REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0031
Date sent:	1st December 2014
Acknowledgement required by:	22nd December 2014
Agreement of Resolution Plan Required by:	23rd December 2014
Resolution of Regulatory Observation required by:	30th June 2015
TRIM Ref.:	2014/441860
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	SSLC and Support System Architecture
Technical area(s) 6. Control & Instrumentation	**Related technical area(s)** 5. Fault Studies 11. Mechanical Engineering

Regulatory Observation

Summary

The UK ABWR safety system logic and control (SSLC) is a Class 1 safety system providing control for the actuation of the UK ABWR plant level category A safety functions. In line with international standards, its internal architecture is a four-division safety system with majority voting to undertake a wide range of safety actuations such as reactor trip. There are a number of plant level safety functions that do not utilise all four safety divisions and some of which appear to fail to meet the single failure criterion at the system level. The purpose of this Regulatory Observation is to seek a safety justification for the architecture of the support systems actuated by the SSLC, particularly the fact that some of the essential safety feature (ESF) actuations are controlled by two divisions of equipment at the safety logic unit (SLU) level which contrast with higher level of SLU redundancy (three or four divisions) for other safety functions. This RO is a joint one between C&I and fault studies as the ONR's challenge is on the adequacy of the delivery systems (for example automatic depressurisation) as well as the C&I (SSLC) controlling the actuation of the safety function.

Background

Relevant good practice in the UK for essential safety feature actuation functions of a primary reactor protection system is that the divisional structure is maintained down to the final actuator. For example, for each pump of a 4-division safety injection system the control and instrumentation would maintain the 4 divisional structure for actuating each pump down to final circuit breaker controlling its start-up. This means that such systems have considerable fault tolerance to demand failures and spurious actuations.

Another important aspect of relevant good practice established in the UK is that primary reactor protection systems are largely dedicated to the role of performing category A safety functions.

Table 5.2-1 from the Preliminary safety Report for the UK ABWR shows that the reactor trip function (RPS) and main steam isolation valves are controlled by four divisions and subject to detailed assessment appear to be consistent with UK's relevant good practice. Similarly, the high pressure emergency core cooling function is engineered in the SSLC by a full three divisional structure consistent the N+2 expectation for such systems (N is the minimum required to deliver the safety function). Control of the three emergency diesel generators is also in three divisions spread across two SLUs. However a number of plant level safety function including automatic depressurisation (ADS, claimed as safety functional Category A) do not meet the N+2 criterion. This potentially indicates that the ADS is either under-classified for its Category A safety functional role or the SSLC interface and the architecture of the ADS are not consistent with UK's expectations.

Hitachi-GE should undertake a review of its design and confirm the categorisation and classification of all plant level systems which are controlled by the SSLC and provide a safety justification to demonstrate that all Category A Safety functions meet the N+2 criterion. Where they are Category B or lower a full justification will be required as to why the SSLC is used for a lower function.

For all plant level safety functions Hitachi-GE will need to assign a safety category. Where an assignment is category A ONR's expectation would be, as a minimum, that the overall system delivering the safety function would follow the same three divisional architecture of the main ECCS (for example there would be an ADS(A), ADS(B) and ADS(C) an FPC(A), FPC(B), FPC(C) etc.). If the function is category B then a justification would be required why such actuations are controlled by the safety class 1 SSLC.

Regulatory Observation Actions

RO-ABWR-0031.A1

Hitachi-GE should review and assign a safety functional category to all of the SSLC plant level functions. A list of safety function and category should be submitted to ONR for assessment.

Resolution required by January 2015

RO-ABWR-0031.A2

Where the functions listed above are assigned to a category A safety function then ONR's expectation is that they are designed to follow an N+2 format consistent with the ECCS and therefore the SSLC and the systems it is actuating are modified accordingly. Where the functions are category B or lower then a safety justification should be provided why the SSLC is used for a lower safety functional category role. Where category B is required and two divisions or lower is retained then full justification that no failure in this reduced architecture (dual or single division) could interfere with the operation of the whole four divisional SSLC. Hitachi-GE should identify, and submit a document that descibes any design changes that are required to comply with the expectations set out in the RO.

Resolution required by June 2015

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	