Hitachi-GE Nuclear Energy, Ltd.
UK ABWR GENERIC DESIGN ASSESSMENT
Resolution Plan for RO-ABWR-0032
Safety System Logic & Control (SSLC) Design

RO TITLE:	Safety System Logic & Control (SSLC) Design	
REVISION :	1	
Overall RO Closure Date (Planned):		30 May, 2015
REFERENCE DOCUMENTATION RELATED TO REGULATORY OBSERVATION		
Regulatory Queries	-	
Linked ROs	-	
Other Documentation		

Scope of work :

Background

The ONR have raised RO-ABWR-0032 regarding to the design process and organizational independence of the team developing the new platform which will be used for Safety System Logic & Control (SSLC) system. In order to achieve high safety integrity of the SSLC system for the new-build Advanced Boiling Water Reactor (ABWR) power plant in the United Kingdom and to eliminate common cause failures (CCFs) with the Plant Control System and Hardwired Backup System, Hitachi is developing a next generation platform. The ONR have identified that:

(1) The new platform development shall employ the design process adequate to support the safety categorization and safety classification claims made upon them, and

(2) Common cause failures (CCFs) between platforms caused by human error of the same design personnel being involved in the multiple platforms shall be avoided.

Scope of Work:

Hitachi understands that the next platform shall be designed by applying a high safety integrity level design process. Hitachi also understands that organizational measures shall be taken in order to prevent CCFs of the SSLC, Plant Control System and Hardwired Backup System, which may be caused by human error. This resolution plan states how human errors are not implemented in the next platform.

This resolution plan describes Hitachi's plan to establish the design process. This resolution plan also describes the plan to establish organizational measures to prevent CCFs with other systems from being implemented to the new platform. Justification of the design process is in the RO on Production Excellence.

Description of work:

Action # 1: Design Process

The RO action states that:

> Hitachi-GE are to develop suitable documentation that describes and justifies the design and development process for the FPGA based SSLC and supports this with and Activity Schedule that demonstrates the design will be sufficiently complete by the end of GDA to enable ONR to complete its assessment.

In order to achieve high safety integrity, Hitachi will develop the next platform according to design and development process including verification and validation (V&V) activities compliant with SIL 3 per IEC 61508, as well as SIL 4 to a level practicably achievable employing state-of-the-art techniques and measures. IEC 62566 requirements will also be taken into account in the FPGA design process. This will lead to compliance with good practice established in UK such as ONR Nuclear Safety Technical Assessment Guide NS-TAST-GD-046 (TAG 46). The design and development process will be described in a document called Safety Plan. The Safety Plan includes the following information:

(1) Project organization:

Definition of high-level design activities.

Definition of parties involved in the design, development, verification and validation activities.

Definition of responsibilities of the parties, training, etc.

(2) Project lifecycle:

Definition of lifecycle phases and major input/outputs during each phase.

(3) Design process

Definition of design, development, verification and validation activities in each lifecycle phase, including coding rules, testing, document control, modification and maintenance.

(4) Software Tools

List of software tools used for the design, development, verification and validation activities.

Schedule of design, development and verification activities will be planned so that all activities, including assessment by ONR and third party inspection firm, will be complete within the GDA period. The schedule will then be documented into a Gantt chart going to the detailed program. The Gantt chart will be based on the Gantt chart previously presented to ONR (331-XUK-D049) with addition of time and parties in charge of major verification and validation activities.

Scope of development activity during GDA to be shown in the Gantt chart will be as indicated in Topic Report on Class 1 Platform (GA91-9201-0001-00045), reflecting discussions in the meetings with ONR during Step 2 of the GDA.

Action # 2: Design Organization

The RO action states that:

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

Hitachi understands that human error is a major cause of systematic failures, and CCF due to human error being implemented into multiple platforms shall be avoided. For this reason, Hitachi has formed a dedicated team for the new platform design. Hitachi will also involve independent organizations into verification and validation activities.

Specific details of how independence of the new platform design team will be maintained, how the other independent organizations participate in the V&V activities will be described in the Safety Plan ((1) above).

List of Output Documents:

(1) Safety Plan

(2) Proposed Detail Project-Schedule for New Class 1 Platform (331-XUK-D049, updated)

(3) Concept Approval Report by third party inspection firm

For Hardwired Backup System modules, products developed by an organization other than Hitachi-GE will be applied; in other words, products developed independently from both Class 1 and Class 2/3 platforms will be applied for Hardwired Backup System. Further information on Hardwired Backup System will be shown in response to RO-ABWR-0027.

Summary of impact on GDA submissions:

Submitted document	No	Potential Impact
Proposed Detail Project-Schedule for New Class 1 Platform	331-XUK-D049	(1) Adjustment of activity schedule to include ONR and third party inspection firm activities and to be in accordance with the Safety Plan. (2) Addition of party in charge of each activity. To be re-issued 30 April, 2015.

Preparation of the Safety Plan and third party assessment are included in the initial plan. Safety Plan will be submitted in the following two phases:

(1) Independence of organization related part: 30 January, 2015

(2) Remaining parts: 30 April, 2015.
However, compliance with TAG 46 and IEC 62566 requirements will be submitted in 30 June, 2015 as part of resolution for SSLC Production Excellence.

Concept Approval Report by third party inspection firm: 30 May, 2015.

Programme Milestones/ Schedule:

See attached Gantt Chart (Table 1).

Reference:

-

Table-1 Resolution Plan Gantt Chart for RO-ABWR-0032

Resolution Plan for RO-ABWR-0032 Action #1				October				November				December					January				February				March					April				May				June				
				6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29
No	Action Item	Start	Finish																																							
1	Design Process																																								
1	Preparation of Safety Plan	3-Oct-2014	26-Dec-2014																																							
1	Third party concept assessment	12-Jan-2015	30-Apr-2015																																							
1	Thrid party concept approval report	26-May-2015	30-May-2015																																							
2	Gantt Chart																																								
2	Update existing Gantt Chart	1-Apr-2015	30-Apr-2015																																							
3	Resolution																																								
3	Formal submission of outputs to ONR	4-May-2015	8-May-2015																																							

Resolution Plan for RO-ABWR-0032 Action #2				October				November				December					January				February				March					April				May				June				
				6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29
No	Action Item	Start	Finish																																							
1	Design Organization																																								
1	Preparation of Safety Plan	3-Oct-2014	26-Dec-2014																																							
2	Resolution																																								
2	Formal submission of outputs to ONR	30-Jan-2015	30-Jan-2015																																							