REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0078
Date sent:	09/01/2017
Acknowledgement required by:	31/01/2017
Agreement of Resolution Plan Required by:	07/02/2017
Resolution of Regulatory Observation required by:	To be determined by Hitachi-GE Resolution Plan
TRIM Ref.:	2017/9447
Related RQ / RO No. and TRIM Ref. (if any)**:**	RQ-ABWR-1060 (2016/322354)
Observation title:	Exceptions to Segregation
Technical area(s) Internal Hazards	**Related technical area(s)** Fault Studies, PSA, C&I, Electrical Engineering.

Regulatory Observation

Summary

Hitachi-GE's Topic Report on Exceptions to Segregation [1] does not appear to state how the fundamental principles of segregation, redundancy and diversity have been applied in line with expectations in ONR Safety Assessment Principles (SAPs) and, specifically, EDR.2. There is also a lack of a systematic Internal Hazards (IH) identification and consequences analysis, including identification and justification of suitable and sufficient safety measures to deliver the Fundamental Safety Functions (FSF). Furthermore, the claims, arguments and evidence presented are not coherent. Therefore, the internal hazards safety case in this area is not in line with ONR's expectations. This RO aims to deliver:

- A high level design philosophy for the approach to exceptions to segregation for all Control and Instrumentation (C&I), Electrical and Mechanical SSCs;
- A systematic analysis of Internal Hazards consequences and identification of safety measures to deliver the FSFs;
- Cohesive claims, arguments and evidence;
- Demonstration of ALARP.

The context of ONR's concerns in this area is explained below with reference to the applicable SAPs.

Background

Hitachi-GE submitted a Topic Report on Exception to Segregation (GA91-9201-0001-00084 Rev. 2). ONR has undertaken an assessment of the report and has issued RQ-ABWR-1060 (TRIM Ref. 2016/322354). The detailed comments are not repeated here. ONR's comments could be summarised as follows:

- The majority of the exceptions to segregation involve C&I components. Categorisation and Classification of the C&I systems is key to adequate application of the principle of segregation, however, this is not explicitly addressed in the Topic Report. There is a lack of a high level design philosophy and methodology on the design approach for the exception to segregation and management of segregation of C&I systems between different Cat & Class of C&I systems and between different divisions. There is also a need to consider the segregation of electrical power supplies to support the SSCs.
- The specific Internal Hazards events causing loss of SSCs subject to Exceptions to Segregation have

not been discussed. The IH safety case should systematically identify all IH events, identify all SSCs affected by the event, assess the potential consequences and identify SSCs to deliver the Fundamental Safety Functions, in line with ONR expectations in SAPs EHA.14 and ECS.2. In this context, appropriate claims, arguments and evidence should be provided (ONR SAPs para. 86). Appropriate defence-in-depth arguments and demonstration of ALARP should also be provided (SAP EKP.3). Furthermore, the Topic Report should explicitly address:

- Single failure assumption and equipment unavailability due to maintenance: The Topic Report assumes that a loss of a single division of an A1 safety function due to an internal hazard is acceptable in all cases. However, as the UK ABWR design usually assumes 3 x 100 % A1 functions, the loss of one train leads to only two trains being available to control an event. If the IH event also triggers a design basis fault for which the affected A1 system provides the primary means of protection, applying single failure assumption and equipment unavailability due to maintenance may result in the absence of Class 1 protection for that sequence. Please see also RQ-ABWR-1004 on Design Basis Analysis (DBA). The expectations on single failure assumptions and equipment unavailability in DBA have previously been discussed in RQ-ABWR-021. Single failure assumption and equipment unavailability due to maintenance is not addressed in the Exceptions to Segregation report or in the Internal Hazards safety case more generally. It is also noted that a four divisional C&I architecture generally meets N+2. However, there are C&I functions with three trains and there are only two Fuel Pool Cooling (FPC) trains (RO-ABWR-0031). ONR expectations on single failure assumptions are in SAPs EDR1 and EDR.4. For expectations on DBA in the context of this report, Hitachi-GE is referred to SAPs EHA.5 and EHA.6.
- Common Cause Failures: The Topic Report did not address how common cause failures are minimised or avoided in the context of the systems in the scope of the Exceptions to Segregation report e.g. the RHR system. SAP EDR.3 lays out ONR expectations on that Common Cause Failure should be addressed where SSCs involve redundant or diverse components and that Common Cause Failure claims should be substantiated. All Class 1 protection systems should employ diversity in their detection of and response to fault conditions, preferably by the use of different variables (ESS.7).
- Suitability and sufficiency of identified SSCs: The Topic report concludes that segregated SSCs are available to deliver the FSFs and this may include alternative diverse devices in different locations. However, no further information has been provided on the suitability and sufficiency of these devices or on their classification. Implicit claims have been made throughout the report. Explicit claims (with the requisite substantiation) should be provided.

Hitachi-GE “Topic report on use of the PSA in ALARP assessment” [1] shows that a large release results in the consequences specified in the societal risk Target 9 and the overall large release frequency is currently above Target 9 Basic Safety Objective (BSO). The dominant contributors to the UK ABWR large release frequency are internal fire and flooding events ([2] and [3]). ONR expectation is that Hitachi-GE uses the PSA as an input into the demonstration of ALARP to provide a robust justification that the UK ABWR design considers everything that is reasonably practicable to reduce the risk as close to and ideally within the BSO, and is in an ALARP position. This demonstration should include consideration of segregation as well as other aspects of internal hazards design not covered by this RO.

Regulatory Expectation

- A high level design philosophy for the Exception to Segregation for all C&I, electrical and mechanical SSCs should be made available. This should state how management of segregation of SSCs and in particular C&I systems between different Cat & Class of C&I systems and between different divisions, is achieved. Adequate segregation and availability of electrical power supplies to support C&I and mechanical SSCs should be considered in the design philosophy.
- The Topic Report should systematically identify all IH events, identify all SSCs subject to Exceptions to Segregation that may be affected by the event, assess the potential consequences and identify the SSCs to deliver the Fundamental Safety Functions in line with ONR SAPs. This should include consideration of single failure criterion and equipment unavailability due to maintenance, and common cause failures. The suitability and sufficiency of identified SSC should be stated.
- Cohesive claims, arguments and evidence should be provided to support the suitability and rigour in the application of the Exceptions to Segregation design philosophy.

- Demonstration of ALARP confirming that segregation is prioritised in all operational states and exceptions to the principle of segregation are avoided as far as is reasonably practicable.

References

[1] Hitachi-GE Nuclear Energy, Ltd., GA91-9201-0001-00232, “Topic Report on Use of PSA in ALARP Assessment - Current Status and Future Applications” Rev. 0, September 2016.

[2] HGNE COMMERCIAL - UK ABWR - GA91-9201-0003-01434 - AE-GD-0751 - Rev 0 - Task Report 14 for Fire PSA (Fire Risk Quantification) - 01 September 2016

[3] HGNE COMMERCIAL - UK ABWR - GA91-9201-0001-00229 - AE-GD-0788 - Rev 0 - UK ABWR GDA Topic Report on Flooding PSA - 09 August 2016

Regulatory Observation Actions

RO-ABWR-0078.A1

- **A1.1** - Provide a document with the design philosophy and rule sets which ensure that a systematic process is followed in the determination of segregation requirements for all C&I, electrical and mechanical SSCs.

  The document should clearly indicate how segregation of C&I, electrical and mechanical systems of different divisions and Cat & Class ensures availability of redundant and diverse systems. It should also state how segregation of SSCs is achieved and managed in all operational states of the plant.

  The document should demonstrate that the FSFs are met in the context of UK ABWR fault sequences and in line with ONR expectations on single failure, DBA and CCF.

  Where weaknesses are identified, e.g. full segregation is not considered feasible, the document should lay out the requirements for diverse systems (functionality, segregation, independence) to support that the design meets ONR's expectations.

- **A1.2** - Provide an internal hazards assessment in the 'Exceptions to Segregation' report.

  The resport should systematically and explicitly identify all IH events (including combined and consequential events) and SSCs which may be compromised by the IH events (identified according to the design philosophy and rule sets in A1.1).

  For each internal hazard, the document should list all potential SSCs affected by the event. It should also provide the assessment of the potential consequences, and identify which other redundant or diverse SSCs deliver the FSF during the operational state considered.

  The assessment should explicitly refer to the Hazard Assessment Topic Reports documenting methodologies and calculation results for the UK ABWR Rooms and Divisions in scope.

  Common cause failures, the single failure criterion and equipment unavailability due to maintenance should be addresed explicitly.

- **A1.3** - Provide the claims, arguments and evidence in support of the suitability and sufficiency of segregation, redundancy and diversity for SSCs identified and studied according to A1.1 and A1.2.

  Defence-in-depth claims should be also stated.

- **A1.4** - Provide an ALARP justification. The ALARP justification / document should demonstrate that:

  - Segregation is prioritised in all operational states and exceptions to the principle of segregation are avoided so far as is reasonably practicable.

- Optioneering studies aimed at avoiding / eliminating exceptions to segregation are carried out.
- The UK ABWR PSA should be used to inform the scope of the optioneering studies and provide an estimate of the safety benefit in terms of core damage frequency and large release frequency reduction associated to the options considered in the ALARP justification.

The options considered, ratings and the outcome selected should be provided to demonstrate that exceptions to the principle of segregation are avoided so far as is reasonably practicable.

Resolution required by to be determined by Hitachi-GE Resolution Plan

REQUESTING PARTY TO COMPLETE	
Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	