REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0032
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 April 2015
TRIM Ref.:	2014/441983
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	Safety System Logic & Control (SSLC) Design
Technical area(s) 6. Control & Instrumentation	**Related technical area(s)** 5. Fault Studies 4. PSA 14. MoS & QA

Regulatory Observation

Summary

Hitachi-GE's Step 2 Preliminary Safety Report (PSR) and Chapter 14 of the Pre-Construction Safety Report (PCSR) provides high level information relating to the design processes that will be used during the development of the Control and Instrumentation (C & I) systems for the UK ABWR. In particular these documents provide a high level outline of the lifecycle approach to the design of C & I systems by briefly describing the stages of the process. The information is generic in nature and could be applied to any C & I system. During Step 2 of the Generic Design Assessment (GDA) Hitachi-GE committed to modify the platform technology for the main safety class 1 Safety System Logic and Control (SSLC). This commitment was given to improve the diversity of this system from the other major C & I platforms by developing a new platform based on Field Programmable Gate Array (FPGA) technology. The proposed design of the FPGA based SSLC will therefore be new and its design will need to follow a defined process that is commensurate with its deterministic and probabilistic safety claims.

The current C & I safety case submissions do not cover the specific design and development processes for the FPGA based SSLC. The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the design and development process for the new design SSLC.

Background

To support the design of the C & I systems for the UK ABWR it is essential that the design processes are adequate to support the safety categorisation and classification claims made upon them. This is particularly important when a new design, such as is the FPGA based SSLC, is started. Where functional claims of protection against common cause failures are made (e.g. independence) on the physical systems these requirements also extend to the design and development processes for these systems.

The Step 2 C & I PSR and Chapter 14 of the PCSR (Control & Instrumentation) set out the Hitachi-GE high-level design development approach. ONR's Step 2 C & I assessment of the UK ABWR C & I design identified two areas, associated with this RO, that required follow up during Steps 3 and 4 of GDA. These two areas requiring further work are related to the development of processes for the design of complex components such as FPGAs and the demonstration of the independence of the SSLC design team from teams developing other UK ABWR C & I platforms. This RO is therefore focused on the overall design and development process for the FPGA based SSLC and the independence of the SSLC design team from other C & I platform design teams.

ONR recognises that Hitachi-GE have developed, over a long period of time, design and development

processes which it considers to be fit for purpose. As the use however of FPGA technology for the primary protection system of a nuclear power plant is new to Hitachi-GE and will be first time this technology has been used for this purpose in the UK. In view of this position there is a regulatory expectation that Hitachi-GE will demonstrate the robustness of its design and development processes.

Design Process

International standards set out expectations for the design of C & I safety systems which require the design processes to be commensurate with their deterministic and probabilistic safety claims. This is particularly important when designing systems which perform Category A, Classification 1 functions. Where new systems such as the FPGA based SSLC are being designed and developed the design processes should be set out at the beginning of the design lifecycle. The PSR sets out a lifecycle approach giving, in some cases, only high-level information and in other cases referencing out to the PCSR where again only high level information is provided.

To enable ONR to complete its assessment during GDA it will need to gain confidence that the FPGA based SSLC is designed to fulfil its safety requirements and complies with the appropriate international standards and relevant good practice. To meet this objective Hitachi-GE should develop its design and development process taking into account requirements specified in international standards and relevant good practice established in the UK. It is expected that the design and development process should be based on the overall life-cycle approach and apply validation and verification (V & V) activities throughout the design process. These V & V activities should be commensurate with the safety claims made upon the systems and be demonstrably robust and independent from the design function (graded in accordance with the classification of the system). The activities associated with the design and development lifecycle should be identified within a suitable document and activity schedule (Gantt chart) which will give ONR clear visibility of all the activities Hitachi-GE intend to carry out during GDA and after GDA. The design and development process along with the overall activity schedule should be submitted to ONR for assessment.

The key products of this section of the RO will be:

1. A comprehensive design and development lifecycle plan which identifies and describes all activities including verification and validation.
2. An activity schedule which identifies all activities from point 1. This schedule should allow for regulatory interaction and indicate key milestones.
3. Where independent organisations are being utilised by Hitachi-GE to support the overall design process this should be clearly identified on the activity schedule.
4. A demonstration that the design and development of the SSLC will be sufficiently complete by the end of GDA to enable ONR to complete a meaningful assessment.

Independence of Design Teams

The Hitachi-GE Step 2 C & I PSR and chapter 14 of the PCSR states that measures will be applied to protect against common cause failures affecting the three main C & I platforms. These claims include the use of independence, diversity and separation as ways of protecting against this type of failure.

IEC 61513, section 5.4.2.6 Defence against CCF, states:

The origin for systematic latent faults is mostly related to human errors. They may be introduced in any phase of the life cycle of an I & C system. The use of computers allows more complex algorithms and processes to be used than is possible with hardware alone. Furthermore the design effort of computer based I&C, including the activities related to the design of the underlying I&C platform, is higher than for hardware I&C, and the design may be more complex.

To reduce the likelihood that common cause failures introduced by the use of the same design personnel for the design of multiple UK ABWR C & I systems it is ONR expectation that the design team for the SSLC will be independent from the design teams for the other C & I platforms. This independence should extend to the teams that will perform the V & V activities associated with the SSLC design.

The key product of this section of the RO will be:

1. Demonstration that the design organisation for C & I systems is structured to provide independence in the design of the 3 main C & I platforms (SSLC, Hardwired Backup System, Plant Control System) in particular the independence of the design team for the SSLC.
2. Inclusion into the Hitachi-GE UK ABWR design and development processes the requirement for independent C & I design teams.

An important outcome of this RO will be the agreement with ONR that the design processes and supporting organisational structure are adequate to support the on-going design and development of the FPGA based SSLC. ONR recognises that the detailed design and development of the SSLC will not be completed during GDA and on-going design activities will be required after GDA for the site specific phase of the project. However, during GDA, to provide ONR with the confidence that the SSLC design is adequately controlled throughout its lifecycle Hitachi-GE should provide a justification that they have developed a sufficiently robust design and development process to support the post GDA activities.

Reference Documents;

Step 2 C & I PSR GA91-9901-0001-00001, XE-GD-0107, Rev B

Chapter 14 of the PCSR - Generic PCSR Chapter 14 Control & Instrumentation GA91-9101-0101-14000, 3E-GD-A0063, Rev A

Regulatory Observation Actions

RO-ABWR-0032.A1

Design Process
Hitachi-GE are to develop suitable documentation that describes the design and development process for the FPGA based SSLC and supports this with an Activity Schedule that demonstrates the design will be sufficiently complete by the end of GDA to enable ONR to complete its assessment. The description should include the rationale why Hitachi-GE believes the process is suitable for the design and development of a Class 1 FPGA safety system.

Resolution required by April 2015

RO-ABWR-0032.A2

Design Organisation
Hitachi-GE to demonstrate that the design team for the SSLC is effectively independent from other C & I system design teams and that the independence is included in relevant design and development processes and procedures.

Resolution required by January 2015

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	