REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0061
Date sent:	13 July 2015
Acknowledgement required by:	7th August 2015
Agreement of Resolution Plan Required by:	21st August 2015
Resolution of Regulatory Observation required by:	31st January 2017
TRIM Ref.:	2015/260295
Related RQ / RO No. and TRIM Ref. (if any)**:**	RQ-ABWR-0436
Observation title:	Reactor Pressure Vessel Instrumentation Connections
Technical area(s) Control & Instrumentation	**Related technical area(s)** Fault Studies Probalistic Safety Assessment Mechanical Engineering Structural Integrity Reactor Chemistry Human Factors Internal Hazards External Hazards Civil Engineering

Regulatory Observation

Summary

During Step 2 of the Generic Design Assessment (GDA) of the UK Advanced Boiling Water Reactor (ABWR) an area to follow up during Step 3 was identified (see ONR Step 2 UK ABWR Control and Instrumentation Assessment Report ONR-GDA-AR-14-006).

This area was related to the sharing of instrumentation connection lines, often referred to as instrument impulse lines, by the Primary Protection System (SSLC), Secondary Protection System (HWBS) and Plant Control System (PCntlS) to the Reactor Pressure Vessel (RPV). The particular concern being the potential susceptibility of the proposed design to common cause failure of the four lines that would affect all divisions of the three main Control and Instrumentation (C & I) systems simultaneously. The SSLC design proposed for the UK ABWR is based on a four division design with four sets of instrument impulse lines providing the means of connection to the RPV. The four sets of RPV impulse lines are also shared by the HWBS and the PCntlS.

ONR's assessment during Step 3 has revealed further information relating to the instrumentation impulse line connections, in particular their use for additional instrumentation associated with the automation of some of the Secondary Protection System safety functions which may also be connected to the RPV impulse lines.

During Step 3 Hitachi-GE issued a Topic Report on the Reactor Pressure Vessel Instrument System (GA91-9201-0001-00056) which states within Section 3.1;

"Common pressure taps / sensing lines are used for a number of the sensors in order to minimise the number of penetrations of the reactor pressure vessel"

Further information is provided in Fig. 3.1-1 of GA91-9201-0001-00056 which diagrammatically shows the instrumentation connections of the Safety Class 1 and 2 instruments and other instrumentation.

The current C & I safety case submission does not include adequate justification for the use of common RPV

instrumentation impulse lines and how common cause failures are protected against. ONR is aware that Hitachi-GE is currently reviewing the design of the RPV impulse lines and is undertaking an optioneering exercise. The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the connection of instrumentation to the RPV.

Background

ONR's high-level principles for the architecture of C & I systems for nuclear power plant (NPP) are based on the use of three independent, diverse and segregated platforms. Independence of each platform is expected throughout the design from the instrumentation that senses the process variable, the safety systems logic solver or control system function that make decisions, and the final actuation equipment that acts on the plant to terminate a fault or provide control. Independence, diversity and segregation are means of protecting against common cause failures and any design submitted to ONR is subject to an in-depth assessment to identify where these principles are challenged. Common cause failures are a particular concern when common equipment or services are utilised to support the function of all three C & I platforms. It is therefore ONR's expectations that independence should be provided and where it is not a robust detailed justification which takes into account all potential failures is provided and the overall risk to the public and workers is As Low As is Reasonably Practicable (ALARP).

ONR's Safety Assessment Principles (SAPs) set out the expectations with regard to the claims that can be made for common cause failure. Engineering Principle EDR.3, Design for Reliability specifically addresses common cause failure.

Engineering Principles: design for reliability	Common cause failure	EDR.3
Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.		

Further explanation is given in paragraphs 184 to 187 of ONR's SAPs.

184. CCF claims should be substantiated.
185. In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by ONR of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis. A worse figure may need to be used (say 1 per 10 000 or 1 per 1000) according to the complexity and novelty of the system, the nature of threat and the capability of the equipment.
186. Nevertheless, it is conceivable that the continuing accumulation of good data and advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the dutyholder for better figures. Such a case would not then be ruled out of consideration.
187. Where required reliabilities cannot be achieved due to CCF considerations, the safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.

This RO is therefore focused on ONR obtaining a clear understanding of the design of the RPV instrumentation system Hitachi-GE propose for the UK ABWR and how common cause failures are included in the overall justification.

The submissions received to date do not provide adequate substantiation of the use of common or shared RPV instrumentation impulse lines.

The key products of this RO will be:

1. A holistic review of the design of the RPV instrumentation system which demonstrates the design is ALARP. This should include a justification for any design changes Hitachi-GE propose to address this RO in respect of:
    a. the use of the same impulse lines by all three major C & I systems

   b. the use of a common physical measurement, pressure, as both a direct input to the protection and control systems and as a surrogate for other measurements such as level and flow.
2. A thorough review of common cause failure mechanisms which should include, but not limited to;
   a. Internal hazards
   b. External hazards
   c. Maintenance errors
3. A review of the Fault Analysis to identify where there are potential vulnerabilities to common cause failures and a demonstration that the design is ALARP. Where vulnerabilities are identified the associated faults should be stated.
4. Inclusion and assessment of the all equipment in the RPV instrument impulse lines in the probabilistic safety analysis. This should include all mechanical and process equipment associated with the RPV impulse lines such as pipes, valves etc and consider common cause failures.

Due to the potential effect, on the RPV design, piping design and layout, of any design changes required to respond to the actions in this RO, Hitachi-GE should demonstrate that the Structural Integirty and Civil Engineering disciplines have been involved in the optioneering process. This is particularly important where there are arguments presented with regard to the design of Reinforced Contrete Containment Vessel (RCCV). It is ONR's intention to issue a Structural Integrity Regulatory Oberservation on this topic.

All of the above points should take into account any changes that have been made to the UK ABWR safety case, in particular the changes in claims on the PCntlS and the design basis transient analysis, and the overall design.

An important outcome of this RO will be the agreement with ONR that the design of the RPV instrumentation system meets the independence requirements and has adequately considered common cause failures of the four division RPV instrumentation impulse lines. In addition the claims of independence and common cause failure will be considered specifically by the ONR Fault Studies and Probabilistic Safety Assessment Specialist Assessors and will form part of the their overall assessment. Other ONR Specialist Assessors will also take into consideration Hitachi-GE's response to this RO.

Regulatory Observation Actions

RO-ABWR-0061.A1

Hitachi-GE are to develop suitable documentation that includes a description of the optioneering studies that have been carried out to determine the form of the RPV instrumentation lines used for pressure and level measurement. The optioneering should address how specifically common cause failures have addressed in respect of the impact on pressure and level measurement and impact on the three major C & I systems.

Resolution required by:- October 2015

RO-ABWR-0061.A2

Hitachi-GE are to develop suitable documentation that substantiates the proposed design of the RPV Instrumentation System in respect of C & I including the consequences of common cause failure. It is expected that the documentation will follow the claims, arguments and evidence approach.

Resolution required by:- March 2016

RO-ABWR-0061.A3

Hitachi-GE should confirm that the proposed design of the RPV impulse lines has been included in the safety cases for all affected topic areas including structural integrity, mechanical engineering, Fault Studies and PSA.

Resolution required by:- January 2017

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