Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-FS-03
Diversity for Frequent Faults

MAIN ASSESSMENT AREA	RELATED ASSESSMENT AREA(S)	RESOLUTION PLAN REVISION	GDA ISSUE REVISION
Fault Studies	PSA C&I	1	0

GDA ISSUE:	Demonstration of functional diversity for frequent faults.
ACTION: GI-AP1000-FS-03.A1	Implement the revised moderator temperature coefficients assumed in the ATWS analysis reported in UKP-GW-GLR-016 within the **AP1000®** safety analysis checklist document WCAP-9272-P-A. These should be referenced within the PCSR as the limits and conditions as the relevant core parameters identified by the fault studies for ultimate incorporation within the technical specifications for the **AP1000** plant (see also GDA issue GI-**AP1000**-FS-02). Alternatively, Westinghouse may wish to provide a revised analysis with parameters consistent with those presented in Chapter 4 of the DCD. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-FS-03.A2	• Demonstrate protection for the excessive increase in secondary steam flow fault at full power for both the case with successful reactor trip and the case with failure of the reactor to trip due to either mechanical failure of the rods to insert or failure of the reactor protection system. Or • Propose design changes to provide protection against the excessive increase in secondary steam flow faults. In the European DCD and the UKP-GW-GLR-016, the analysis of excessive increase in secondary steam flow with failure to trip is limited to consideration of the condition II event, which limits flow increases to less than 10% at full power. Westinghouse has not presented any analysis for a more challenging excessive increase in secondary steam flow fault at full power. Westinghouse will need to demonstrate adequate diverse protection for such faults for both the case with successful reactor trip and for the case with failure of the reactor trip due to either mechanical failure of the

	rods to insert or failure of the reactor protection system. In particular, in the case of PMS failure, Westinghouse will have to demonstrate that there are adequate trip parameters on the diverse actuation system (DAS). Any design modifications identified as necessary will need to complete the six-stage modification process for inclusion in the PCSR. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-FS-03.A3	• Demonstrate the provision of diverse protection against rod misplacement faults including one or more dropped rods. Or • Propose design changes to protect against the consequences of such a fault. The analysis of these faults presented by Westinghouse assumes that although the protection and monitoring system (PMS) is unavailable the flux monitoring system remains available to the plant control system (PLS) and provides protection against these faults. This fails to demonstrate any diversity within the flux protection system. For this reason, Westinghouse are requested to provide explicit transient analysis using design basis analysis techniques for these faults to demonstrate that the diverse actuation system (DAS) is functionally capable of protecting against this fault. A modification to include the provision of a negative rate flux trip signal on the diverse actuation system (DAS) is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion with the PCSR. Note this action is also closely related to GDA issue GI-**AP1000**-FS-04. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-FS-03.A4	Implement the proposed modification to provide a high hot leg temperature trip on the Diverse Actuation System to protect against the RCCA bank withdrawal fault at full power with failure of the PMS. Westinghouse has identified that a modification is required to provide a reactor trip signal on high hot leg temperature on the Diverse Actuation System. This is to protect against a RCCA bank withdrawal fault at full power with failure of the Protection and Monitoring System (PMS). The design for the proposed modification will need to complete the sixstage modification process for inclusion within the PCSR. With agreement from the Regulator this action may be completed by alternative means.

ACTION: GI-AP1000-FS-03.A5	Demonstrate protection against a complete loss of forced flow fault as a result of perturbations in grid frequency for both the case with successful reactor trip and the case with failure of the reactor trip due either mechanical failure of the rods to insert or failure of the reactor protection system. In the Westinghouse submissions assessed, the analysis of complete loss of flow fault with failure to trip is limited to consideration of initial conditions associated with nominal full power conditions. Westinghouse has not presented any analysis considering the effect of grid perturbations on the initial reactor conditions. It is likely that in such circumstances, the reactor control system will attempt to increase power to compensate for any grid frequency reduction. This will perturb both the initial reactor power and the initial power distribution of the core including the axial offset. Westinghouse will need to demonstrate adequate diverse protection for such faults for both the case with successful reactor trip and for the case with failure of the reactor trip due to either mechanical failure of the rods to insert or failure of the reactor protection system. In particular, in the case of PMS failure, Westinghouse will have to demonstrate that there are adequate trip parameters on the diverse actuation system (DAS). Any design modifications identified as necessary will need to complete the six-stage modification process for inclusion in the PCSR. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-FS-03.A6	• Demonstrate the provision of diverse protection against loss of CVS following a normal reactor trip and xenon decay including demonstration of diversity to operator action. Or • Provide a consequence analysis demonstrating the acceptability of the design against HSE's accident frequency targets. After every reactor trip from full power there is an eventual decay in the level of xenon poisoning within the reactor core. The resultant swing in reactivity needs to be compensated for through increasing the boron concentration in the reactor to ensure an adequate shutdown margin. While the core make-up tanks (CMTs) and the incontainment refuelling water storage tank (IRWST) systems provide two diverse sources of borated water should the operator fail to ensure adequate shutdown margin using the Chemical and Volume control system (CVS), both these systems are

	also dependent upon operator action for actuation. Although timescales are long (many hours), this implies a combined human reliability of 1 x 10^{-7} per demand to meet the design basis target. For this reason, Westinghouse is to provide an ALARP study into the feasibility of automatically actuating the CVS to inject borated water after every reactor trip and for the CMTs to be automatically actuated following failure of the CVS. Alternatively, Westinghouse may wish to provide a consequence analysis of what would happen should the operator fail to ensure adequate shutdown margin. With agreement from the Regulator this action may be completed by alternative means.
ACTION: GI-AP1000-FS-03.A7	Analyse the homogenous boron dilution fault occurring in shutdown conditions with failure of the protection and monitoring system to demonstrate that there is diverse protection against the fault. This fault would be very difficult to detect should there be a failure of the flux instrumentation or the protection and monitoring system (PMS). For this reason, Westinghouse is to provide explicit transient analysis using design basis analysis techniques for this fault to demonstrate that the diverse actuation system (DAS) is functionally capable of maintaining adequate margin to departure from nucleate boiling. A modification to include the provision of a boron dilution block signal and a CMT actuation signal on the DAS (actuated by low doubling time and/or high source-range flux level) is to be considered as a possible ALARP measure. The design of any proposed modification will need to complete the six-stage modification process for inclusion within the PCSR. Westinghouse also needs to identify as a limit and condition for the reactor core design technical specifications the limiting moderator reactivity coefficients assumed in the analysis. With agreement from the Regulator this action may be completed by alternative means.
RELEVANT REFERENCE DOCUMENTATION RELATED TO GDA ISSUE	
Technical Queries	
Regulatory Observations	RO-**AP1000**-47 RO-**AP1000**-51 RO-**AP1000**-91
Other Documentation	

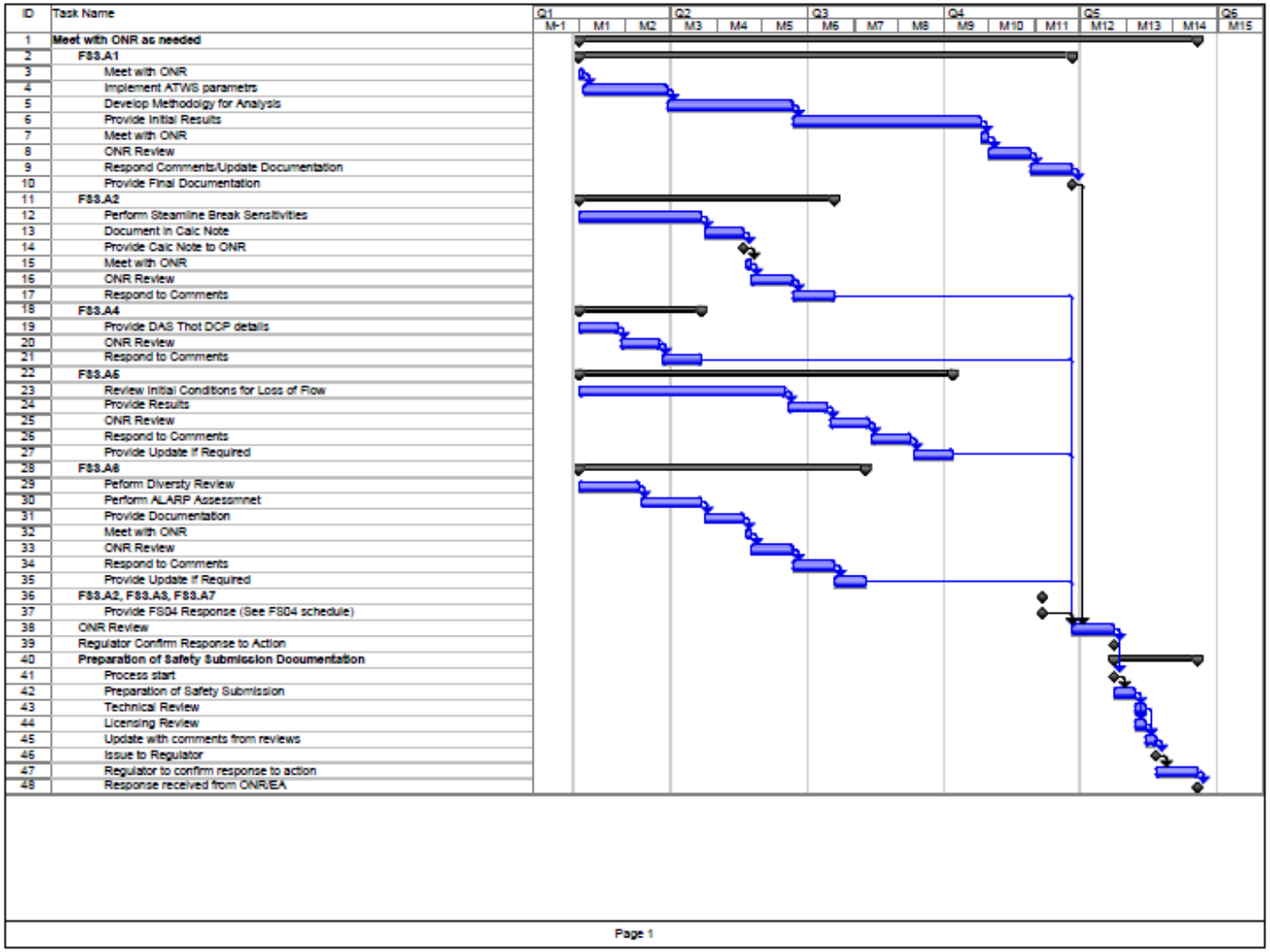
Scope of work:
During the Step 4 GDA review, the ONR requested Westinghouse to provide an integrated assessment of the **AP1000** design to demonstrate its capability to address postulated common mode failures for frequent faults. In UKP-GW-GL-067, Rev 0, Westinghouse has provided an evaluation of the **AP1000** frequent faults demonstrating that diverse protection is provided for frequent faults (i.e. those faults with an expected frequency of occurrence greater than 1E-3/yr). The document includes a list of which faults are frequent. It also includes an evaluation of mitigation of these faults showing what equipment provides the diverse protection. Finally the limiting faults are identified and reference is made to plant analysis that provides evidence that the mitigating features are capable of providing the necessary protection. Additionally, to address the ONR request that the possibility of a cliff edge in the frequency should be considered, this document also addresses events that have a frequency lower than 1E-3/year but for which there may be a question as to whether the frequency is sufficiently lower than 1E-3/year to ignore the event as a frequent fault. As a result of the studies summarised in UKP-GW-GL-067, a revised Fault Schedule (documented in UKP-GW-GLR-003, Revision 1) was developed to document an integrated fault schedule for the **AP1000** plant, including how the diversity requirement is met for all frequent faults. This fault schedule is also included in Revision 0 of the **AP1000** PCSR (UKP-GW-GL-793). Additional discussion on diversity for each applicable fault group is provided also in Chapter 9 of the PCSR, as appropriate. In GI-AP1000-FS-03, the ONR has identified some specific areas where additional information and supporting evidence is requested for Westinghouse to ensure that the claims and arguments provided in UKP-GW-GL-067 are fully supported. In some cases Westinghouse believes it will be sufficient to provide extra information following discussions with ONR. In other cases, the actions in this issue require some additional ALARP investigation and assessment to confirm all aspects of the design against the diversity requirement.

Description of work:	
Westinghouse will provide the following:	
FS-03.A1	Westinghouse will implement the ATWS Moderator Temperature Coefficients in the Safety Analysis Checklist. A methodology that provides an acceptably conservative result will be developed and an initial demonstration will be provided.
FS-03.A2	For the successful reactor trip case a parametric sensitivity study will be presented to secondary break size (or equivalent flow rate) for full power operation to demonstrate that the protection prevents fuel from entering DNB for an appropriate range of break sizes (or flow rates). Demonstrate for frequent faults by drawing on already existing DBA and

	ATWS analyses, and possibly additional sensitivities, Westinghouse will provide additional safety arguments to address the capability of the Plant to mitigate an excessive increase in secondary steam flow fault at full power both with reactor trip and with failure of the reactor to trip. Potential modifications and their ALARP assessment will be evaluated under GDA issue GI-**AP1000**-FS-04 as therein described.
FS-03.A3	This action is to consider rod misalignment faults including dropped rods is already covered in the Resolution Plan for GI-**AP1000**-FS-04 Flux Protection.
FS-03.A4	The DAS High Hot Leg logic was clarified and finalised in Design Change APP-GW-GEE-1481, which is included in the Design Reference Point for the **AP1000** GDA. The DCP has been approved and is now part of the safety case. As part of the resolution plan the DCP will be reviewed with the regulator to confirm that the DAS Thot reactor trip is correctly implemented in the design.
FS-03.A5	Westinghouse will justify that the effects of grid perturbations on the reactor control system and the RCP power supplies have been taken into account in specifying the initial conditions for the analysis including the effect upon power level, axial offset, radial peaking factors, and transient flow rate. The aim will be to demonstrate that the fuel does not enter DNB as a result of this transient. Should this not be the case then potential modifications will be subject to an ALARP assessment. If any 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".
FS-03.A6	Westinghouse will demonstrate the provision of diverse protection against loss of the CVS. Should this not be the case then Westinghouse will perform an ALARP assessment to evaluate why the current design as is remains ALARP without need of any further automatic action.
FS-03.A7	This action is to consider boron dilution faults from shutdown conditions with failure of the flux protection and is now covered in the Resolution Plan for GI-**AP1000**-FS-04 Flux Protection

Schedule/ programme milestones:

Because all Resolution Plans start dates are subject to future contract placements, dates are presently undefined; therefore schedule dates have been anonymised for consistency. Actual dates will be inserted when contracts are placed.



ID	Task Name
1	**Meet with ONR as needed**
2	**FSS.A1**
3	Meet with ONR
4	Implement ATWS parametrs
5	Develop Methodolgy for Analysis
6	Provide Initial Results
7	Meet with ONR
8	ONR Review
9	Respond Comments/Update Documentation
10	Provide Final Documentation
11	**FSS.A2**
12	Perform Steamline Break Sensitivities
13	Document in Calc Note
14	Provide Calc Note to ONR
15	Meet with ONR
16	ONR Review
17	Respond to Comments
18	**FSS.A4**
19	Provide DAS Thot DCP details
20	ONR Review
21	Respond to Comments
22	**FSS.A5**
23	Review Initial Conditions for Loss of Flow
24	Provide Results
25	ONR Review
26	Respond to Comments
27	Provide Update if Required
28	**FSS.A6**
29	Peform Diversity Review
30	Perform ALARP Assessmnet
31	Provide Documentation
32	Meet with ONR
33	ONR Review
34	Respond to Comments
35	Provide Update if Required
36	**FSS.A2, FSS.A3, FSS.A7**
37	Provide FS04 Response (See FS04 schedule)
38	ONR Review
39	Regulator Confirm Response to Action
40	**Preparation of Safety Submission Doumentation**
41	Process start
42	Preparation of Safety Submission
43	Technical Review
44	Licensing Review
45	Update with comments from reviews
46	Issue to Regulator
47	Regulator to confirm response to action
48	Response received from ONR/EA

Methodology:
No new methodology will be used. Required analyses will be performed with the usual codes: LOFTRAN, VIPRE, Relap.

Justification of adequacy:
As described above, some of the actions have already been addressed as part of other Resolution Plans. For all remaining actions, the approach outlined above should sufficiently satisfy ONR's concerns by providing the necessary analyses to demonstrate the functional diversity for frequent faults.

Impact assessment:
• Chapter 9 of the PCSR • Chapter 15 of the EDCD, if required.