Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-C&I-06 & GI-AP1000-C&I-07
Ovation based DCIS justification for use

MAIN ASSESSMENT AREA	RELATED ASSESSMENT AREA(S)	RESOLUTION PLAN REVISION	GDA ISSUE REVISION
C&I	PSA, FS,FD	5	0

GDA ISSUE:	ONR is seeking an adequate safety case for the Ovation platform that supports the Class 2 closed loop controls and the Class 3 manual controls and displays of **AP1000®**. Westinghouse submitted information on the platform but progress on its assessment was delayed due to priority being given to topics relating to the protection systems including the PMS/CIM safety case, CIM/DAS diversity and PMS blocker. A basis of safety case for the Ovation platform and access to it supporting evidence is required. For further guidance, see T15.TO1.01 in Annex 5 of ONR C&I Assessment Report ONR-GDA-AR-11-006, Revision 0.
ACTION: GI-AP1000-C&I-06.A1	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the Ovation platform. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-C&I-06.A2	Westinghouse to provide a basis of safety case (BSC) that includes a justification of the suitability of the Ovation platform for Class 2 and 3 systems. 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. 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:	The **AP1000** automatic controls and its manual controls and displays are in the DCIS (PLS/DDS). The systems have to be justified as Class 2 (PLS) and Class 3 (DDS) respectively as part of the plant safety case; this requires a new justification as the systems are given a non safety classification in the US. The justification is expected to be in the form of a basis of safety case supported by documented evidence substantiating the claims for the systems and their development. For further guidance, see T15.TO2.36 in Annex 5 and T16.TO1.05 and its associated TO2s, and T16.TO2.19 to 27 in Annex 6 of ONR C&I Assessment Report GDA-AR-11-006, Rev. 0.
ACTION: GI-AP1000-C&I-07.A1	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the PLS and DDS applications. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-C&I-07.A2	Westinghouse to provide a basis of safety case that includes a justification of the suitability of the PLS application at Class 2 (control) and the DDS application at Class 3 (manual control and display). The content of a BSC is outlined 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-06, Revision 0 GI-**AP1000**-C&I-07, Revision 0 Step 4 C&I Division 6 Assessment Report, ONR-GDA-AR-11-006 Revision 0
Technical Queries	TQ-**AP1000**-1117 & TQ-**AP1000**-1222
Regulatory Observations	RO-**AP1000**-78 & RO-**AP1000**-80
Other Documentation	UKP-GW-GLR-021

Scope of work:
Westinghouse has provided the draft version of UKP-GW-GLR-021, “Basis of safety case for Ovation based Distributed Control and Information System” to ONR on 28 February 2011. The intent of this BSC is to respond to Actions GI-**AP1000**-C&I-06.A2 and 07.A2. The draft DCIS BSC shall be revised to address observations identified in the GDA final report. Based on gaps identified in the DCIS BSC, the Westinghouse design processes shall be

revised to provide appropriate safety measures for class 2 and class 3 applications. Where necessary, the process changes will be instituted through modification to the QMS level 3 procedures or modification/creation of work instructions.

The documentation package that justifies qualification of the Ovation platform for class 2 and class 3 applications shall be prepared.

The DCIS BSC shall reflect changes made in the design process and the qualification evidence produced.

Westinghouse will facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the PLS and DDS applications.

Westinghouse will work with Emerson to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the Ovation platform.

Deliverables/description of work:

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

1. A DCIS Basis of Safety Case with a programme plan for the production of PLS and DDS included as an annex*
2. A clause by clause compliance matrix for the tier 1 IEC standards (as an annex to the BSC)
3. A revised DCIS design process that is consistent with the Safety Assessment Principles as identified in the BSC
4. Documentation of the Ovation platform qualification of suitability for application to class 2 and class 3
5. The BSC to incorporate the changes to the design process and qualification documentation
6. Access to supporting evidentiary documentation, both Westinghouse and Emerson, in the UK for ONR review.

* The PLS and DDS designs are completed for China and will be completed for Vogtle and Summer during GDA. Westinghouse can provide those documents applicable to the UK **AP1000** Plant in order to demonstrate the production of the PLS and DDS.

Westinghouse will develop and provide in the BSC, as an annex, a programme plan for the production of the PLS/DDS for the UK, so that the production of the BSC for the completed design can be made visible. The programme plan for the production of PLS and DDS will include the identification of PLS/DDS documentation issuances covering key PLS/DDS design stages such as system definition, detailed design, manufacturing detail and factory acceptance testing.

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.

Westinghouse has provided the draft version of UKP-GW-GLR-021, “Basis of safety case for Ovation based Distributed Control and Information System” as an initial response to the identified actions. This draft BSC will be revised to address the related GDA open issues per ONR expectations. Additionally, the revision will be guided by the relevant TSC TOs identified in the Step 4 Division 6 Assessment Report, GDA-AR-11-006, Revision 0.

The revised DCIS BSC for PLS / DDS and the Ovation Platform will include, as an annex or reference to a document, a clause by clause assessment of compliance to the relevant tier 1 IEC standards, namely:
- IEC 61513 – system principles
- IEC 61226 - classification
- IEC 62138 – software for category B & C functions
- IEC 60987 – hardware for important to safety computer systems

The compliance statements included in this annex or report will be referenced in the BSC proper as appropriate to support the Claims, Arguments and Evidence reasoning presented there. Additionally, IEC 61508 will be evaluated for guidance on hardware aspects for class 3 applications since this class is excluded from the scope of IEC 60987.

The revised DCIS BSC will identify and justify all systems connected directly or indirectly to the DCIS (e.g. BEACON).

The **AP1000** DCIS is based on the commercially available Ovation platform, a product of Emerson. This platform has been assessed to be suitable for application to important to safety functions, however, the documentation of that qualification is lacking. Based on industry standards, the requirements to support this justification will be established and supporting evidentiary documentation will be collected into an organised argumentation of the suitability for purpose of the platform and documented in the BSC.
PLS/DDS applications are designed and implemented at Westinghouse, with support from Emerson, following a documented design process that is consistent with the QMS procedures. As it stands, this process does not fully address the Safety Assessment Principles. In particular, it does not draw a distinction between class 2 and class 3 important to safety applications. The design process will be revised to address these gaps. Process documents will be referenced to show compliance to the applicable Safety Assessment Principles and international standards. This will include documents defining subordinate processes such as configuration management, requirements management, and verification and validation. Where necessary process documents will be revised to institute the revised design process.

Westinghouse will work with Emerson to facilitate ONR access in the UK to the detailed evidence used to support the BSC for the Ovation platform as well as for the **AP1000**

specific class 2 and class 3 applications. However, it must be recognised that much of the Ovation platform information is Emerson proprietary information. As such, Westinghouse and other external parties will have limited access to Emerson documents.

Schedule/ programme milestones:

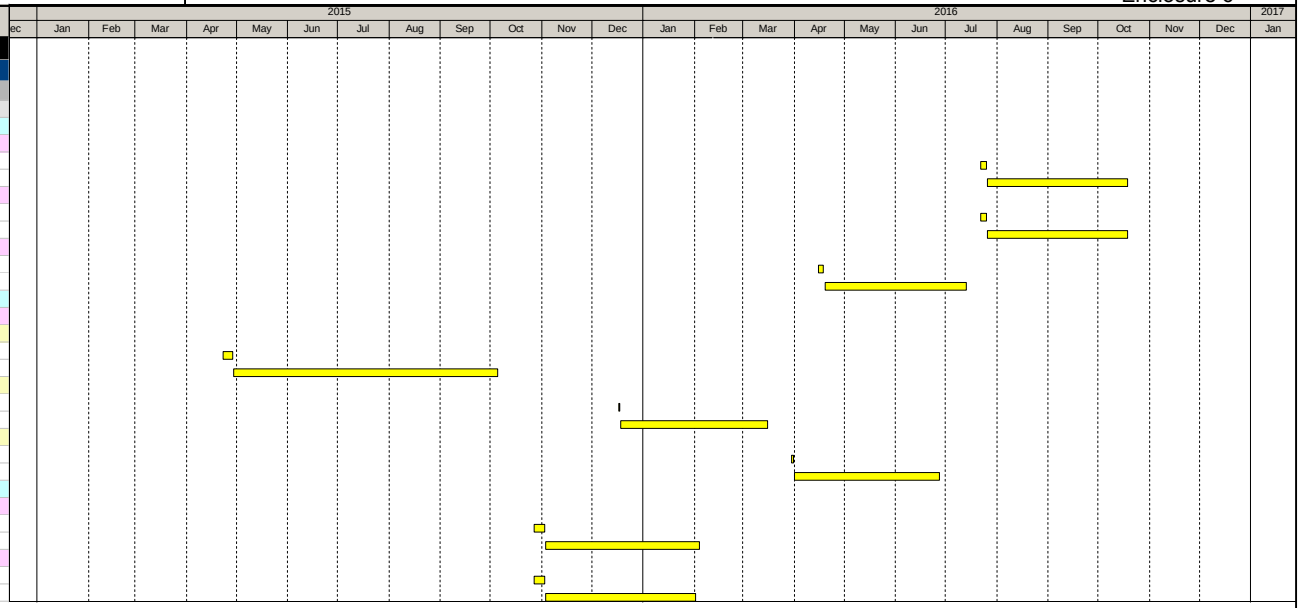
Periodic status meetings will be conducted between Westinghouse and ONR personnel to ensure that C&I GDA open issues are being resolved in timely and quality manner.

Schedule Overview

The following schedule identifies major work efforts and associated milestones for GI-**AP1000**-C&I-06 and GI-**AP1000**-C&I-07:

- The DCIS BSC will be revised, internally reviewed and transmitted to the ONR including a programme plan.
- This revision will address the TSC TOs identified in the Step 4 report.
- Once the design process gaps have been identified in the BSC, the design process documents will be revised to align with the SAP.
- Following the revision of the design process, the BSC will be revised to reflect the changes.
- Evidentiary documents identified in the BSC which support claims made against the SAP will be made available for ONR review in the UK.

#	Activity Name
1	UK Generic Design Assessment (GDA) Resolution Plans (51)
2	CONTROL & INSTRUMENTATION
3	CI.06&07 Ovation Suit-CL 2&3/PLS Suit @ CL2 DDS @ CL3-Resolution Plan
4	CI.06&07 ONR Deliverables/Supporting Documents
5	CI.06&07 Development
6	PLS BSC Rev 0
7	PLS BSC Rev.0-Submit to ONR
8	PLS BSC Rev.0-ONR Review of Submittal
9	DDS BSC Rev 0
10	DDS BSC Rev 0-Submit to ONR
11	DDS BSC Rev 0-ONR Review of Submittal
12	PLS IEC-62138 Argumentation Tables
13	PLS IEC 62138 - Submit to ONR
14	PLS IEC 62138- O_NR Review of Submittal
15	CI.06&07 DCIS Common
16	CI.06&07 Platform
17	CI.06&07 DCIS Commercial Dedication Plan (WNA-PV-xxxxx-GEN)
18	DCIS Commercial Dedication Plan (WNA-PV-xxxxx-GEN)-Submit to ONR
19	DCIS Commercial Dedication Plan (WNA-PV-xxxxx-GEN)-ONR Review of Submittal
20	CI.06&07 DCIS Commercial Dedication Report (WNA-VR-xxxxx-GEN)
21	DCIS Commercial Dedication Report (WNA-VR-xxxxx-GEN)-Submit to ONR
22	DCIS Commercial Dedication Report (WNA-VR-xxxxx-GEN)-ONR Review of Submittal
23	CI.06&07 DCIS Commercial Dedication Instruction (WNA-CD-xxxxx-GEN)
24	DCIS Commercial Dedication Instruction (WNA-CD-xxxxx-GEN)-Submit to ONR
25	DCIS Commercial Dedication Instruction (WNA-CD-xxxxx-GEN)-ONR Review of Submittal
26	CI.06&07 PLS/DDS Application Standards Compliance Matrices
27	CI.06&07 IEC 62138 (UKP-GW-GL-XXX)
28	DDS IEC 62138 (UKP-GW-GL-XXX)-Submit to ONR
29	DDS IEC 62138 (UKP-GW-GL-XXX)-ONR Review of Submittal
30	CI.06&07 IEC 60987 (UKP-GW-GL-XXX)
31	IEC 60987 (UKP-GW-GL-XXX)-Submit to ONR
32	IEC 60987 (UKP-GW-GL-XXX)-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."

The initial draft of UKP-GW-GLR-021, "Basis of safety case for Ovation based Distributed Control and Information System," was sent to ONR in February 2011. The first revision to this draft will include the following:

- Addressing of TSC TOs identified in the Step 4 C&I Division 6 Assessment Report
- Clause by clause compliance assessment against tier 1 IEC standards
- Strengthening of CAE resulting from cooperative review of the draft BSC by Emerson
- Progress made on the accumulation of evidence as the normal course of design completion for **AP1000** DCIS
- The BSC shall describe the allocation of control functions to controllers for dependability and defense-in-depth. The BSC will describe how the stability of the close loop control functions are established, verified and validated.
- A preliminary programme plan* for the production of the UK PLS/DDS, so that the production of the BSC for the completed design can be made visible. The programme plan for the production of PLS and DDS will include the identification of PLS/DDS documentation issuances covering key PLS/DDS design stages such

as system definition, detailed design, manufacturing detail and factory acceptance testing.

* The PLS and DDS designs are completed for China and will be completed for Vogtle and Summer during GDA. Westinghouse can provide those documents applicable to the UK **AP1000** plant to demonstrate the production of the PLS and DDS.

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.

Completion of the BSC may lead to the identification of gaps in the processes as compared to industry standards and the SAP. This gap identification will largely be through self assessment, but will also include feedback from ONR. The process and the results of the gap identification and closure activities from the IEC and SAP assessments will be described in those assessments. The relevant design process documents will be referenced identifying any gaps. Specific process documents will be referenced including requirements management, configuration management, verification and validation, and so forth. Where necessary Level III QMS procedures or other work instructions that implement these processes will be updated to reflect the changes needed to close the gaps. The manner in which these updated procedures and work instructions will be invoked for use for the UK AP1000 plant will be described in the BSC. While Westinghouse does not have flexibility to alter the processes applied at Emerson, the means available to request design changes (or if necessary process changes) to meet the needs of class 2 and class 3 applications will be described.

In parallel with the effort to update the Westinghouse processes, a formal documentation of the platform qualification will be undertaken. This documentation will include:

- Determination of the qualification requirements, based on industry standards, appropriate to class 2 and 3 applications
- Assessment of the Ovation platform design and the Emerson lifecycle processes against those requirements
- COTS evaluation of the base software (third party) used in the DCIS workstations and controllers
- Validation of the algorithm libraries used to create plant specific applications
- Software configuration/"lock down" procedures to assure that the installed software is consistent with that evaluated
- Review of existing environmental qualifications (including temperature, humidity, seismic, and EMC) for compliance to identified requirements

Once the processes have been updated and the Ovation platform qualification documented, the BSC will be revised to reflect these changes. Other progress on completing the body of evidence will be included as will resolution of any further

feedback from ONR. An additional focus will be placed in this revision on the validation of the suitability of class 2 equipment in the role of backup to the category A safety functions. This validation will examine claims made by the plant fault studies and PSA on the class 2 systems to ascertain compliance in the system design.

Westinghouse will work with Emerson to facilitate ONR access in the UK to the detailed evidence used to support the BSC for the Ovation platform as well as for the **AP1000** specific class 2 and class 3 applications. However, it must be recognised that much of the Ovation platform information is Emerson proprietary information. As such, Westinghouse and other external parties will have limited access to Emerson documents.

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

Impact assessment:

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

- UKP-GW-GLR-021, "United Kingdom **AP1000** Basis of Safety Case for the Ovation Based Distributed Control & Information System."
- UKP-GW-GL-793, Chapter 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 DCIS BSC. In addition, the GI-**AP1000**-FD-03 GDA Issue on the use of BEACON resolution may impact the work on 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 DCIS 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.