REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0030
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.:	2014/441707
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	Embedded C&I subsystems and smart devices
Technical area(s) 6. Control & Instrumentation	**Related technical area(s)** 5. Fault Studies 11. Mechanical Engineering

Regulatory Observation

Summary

Many support systems important to safety for the UK ABWR will have embedded control and instrumentation (C & I) subsystems and smart devices. The correct operation of these will be critical for the achievement of the safe operation of the UK ABWR.

Typical support systems important to safety employing C&I based embedded subsystems include heating and ventilation, chilled water, electrical power, variable speed drives, complex plant sensors and plant actuators.

The current safety submission for the UK ABWR does not cover these important embedded C&I subsystems and the purpose of this regulatory observation is to provide guidance on their identification and safety justification.

Appendix 1 of this RO gives a definition of embedded control and instrumentation subsystems and smart devices.

Background

Safety systems such as the High Pressure Core Flooder System and Safety System Logic and Control require safety support systems for their correct operation. For the UK ABWR these support systems include heating, ventilation and air conditioning (HVAC), electrical power supply systems and many others. There are other systems, for example, suppression pool clean up, offgas and process radiation monitoring systems that may also include embedded C & I systems must be included in this RO.

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 does not cover important C&I systems embedded within other key safety support systems, for example HECW, HVAC, Electrical Power Systems and Reactor Internal Pump drives. Embedded C&I systems have an important role in the overall safety of the UK ABWR. The reasons for this is their spurious failure or failure to act on demand could lead to failure of the support system they controlling with consequential failures of the frontline safety systems due to loss of functions such as cooling or the provision of power.

An additional complicating factor is that many of these embedded C & I systems use complex programmable technology, this is often referred to as Smart technology or Smart devices. This complication is compounded by the fact that many of the suppliers of such support systems use commercial off-the-shelf (COTS) components for the design of their embedded C & I. Whilst COTS components are suitable for commercial use their standard of design, production and analysis falls considerably short of that required for safety class (as set out in IEC 61513 and 61226) 1 (SC1) and safety class 2 (SC2) systems and many of the UK ABWR support system will almost certainly be classified as either SC1 or SC2.

Identifying the embedded C & I systems during the GDA is necessary to ensure that ONR's assessment process is complete and covers all sources of major risks to the safety of the facility. Justifying a COTS component to meet SC1 and SC2 standards is a complex process and therefore early agreement with the regulator during GDA of the principles and methods of their design and safety justification is important to eliminate the risk of late regulatory challenges during the site-specific phase of the project.

For ONR to complete its GDA work, Hitachi-GE should use the outcome of the regulatory observation 8 (RO 8) and RO 10 to identify those support systems to whose correct operation is necessary to support frontline safety systems performing Category A and B functions. Once this work is completed, Hitachi-GE should review each system for its use of embedded C & I, particularly those systems employing smart devices. In addition to this work, Hitachi-GE should review its existing designs for the use of smart devices elsewhere in the facility covering functions such as smart valves, smart sensors and the use of complex programmable devices on variable speed drives such as the reactor internal pumps. As stated at the beginning Hitachi-GE are to review other systems such as offgas and process radiation monitoring for the potential use of smart devices.

The three key products of this RO will be:

1. A comprehensive list of all embedded C & I systems which clearly identifies where smart technology (using either microprocessor or programmable complex electronic components for example ASIC, FPGA, CPLD, PLA, PAL, PLD, ROM) is planned to be or is highly likely to be installed in any SC1 or SC2 support or direct acting safety system.
2. The development of the principles of the assessment of production excellence and independent confidence building for all SC1 and SC2 devices to enable ONR assess the proposal using its Technical Assessment Guide 46 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf.
3. During Step 4 of GDA applying the principles of the assessment of production excellence and independent confidence building developed in action 2 to one SC1 and one SC2 devices from the comprehensive list of devices given in action 1.

An important outcome of this RO will be the agreement with the regulator to the use of the principles of production excellence and independent confidence building in the design, production and safety justification of smart embedded devices during the site-specific phase. ONR recognises that much of the detailed analysis of the design of many embedded C&I systems and Smart devices cannot be undertaken until the site-specific phase. However, during GDA, Hitachi-GE should have good knowledge of where the designers will need to use embedded C & I systems and smart devices and in some cases have sufficient detailed information to undertake a full justification of two devices. The reason ONR is seeking two examples is that it will give regulatory confidence that the principles of production excellence and independent confidence building agreed with ONR from action 2 can be applied to a much larger number of devices during the later site-specific phase of the project.

Regulatory Observation Actions

RQ-ABWR-0030.A1

Hitachi-GE are to derive a list of embedded SC1 and SC2 C&I systems which clearly identifies the use of smart devices based on the analysis of

- *RO 8 and RO 10.*
- *Knowledge of the location of other sources of smart devices as sensors, actuators and variable speed drives used in SC1 and SC2 systems throughout the facility.*

Resolution required by June 2015

RO-ABWR-0030.A2

Hitachi-GE are to develop a topic report on their proposed approach to the assessment of the production excellence of all smart devices and to give recommendations to a future licensee on methods of independent confidence building.

Resolution required by April 2015

RO-ABWR-0030.A3

From the outcome of action 2 Hitachi-GE are to develop a topic report demonstrating the viability of the production excellence and independent confidence building process by applying these methods to one SC1 and one SC2 devices taken from the list derived in action 1.

Resolution required by June 2017

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