. The details required are as indicated above. The descriptions should be supported by a substantiation of the adequacy of the supplies including their qualification, capacity and a demonstration that supply performance is consistent with the reliability claims on and the availability / endurance of the DAS. Note: the description and substantiation of the adequacy of the supplies should be included in the basis of safety case for the DAS. 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-01, Revision 0 GI-**AP1000**-C&I-02, Revision 0 Step 4 C&I Division 6 Assessment Report, ONR-GDA-AR-11-006, Revision 0
Technical Queries	TQ-**AP1000**-991, TQ-**AP1000**-1031, TQ-**AP1000**-1032, TQ-**AP1000**-1113 & TQ-**AP1000**-1114
Regulatory Observations	RO-**AP1000**-71 & RO-**AP1000**-81
Other Documentation	UKP-DAS-GLR-001

Scope of work:
Westinghouse will provide by formal transmittal letter(s), APP-GW-GEE-2286, “Changes to Diverse Actuation System (DAS) Voting Logic and Associated Architecture”, APP-GW-GEE-2287, “Changes to Diverse Actuation System (DAS) Platform Implementation”, APP-GW-GEE-3001, “Modifications to Diverse Actuation System (DAS), and APP-GW-GEE-4517, “Corrections to Power Sources for Diverse Actuation System.” These DCPs formally document design changes needed to substantiate the safety case argumentation and evidence for the DAS. The DAS 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. DAS and Westinghouse 7300 Series platform documentation, used to support the basis of safety case for the DAS.

The DAS BSC shall be revised to provide substantiation that the automatic DAS remains in service during reactor power operation including meeting the requirements for maintenance and proof testing and that the automatic and manual DAS meets their reliability targets.

The DAS BSC shall be revised to provide a description of the sources of power for the DAS and their physical location on the plant. Included will be the safety class of the supply, the source of supply and loads supplied. For battery backed supplies the battery operating time will be identified with basis provided.

Westinghouse will develop a preliminary programme plan for the completion of the DAS design.

Deliverables/description of work:

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

1. A revision to the DAS BSC.
2. A preliminary Programme Plan for Production DAS which may be included an annex to the DAS BSC revision. The Programme Plan will describe the activities for the DAS equipment qualification for AP1000.
3. A set of architecture drawings which may be included as an annex to the DAS BSC revision.
4. A set of logic drawings which may be included as an annex to the DAS BSC revision.
5. An FMEA based on the system design in the BSC.
6. A reliability analysis based on the system design in the BSC.
7. 7300 platform equipment qualification documentation.

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.

Specifically the revision to the DAS BSC will ensure related GDA open issues are resolved per ONR expectations.

The preliminary Programme Plan for Production DAS will include the identification of subsequent BSC issuances covering key DAS design stages such as design concept, system definition, detailed design, manufacturing detail and factory acceptance testing. The plan will include key milestones such as 1) placement of order, 2) start of nuclear site construction, and 3) delivery of equipment to site, and should show the tasks and

deliverables at each stage.

The DAS 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, GDA-AR-11-006, Revision 0 will be evaluated early in the resolution plan execution cycle for inclusion in the revision of the DAS BSC as appropriate.

3. The BSC will provide substantiation that the proposed architecture design permits a channel to be taken out of service for test and/or maintenance and the DAS will still meet its intended reliability target. In particular, evidence will be made to show that during a channel outage due to test and/or maintenance, the remaining channels have no unrevealed fail to danger modes. Compliance to SAP EDR.1 (Failure to Safety) will be included in the DAS BSC.

4. The BSC will include a description of the system, breaking it down such that the major elements can be identified (such as input/output and logic cards). Included hall be the demonstration of adequacy for each of these elements (including identification of revisions) as well as the DAS as a whole. The BSC will identify production excellence arguments and identify the independent confidence building measures.

5. The BSC will include a description of the project QA arrangements, e.g. ISO 9001, this should include a clear description of the interface to the DAS supplier (and any other suppliers). The BSC will also include an outline of the DAS supplier QA arrangements.

6. The BSC will identify the pedigree and justification for use of any COTS identified to be used in the DAS design. Included will be a discussion on lifecycle management (e.g., configuration management, operating experience, change implementation/capture).

   In particular, the BSC will provide substantiation as to why the 7300 boards are fit for purpose via production excellence. Westinghouse will provide evidence that shows part numbers and associated revisions for candidate UK **AP1000** DAS equipment reflects operational hours data and defect history.

   The BSC will describe the qualification that has been performed to date on the 7300 platform. The BSC will also reference the **AP1000** requirements for DAS equipment qualification and justify their adequacy. The BSC will identify the gaps in equipment qualification for AP1000, the required additional activities to close those gaps, and the justification that these activities will adequately address these gaps.

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

In particular, the BSC will provide further justification to the reliability analysis and MTBF values previously declared in the initial issuance of the BSC. Both calculated values and usage data will be used to substantiate the MTBF values.

8. The BSC will identify the design process by which the individual components will be brought together and integrated as a system.

9. The BSC will identify how the design and implementation of the DAS complies with relevant Westinghouse safety principles and standards if the DAS system makes use of complex electronic devices, e.g. FPGAs (but not microprocessors).

10. The BSC will substantiate that the automatic DAS remains in service during reactor power operation including meeting the requirements for maintenance and proof testing.

11. The BSC will substantiate that the automatic and manual DAS meets their reliability targets.

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

13. The BSC will describe and identify the basis for remote DAS controls and associated displays. This includes a description and basis for manual DAS-based squib valve controls.

14. The BSC will provide a clear and coherent description of the external and internal DAS power supply architecture along with the substantiation of the safety claims made on them.

15. The BSC will include a preliminary programme plan for the completion of the DAS design. The plan will include the identification of subsequent BSC issuances covering key DAS design stages along with key design and site milestones.

Programme Plan for Production DAS

The completion of DAS design is beyond the current GDA exercise and the design of the DAS will not be progressed until an order has been placed. As such, Westinghouse will develop and provide in the BSC, as an annex, a preliminary programme plan for the production of the DAS, so that the production of the BSC for the completed design can be made visible.

Schedule/ programme milestones:

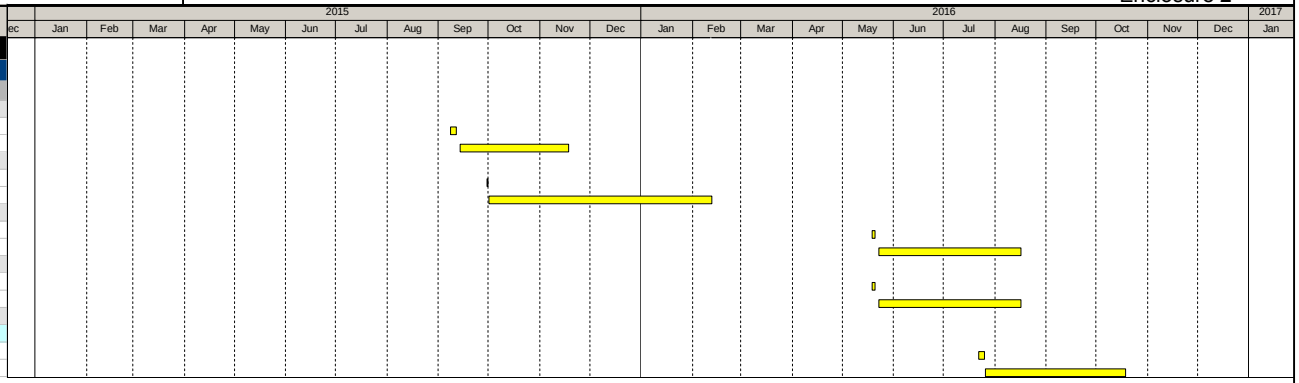
Periodic status meetings will be conducted between Westinghouse and ONR personnel to ensure that C&I GDA open issues are being resolved in timely and quality manner.

Schedule Overview

The following schedule identifies major work efforts and associated milestones for GI-

AP1000-C&I-01 and GI-**AP1000**-C&I-02. DAS-related DCPs will be formally transmitted to the ONR. The DAS BSC will be revised, internally reviewed and transmitted to the ONR. Included in this effort will be the development of preliminary DAS Programme Plan. If needed based on ONR comments, a subsequent revision to the DAS BSC will developed and issued.

#	Activity Name
1	**UK Generic Design Assessment (GDA) Resolution Plans (51)**
2	**CONTROL & INSTRUMENTATION**
3	**CI.01&02 DAS Safety Principles/DAS Reliability - Resolution Plan**
4	**CI.01&02 Design Process Document**
5	DAS Design Process Document-Submit to ONR
6	DAS Design Process Document-ONR Review of Submittal
7	**CI.01&02 Qualification Assessment**
8	DAS Qualification Assessment-Submit to ONR
9	DAS Qualification Assessment-ONR Review of Submittal
10	**CI.01&02 FMEA**
11	DAS FMEA Documentation-Submit to ONR
12	DAS FMEA documentation-ONR Review of Submittal
13	**CI.01&02 Reliability Analysis Report (RAR)**
14	DAS Reliability Analysis Report-Submit to ONR
15	DAS Reliability Analysis Report- ONR Review of Submittal
16	**CI.01&02 DAS BSC Revision 1**
17	**CI.01&02 Generation of DAS BSC Revision 1**
18	DAS BSC Rev.1-Submit to ONR
19	DAS 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 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.

<u>DAS Design Contract</u>

As normal Westinghouse practice, the identification of the key competent staff, organisational structure and, policies and procedures to be used for a UK-based C&I DAS design will be developed and issued in the form of production Programme Plan when a design contract is in place. As previously identified, a preliminary Programme Plan will be developed as an Annex to the DAS BSC. This preliminary document will be used as the basis for the production Programme Plan.

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

Impact assessment:
Other assessment areas that can be impacted include ME, EE, and IH. The safety submission document impacted by the implementation of the resolution plan: • UKP-DAS-GLR-001, "United Kingdom **AP1000** Basis for the Safety Case of the 7300 Based Diverse Actuation System." • UKP-GW-GL-793, Chapters 18 and 19, "**AP1000** Pre-Construction Safety Report." The diversity analysis developed through the resolution of GDA Issue GI-AP1000-CI-03 will need to be addressed by the DAS BSC. In addition, the resolution of GDA Issue GI-AP1000-ME-01 on the SQUIB Valve may impact the resolution of this GDA Issue. 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 DAS 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.