REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0027
Date sent:	29th April 2016
Acknowledgement required by:	27th May 2016
Agreement of Resolution Plan Required by:	*To be determined by Hitachi-GE Resolution Plan*
Resolution of Regulatory Observation required by:	*To be determined by Hitachi-GE Resolution Plan*
TRIM Ref.:	2016/179080
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	Hardwired Back Up System
Technical area(s) 6. Control & Instrumentation	**Related technical area(s)** 4. PSA 5. Fault Studies 7. Electrical Power Supply 11. Mechanical Engineering

Regulatory Observation

Summary

Hitachi-GE's Step 2 Preliminary Safety Report (PSR) and the Chapter 14 of the Pre-Construction Safety Report (PCSR) provides high level information relating to the design of the Hardwired Backup safety System. The information is limited to describing the extent of the safety functions it provides and a brief description of the technology that will be used to implement these functions.

The Basis of Safety Case (BSC) for the Hardwired Backup System (GA91-9201-0002-00029 - 3D-GD-A0009 - Rev 0) provides further information than provided in the PSR and PCSR but does not give a full description of the overall system. Both reports and the BSC indicate that the UK ABWR Hardwired Backup System will consist of hardwired relay logic and trip amplifiers and will be diverse from the Safety System Logic and Control (SSLC) system.

During Step 2 a Regulatory Query (RQ) was raised (RO-ABWR-00273) requesting clarification of what technology would be used for the Hardwired Backup System. The response to this RQ (GA91-9201-0003-00112) indicated that

"The selection of the hard wired backup system technology is still to be confirmed. The current intention is to use analogue Trip Units and relay logic for voting. The inter connections will be hard wired."

The current C & I safety case submissions or information provided in the response to RO-ABWR-00273 does not include sufficient information on the overall design of the Hardwired Backup System, the technology the system will be based on and how the design will address common cause and systematic failures (refer to IEC 61508). The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the design and extent of the Hardwired Backup System.

Background

The hardwired backup system has an important role in the overall safety of the UK ABWR. The reason for this is that it provides defence in depth and supports the overall probabilistic claims for the UK ABWR. During Step 2 of GDA Hitachi-GE have developed and presented safety case information on the major C & I systems for the ABWR covering the Safety System Logic and Control (SSLC), the hardwired back-up system and the main plant distributed control and instrumentation system. Currently the safety case for the hardwired backup System for the UK ABWR has not been sufficiently developed to enable ONR to perform a comprehensive

assessment.

The provision of secondary or backup protection systems is a UK regulatory expectation for defence in depth and to protect against frequent faults. The safety functional requirements for backup protection systems should be clearly linked to design basis and probabilistic safety analysis and identified in the UK ABWR Fault Schedule. The design of the hardwired backup system should be sufficiently described and justified during GDA to give ONR confidence that it can deliver its safety function requirements.

The UK ABWR C & I PSR, chapter 14 of the PCSR and the Hardwired Backup Systems BSC state that the hardwired backup system will use diverse technology from the primary protection (Safety System Logic and Control – SSLC) and the plant control system, but does not explain the overall architecture or provide any design information for the equipment and components that the system will utilise. The current design for the UK ABWR appears to be a collection of systems performing dedicated safety functions and does not take into account common cause or systematic failures. In addition the safety function requirements of the UK ABWR hardwired backup system are currently being reviewed and update to accurately reflect the requirements of the deterministic and probabilistic safety analysis which is currently being carried out for the UK ABWR.

For ONR to complete its work, Hitachi-GE should develop the design of the hardwired backup system to provide confidence that the system will support the safety claims made against it.

The key products of this section of the RO will be the provision of documents describing:

1. A full list of safety functions which are referenced to the UK ABWR fault schedule.
2. Design standards and methodologies used for the design and development of the hardwired system.
3. The technology the hardwired backup system and how the technology will be used to perform the safety functions identified above. (Component manufacturer level information is not required)
4. The development of a hardwired backup system architecture drawing which includes interfaces to other systems.
5. A description of how the design protects against common cause and systematic failures.

An important outcome of this RO will be the agreement with ONR that the design of the hardwired backup systems is correctly classified and that it can meet the safety function requirements identified in the UK ABWR Fault Schedule.

Regulatory Observation Actions

RO-ABWR-0027.A1

Hitachi-GE are to develop a comprehensive list of safety function requirements for the hardwired backup systems which are linked to the UK ABWR Fault Schedule.
Resolution required by September 2015

Resolution required by September 2015

RO-ABWR-0027.A2

Hitachi-GE are to develop suitable documentation that describes the design, design process and potential technology used for the hardwired backup system and how the design protects against common cause and systematic failures. This should describe what design attibutes the hardwired backup system must have to demonstrate common cause and systematic errors relating to other C&I safety systems will be avoided, including interfaces with those systems. An outline architeture drawing of the system should also be included.

Resolution required by June 2016

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	