Hitachi-GE Nuclear Energy, Ltd.
UK ABWR GENERIC DESIGN ASSESSMENT
Resolution Plan for RO-ABWR-0029
SSLC Production Excellence

RO TITLE:	SSLC Production Excellence	
REVISION :	1	
Overall RO Closure Date (Planned):		30 June, 2015
REFERENCE DOCUMENTATION RELATED TO REGULATORY OBSERVATION		
Regulatory Queries	-	
Linked ROs	-	
Other Documentation		

Scope of work :

Background

The ONR have raised RO-ABWR-0029 regarding to the production excellence of the new platform which will be used for Safety System Logic & Control (SSLC) system. In order to achieve high safety integrity of the Class 1 systems for the new-build Advanced Boiling Water Reactor (ABWR) power plant in the United Kingdom and to eliminate common cause failures (CCFs) with the Class 2 and 3 systems, Hitachi-GE is developing a next generation platform for Class 1 application. ONR have identified that:

> Techniques for the design of FPGA technology has many similarities with that of the design of software for computer based safety systems, meaning that ONR's expectations for the safety demonstration of production excellence is given in ONR's Nuclear Safety Technical Assessment Guide NS-TAST-GD-046 (TAG 46) .

Scope of Work:

Hitachi-GE understands that the next platform shall be designed by applying a high safety integrity level design process, which is compliant with the production excellence guidelines in the TAG 46.

This resolution plan describes Hitachi's plan to establish the design process in accordance with production excellence guidelines

Description of work:

Action # 1: Production Excellence

The RO action states that:

> Hitachi-GE to develop a suitable document(s) describing and justifying the methodology for development of the production excellence leg of the SSLC platform design.

In order to achieve high safety integrity, Hitachi-GE will develop the next platform according 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. Production excellence guidelines in ONR Nuclear Safety Technical Assessment Guide NS-TAST-GD-046 (TAG 46) and requirements in the related standards such as IEC 62566 will also be taken into account. The design and development process will be described in a document called Safety Plan. The Safety Plan includes the following information:

[Outline of Safety Plan]

(1) Project organization:

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..

Compliance with IEC 61508, TAG 46 and IEC 62566 requirements.

(4) Software Tools

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

Compliance with IEC 61508, TAG 46 and IEC 62566 requirements.

Compliance with the TAG 46 and related standards will be also documented into the Safety Plan. Safety Plan will be assessed by an internationally well-known third party safety inspection firm, with experience in certification of Hitachi safety products, from the point of view of compliance with IEC 61508 SIL 3 and SIL 4 requirements. The third party will document the result of the assessment into a Concept Approval Report.

Action # 2: Statistical Testing

Hitachi understands that appropriate design features shall be incorporated into the next platform upon its development to allow statistical testing with thousands of test cases, which will be carried out as a part of independent confidence building measures (ICBM), to be done within reasonable time frame. Especially, Hitachi understands that the internal memory re-setting function to keep statistical independence between each test is a key to achieve the above objectives.

In order to facilitate the statistical testing, the next platform will be designed to support quick restart function with memory initialization for the purpose of maintaining statistical independence between each test while keeping total statistical testing duration realistic. Specific method for realizing the quick restart function will be documented into Safety Concept. Safety Concept is a document describing the design of how to realize required safety function, including the quick restart process. The level of description will be high-level but including sufficient information to demonstrate its feasibility of implementation.

[Outline of Safety Concept]

(1) Method to realize safety functions

Definition of safe state.

Fault monitoring and fault detection.

(2) Method to realize other important functions (including quick restart functions)

Hitachi-GE will also provide sufficient information to the parties who carry out the statistical testing, so that they can properly prepare the test environment including the test harness to interface with the division under test and the oracle which will be used as a pass fail comparator. The information includes simulated input condition, behaviour of the system, such as Interlock Block Diagram, as well as external interface of the SSLC, such as terminal block arrangement, electrical levels of the signals. A list of specific documents to be provided and their major contents will be described in the Document List for Statistical Testing.

List of Output Documents:

(1) Safety Plan (with description of compliance to TAG 46 and IEC 62566 requirements)

(2) Safety Concept

(3) Document List for Statistical Testing

Summary of impact on GDA submissions:

Safety Plan (with description of TAG 46 and IEC 62566 compliance): 30 June, 2015

Safety Concept: 30 April, 2015

Document List for Statistical Testing: 30 June, 2015

Programme Milestones/ Schedule:
See attached Gantt Chart (Table 1).

Reference:
-

Table-1 Resolution Plan Gantt Chart for RO-ABWR-0029

Resolution Plan for RO-ABWR-0029 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	Production Excellence																																								
1	Preparation of Safety Plan	7-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																																							
1	Preparation of compliance table against TAG-046 guidelines	1-Apr-2015	26-Jun-2015																																							
2	Resolution																																								
2	Compliance table against TAG-046 guidelines	29-Jun-2015	3-Jul-2015																																							

Resolution Plan for RO-ABWR-0029 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	Statistical Testing																																								
1	Preparation of Safety Concept	1-Nov-2014	31-Jan-2015																																							
1	Preparation of document list for Statistical Testing	1-Apr-2015	26-Jun-2015																																							
2	Resolution																																								
2	Formal submission of outputs to ONR	29-Jun-2015	3-Jul-2015																																							