

Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-C&I-04
PMS Spurious Operation

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

GDA ISSUE:	<p>The PMS has the capability to actuate any of the Engineered Safety Features (ESF) on the AP1000® plant. This includes the potential to spuriously actuate the Automatic Depressurisation System (ADS) valves or the containment recirculation valves. The spurious operation of these functions has the potential to initiate safety significant transients such as a large LOCA or drainage of the in-containment refuelling water storage tank (IRWST). Westinghouse needs to provide a design basis safety case covering such spurious actuations.</p> <p>Westinghouse has proposed implementing an interlock/blocker to reduce the ADS spurious initiating frequency. Westinghouse needs to formally introduce the design change, complete the design and provide a substantiation of the claims made on the blocker device. For further guidance, see T17.TO1.01 in Annex 7 of ONR C&I Assessment Report GDA-AR-11-006, Revision 0.</p>
ACTION: GI-AP1000-C&I-04.A1	<p>Westinghouse to provide a design basis safety case covering spurious PMS actuation of the ADS valves. The safety case will need to demonstrate that the ADS interlock/blocker device provides adequate protection against such faults or provide additional protection or justification as to why the position is acceptable.</p> <p>For the US design the PMS reliability claim is such that these events are outside the plant design basis; however, the UK design makes a lower claim on the PMS reliability, hence, there is a higher assumed dangerous failure rate bringing these events within the design base. The safety case will need to recognise the effectiveness of the blocker device may well be limited by the reliability of the CIM and so additional protection might be required.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>
ACTION: GI-AP1000-C&I-04.A2	<p>Westinghouse is required to provide a design basis safety case covering spurious operation of the containment recirculation squib valves. Westinghouse needs to demonstrate that adequate protection is provided or propose possible design changes to reduce the initiating frequency of the event and/or provide additional</p>

	<p>protection. The safety case needs to provide a full deterministic and probabilistic assessment to demonstrate that the risk of serious consequences following spurious operation of the recirculation valves is below the design basis sequence cut-off frequency of 10⁻⁷ per year while ensuring the reliability of recirculation valves to perform their important safety function has not been significantly affected.</p> <p>Westinghouse has identified that spurious operation of the PMS can potentially result in the inadvertent opening of the containment recirculation squib valves causing the draining of the IRWST. If these valves are not isolated by the operator such a fault has the potential to:</p> <ul style="list-style-type: none"> • flood the containment sump (possibly resulting in RCP trip and consequential reactor trip), and; • result in the consequential failure of the PRHR heat exchanger and the IRWST safety injection system which are the two Class A1 post-trip cooling systems on the AP1000 plant. <p>It is not clear that this situation meets Westinghouse's own design criteria, which is that for every design basis fault there should be at least one Class A1 safety system to protect against the fault and that operator actions should not be required for at least 72 hours.</p> <p>Should Westinghouse choose to implement the blocker device in a similar manner to that applied on the ADS valves then the safety case needs to recognise that the effectiveness of the blocker device may be limited by the reliability of the CIM and so additional protection may well be required.</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>
<p>ACTION: GI-AP1000-C&I-04.A3</p>	<p>Westinghouse to formally introduce the change to the PMS design to introduce the interlock/blocker on the ADS valves via the design change process (DCP).</p> <p>With agreement from the Regulator this action may be completed by alternative means.</p>
<p>ACTION: GI-AP1000-C&I-04.A4</p>	<p>Westinghouse to complete the design of the interlock/blocker and substantiate it for its intended role. Westinghouse presented, in three notes, a concept design for interlocking/blocking the actuation of the ADS 1 to 4 valves using a signal based on measurement of the level of the core makeup tank fed into the existing PMS CIM Z port.</p> <p>ONR reviewed the design concept and comments were provided to Westinghouse. However, the design and design substantiation need to be completed. The design substantiation should include an evaluation of the ADS 1 to 4 valve spurious operation rates (accounting for sensor</p>

	failure and PMS test and maintenance activities). 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-04, Revision 5, DRAFT Step 4 C&I Division 6 Assessment Report GDA-AR-11-006, Revision 0.
Technical Queries	TQ274 &1125
Regulatory Observations	RO82
Other Documentation	IEC61513, IEC62340 & IEC 60987.

Scope of work:
<p>GI-AP1000-C&I-04.A1: Westinghouse shall issue a BSC to address observations identified by the GDA final report and facilitate HSE/ONR access to the UK to the detailed evidence used to support the basis of safety for the PMS Spurious Operation blocking device and its ability to provide adequate protection against such faults or provide additional protection or justification as to why the position is acceptable.</p> <p>GI-AP1000-C&I-04.A2: Westinghouse shall issue a BSC to address observations identified by the GDA final report and facilitate HSE/ONR access to the UK to the detailed evidence used to support the design basis safety case covering spurious operation of the containment recirculation squib valves by the PMS.</p> <p>GI-AP1000-C&I-04.A3: Westinghouse shall submit and make available in the UK, all referenced documentation used to support Design Change Package (DCP) APP-GW-GEE-2411 (ADS Diverse Actuation Interlock). The revision to the PMS design has been formally introduced via the DCP Process. Two other DCPs have been released for incorporation into the PMS Spurious Operation blocker design and will be made available in the UK. The first DCP, APP-GW-GEE-4291, adds the blocking device to the IRWST injection squib valves. The second DCP, APP-GW-GEE-4823, changes the logic by which the ADS and IRWST injection valves are blocked.</p> <p>GI-AP1000-C&I-04.A4: Westinghouse shall develop, test and qualify a device in accordance with the Design Change identified within APP-GW-GEE-2411 (ADS Diverse Actuation Interlock). The design will be considered complete at the point where the requirements, specifications, detailed designs have been completed; prototype equipment has been produced and subject to performance and qualification testing. The verification and validation exercises will also have been completed for the design, implementation and test phases.</p>

Deliverables/Description of work:
The approach that the following resolution plan follows is to provide a diverse PMS blocking device that is reliable enough such that its failure together with a spurious PMS signal is less than 10^{-7} /year. This resolution plan will provide the following deliverables

for ONR assessment:

1. A reliability assessment of the PMS Spurious Operation blocker and its interface with the PMS will be provided. The impact on the reliability of ADS actuation when desired will also be shown to be acceptable. This assessment will be performed for the current blocker design. In addition, an alternate design will be developed that that utilises an interface device that is simpler than the current CIM interface. The current blocker design will be compared to the alternate blocker design to assess their benefits / disadvantages. The blocker design to use going forward will be selected based on this comparison; if the selected design is different than the current design the differences will be incorporated into the **AP1000** plant using the Westinghouse DCP process.
2. An assessment of the plant response to a spurious containment recirc actuation signal, in particular with respect to whether a reactor trip would be caused will be provided. If indicated as necessary by this assessment, plant changes will be proposed to address this event (for example, applying the diverse block device to the recirc valves). Any changes to the plant design will be process through the **AP1000** DCP process.
3. A PMS Spurious Operation BSC that includes:
 - a. A summarisation of the results of deliverables 1 and 2.
 - b. A preliminary Programme Plan for Production (if an alternate approach is selected) which will be included as an annex to the BSC revision.
 - c. 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.
 - d. Specifically the issuance of the PMS Spurious Operation BSC will ensure related GDA open issues are resolved per ONR expectations.

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-04. PMS Spurious Operation blocker related DCPs will be formally transmitted to the ONR. The PMS Spurious Operation BSC will be issued, internally reviewed and transmitted to the ONR. Included in this effort will be the development of a preliminary PMS Spurious Operation blocker Programme Plan if an alternate approach is chosen. If needed based on ONR comments, a subsequent revision to the PMS Spurious Operation BSC will developed and issued.

#	Activity Name	2016												2017				
		ec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
1	UK Generic Design Assessment (GDA) Resolution Plans (51)																	
2	CONTROL & INSTRUMENTATION																	
3	CI.04 PMS Spurious Operation-Resolution Plan																	
4	CI.04 PMS Spurious Operation BSC Rev.0																	
5	PMS Spurious Actuation BSC Rev 0-Submit to ONR																	
6	PMS Spurious Actuation BSC Rev 0-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.

If an alternate approach is selected, the preliminary Programme Plan for Production of the PMS Spurious Operation blocker will include the identification of subsequent BSC issuances covering key 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 PMS Spurious Operation BSC shall be written 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 the Step 4 C&I Division 6 Assessment Report, GDA-ARR-11-006, Revision 0 will be evaluated early in the resolution plan execution cycle for inclusion in the revision of the PMS Spurious Operation BSC as appropriate.
3. The BSC will include a description of the PMS Spurious Operation blocker, breaking it down such that the major elements can be identified (such as input/output and logic cards). Included shall be the demonstration of adequacy for each of these elements (including identification of revisions) as well as the circuitry as a whole. The BSC will identify production excellence arguments and identify the independent confidence building measures.
4. The BSC will include a description of the project QA arrangements based on the Westinghouse QMS. This will include a clear description of the interface to the circuitry supplier (and any other suppliers). The BSC will also include an outline of the circuitry supplier QA arrangements.
5. The BSC will identify the pedigree and justification for use of any COTS identified to be used in the design. Included will be a discussion on lifecycle management (e.g., configuration management, operating experience, change implementation/capture).

Westinghouse will provide evidence that shows part numbers and associated revisions for candidate UK **AP1000** PMS equipment reflects operational hours data and defect history.

6. 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 declared in the initial issuance of the BSC. Both calculated values and usage data will be used to substantiate the MTBF values. The reliability analysis will include the PMS interface which is the CIM. It is recognised that the effectiveness of the blocking device may be limited by the reliability of the CIM. If necessary to meet the reliability objectives of the PMS Spurious Operation blocker plant design changes would be proposed. Any change will follow the Westinghouse QMS Level II Procedure WEC 3.4.1, "Change Control for the **AP1000** Program".

7. The BSC will identify the design process by which the individual components will be brought together and integrated as a system.
8. The BSC will provide further evidence on how the PMS Spurious Operation blocker meets the UK position with respect to ALARP.
9. The BSC will provide a full deterministic and probabilistic assessment to demonstrate

that the risk of serious consequences as a result of spurious ADS operation due to a failure on the PMS is below the design basis sequence cut-off frequency of 10^{-7} per year while ensuring the reliability of ADS to perform its important safety function has not been significantly affected.

10. The BSC will also evaluate the consequences of a spurious containment recirculation actuation. In particular it will be determined if and when the reactor might trip following such a spurious action with consideration for the impact of water flooding on heat removal from the RV, and possible shorting out of power to the reactor coolant pumps and RCS sensors. This evaluation will be used to determine the need / benefit of applying the PMS Spurious Operation blocker to the containment recirculation valves. The safety case will provide a full deterministic and probabilistic assessment to demonstrate that such an actuation does not have serious consequences or that the risk of serious consequences following spurious operation of the recirculation valves is below the design basis sequence cut-off frequency of 10^{-7} per year while ensuring the reliability of recirculation valves to perform their important safety function has not been significantly affected. If a plant change is deemed necessary the change will follow the Westinghouse QMS Level II Procedure NSNP 3.4.1, "Change Control for the **AP1000** Program".

Programme Plan for Production of the Alternate Design of the PMS Spurious Operation Blocker

Should an alternate configuration be determined to be necessary, the design of the alternate configuration shall be developed to an extent that it can demonstrate fulfilment of the safety requirements and the blocking function. Production of the alternate configuration of the blocker will not be completed within the scope of GDA. As such, Westinghouse will develop and provide in the BSC, as an annex, a preliminary programme plan for the production of the circuitry. This preliminary document will be used as the basis for the production programme plan which will not be produced within the scope of GDA.

PMS Spurious Operation Blocker Design Contract

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 PMS Spurious Operation blocker 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 PMS Spurious Operation BSC if an alternate approach is selected.

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 PMS Spurious Operation 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 PMS Spurious Operation BSC will be issued, in accordance to T/AST/051 and per this Resolution Plan, will demonstrate that the PMS Spurious Operation BSC will be sufficiently robust to substantiate the claim that the PMS Spurious Operation Blocker is fit for purpose as described in the BSC.

Impact assessment:

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

- PMS Spurious Operation BSC
- UKP-GW-GL-793, Chapter 19, “**AP1000** Pre-Construction Safety Report.”
- UKP-PMS-GLR-001, “United Kingdom **AP1000** Protection and Safety Monitoring System Safety Case Basis.”

The resolution of GDA Issue GI-**AP1000**-ME-01 on the SQUIB valve may impact the resolution of this GDA Issue and vice versa.

Note that since the approach is to provide a highly reliable blocking device there will no need to perform fault studies and add them to the EDCCD or to the UK PCSR accident analysis sections.