REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0029
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 September 2015
TRIM Ref.:	2014/441595
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	SSLC Production Excellence
Technical area(s) 6. Control & Instrumentation	**Related technical area(s)** 5. Fault Studies 11. Mechanical Engineering

Regulatory Observation

Summary

The UK ABWR's Safety System Logic and Control (SSLC) is the main safety class 1 control and instrumentation (C & I) system performing the safety functions of reactor trip and essential safety feature actuations. To meet ONR's expectations on diversity the platform technology for the SSLC will be based on field programmable gate arrays (FPGA) supported by other more conventional integrated and discrete electronic circuits. 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 technical assessment guide 46 (http://www.onr.org.uk/operational/tech_asst_guides/index.htm). This regulatory observation provides further guidance on the application of TAG 46 specifically on the topic of production excellence for the FPGA based SSLC. For Step 3 this RO is seeking a topic report describing and justifying the methodologies selected by Hitachi-GE.

Background

ONR's document NS-TAST-GD-46 (Rev 3) (TAG 46) gives guidance on the twin legs of production excellence and independent confidence building measures for computer based safety systems. Production excellence is about using a very high quality process the product of which has a very low number of design or production errors (the assumption is that no product of such complexity is free of errors). This RO is entirely about the production excellence leg, another RO will be developed during Step 3 of GDA on the independent confidence building leg. The focus of TAG 46 is on microprocessor based safety systems including technology used for large reactor safety systems that are based on complex multi-microprocessor technology with the implementation of safety functions in application software, which itself requires the services and support of operating system software. The ABWR SSLC does not use microprocessors and does not employ operating system software or applications software; it is based on field programmable gate array (FPGA) technology.

Although the underlying technology for the SSLC is based on FPGAs ONR judges that the safety assessment guidance given in TAG 46 is applicable. Most FPGAs are designed using a hardware description language (HDL) which is similar to more traditional programming languages such as C. The SSLC will require the development of the equivalent of an operating system (platform logic and control) to provide services to the application FPGAs (equivalent to application software) executing the safety functions. The purpose of this RO is to provide guidance on the interpretation of TAG 46 for FPGA technology.

Section 5.3 of TAG 46 covers production excellence and the following paragraphs provide additional guidance in relation to FPGA technology.

Major advances in the use of formal mathematically verifiable methods (formal methods) for the design of

complex control systems have made such techniques commercially viable in the past two decades. For UK Nuclear Power Plant (NPP) to date advanced mathematical techniques have been applied in the independent confidence building part of the process for reactor safety systems. The reason for applying formal methods during the independent confidence building process is that the main platform technology of the systems proposed for the UK had already been developed. Applying formal methods at any stage of a project to deliver a reactor safety system is very beneficial although applying such methods at the end of the process does run the risk of revealing the need for late changes. Hitachi-GE are designing the FPGA based technology for the UK ABWR project and is in the position where they can apply formal methods as part of the design and development process for the SSLC and claim it as part of the production excellence leg.

The application of formal methods in the production excellence leg of the process will form an important element in meeting the expectations given in paragraph 5.3.2 of TAG 46 on the avoidance and detection of errors. Such methods can also provide early and mathematically verifiable justification that the formally developed system meets its requirements specification.

ONR's expectations for paragraph 5.3.4 will be met by showing compliance with IEC 61513 process its referenced standards and specific to FPGAs IEC 62566 will be very relevant.

ONR's expectations on dynamic testing stated in paragraph 5.3.6 TAG 46 is that this is not a part of GDA but is best done as a part of independent confidence building leg by the licensee in the site specific phase of the project. However, during GDA Hitachi-GE will need to demonstrate that the SSLC is capable of undertaking many thousands of dynamic statistical tests ahead of active commissioning on real equipment at the site without making the tests unfeasible in terms of the time between each test. A key to this will be the re-setting of the system to clear it of any memory effects and this will need to be done without putting significant life limiting transients on the system but sufficiently quickly to make many thousands of statistical tests feasible. Hitachi-GE should provide high-level SSLC design information to allow a third party organisation to design a test oracle suitable for statistical testing to be carried out. This is required to build confidence that the SSLC can be subjected to statistical testing.

The appendices of TAG 46 contain very specific information on coding standards, hardware considerations, fault monitoring, verification and validation, testing, documentation, training, operations, modification and maintenance and appendix 3 on probabilistic considerations. All of these topics will need to be covered although some such as operations, modification and maintenance and training will be covered at the level of key principles for GDA.

ONR's expectations are that to meet the requirements of this RO the deliverable will be a topic report describing the design methodology and it is this methodology report that will form the key deliverable for Step 3.

Regulatory Observation Actions

RQ-ABWR-0029.A1

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

Resolution required by June 2015

RQ-ABWR-0029.A2

Hitachi-GE should identify how and what information it will provide to allow a third party to design a test oracle and harness to conduct statistical testing, this should include all the information required to enable an oracle to be designed.

Resolution required by June 2015

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	

NOT PROTECTIVELY MARKED