REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0062
Date sent:	13 July 2015
Acknowledgement required by:	7th August 2015
Agreement of Resolution Plan Required by:	21st August 2015
Resolution of Regulatory Observation required by:	31st January 2017
TRIM Ref.:	2015/260354
Related RQ / RO No. and TRIM Ref. (if any)**:**	Safety System Logic & Control (SSLC) Class 1 HMI 2014/440740
Observation title:	Testing and Maintenance of Safety Systems
Technical area(s) Control & Instrumentation	**Related technical area(s)** Fault Studies Probalistic Safety Assessment Mechanical Engineering Electrical Engineering

Regulatory Observation

Summary

During Step 3 of the UK advanced Boiling Water Reactor (ABWR) Control and Instrumentation (C & I) Generic Design Assessment (GDA) the approach to testing and maintenance of safety systems has been discussed. In particular the testing and maintenance while the nuclear power plant (NPP) is at power. Hitachi-GE have presented the method used for testing and maintaining ABWR safety systems in Japan and the proposed approach for the UK ABWR which aligns with the Japanese method with regard to the methodology and test frequency.

Chapter 14 of Hitachi-GE's Pre-Construction Safety Report (PCSR) (G A10-9101-0101-14000 Rev A) provides high level information relating to the Testing of Safety Systems. The PCSR sets out the high-level requirements for the design of the C & I Architecture and the platforms and systems that it comprises of. Chapter 14 includes summary descriptions of the test and maintenance facilities for C & I systems and links these requirements to Japanese national standards and guides (JEAC and JAEG), international standards and guides (IEC and IAEA) and to the ONR Safety Assessment Principles (SAPs). The PCSR references other supporting documentation in the form of Basis of Safety Cases (BSC)s for C & I safety systems.

Sections 14.5.2, 14.5.2.1 and 14.5.2.2 of Chapter 14 of the PCSR identify specific design features and requirements for the testing and maintenance of the Safety System Logic and Control (SSLC) system. These include Reactor Protection System (RPS), Emergency Core Cooling System (ECCS), Emergency Safety Features (ESF)

14.5.2 SSLC

(c) Redundancy

The SSLC is designed with redundancy of divisions. The redundancy allows the safety functions to be delivered in the event of a division failure while another division is under ***maintenance.***

(h) Testability

SSLC is designed to enable the ***periodic test during power operations****. The arrangement allows each division to be independently tested to confirm its ability to deliver its safety functions and that its independence has not been compromised. In addition, SSLC is designed to enable the safety functions to be delivered by the rest of the divisions during the test.*

14.5.2.1 RPS/MSIV

(3) Testability

The RPS circuits have the following testability:

(a) Manual actuation test of scram pilot valve
(b) Automatic actuation test of scram pilot valve
(c) Detector operation test
(d) Control rod scram test

14.5.2.2 ECCS/ESF

(3) Testability

The ECCS/ESF is testable for each detector and division by the injection of test signals.

The current C & I safety case submission does not include adequate justification for the testing and maintenance of safety systems, particularly with the NPP at power, and does not include the underpinning rationale for the frequency of testing and the ability of the safety system to respond to a demand placed upon it under fault conditions. The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the connection to testing and maintaining of safety systems.

Background

Maintenance, inspection and testing activities of safety systems are a key part of the overall justification of the adequacy of a new design and the ongoing operation of any nuclear facility. Within ONR's SAPs there is a series of principles, Maintenance, inspection and testing (EMT), which set out the regulatory assessment expectations. These principles outline the complete lifecycle from identifying requirements through to the assessment of the continued reliability following an event. In particular EMT.1, 2, 5, 6 and 7 describes the principles that are applicable during GDA. These are;

Engineering principles: maintenance, inspection and testing	Identification of requirements	EMT.1
Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.		

Engineering principles: maintenance, inspection and testing	Frequency	EMT.2
Structures, systems and components should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.		

Engineering principles: maintenance, inspection and testing	Procedures	EMT.5
Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.		

Engineering principles: maintenance, inspection and testing	Reliability claims	EMT.6
Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item.		

Engineering principles: maintenance, inspection and testing	Functional testing	EMT.7
In-service functional testing of structures, systems and components should prove the complete system and the safety function of each functional group.		

Within the UK there are a number of different methods, depending on the the NPP design, to provide at power testing and maintenance facilities. These methods have been subject to assessment by ONR and are considered to be adequate. During Step 3 of GDA ONR presented to Hitachi-GE and the prospective licensee of the UK ABWR the approach to testing carried out in the UK using Sizewell B NPP as an example. ONR considers the testing method presented as one approach which has meet regulatory expectation. During the presentation ONR stated that the method applied at Sizewell B was not a regulatory expectation for the UK ABWR design and that Hitachi-GE should provide a safety case for testing and maintenance of the UK ABWR.

This RO is therefore focused on ONR obtaining a clear understanding of the methodology for testing and maintenance of safety systems, particularly with the NPP at power, Hitachi-GE propose for the UK ABWR.

The submissions received to date do not provide adequate substantiation of testing and maintenance of safety systems.

The key products of this RO will be:

1. An explanation and justifcation of the underpinning rationale for testing and maintenance of safety systems. This should include the identification of any vulnerabilities introduced by testing and maintenance activities, time at risk arguments and how unplanned maintenance is accounted for in the safety case.
2. A list of mechnical process equipment that is specifically installed to enable on-line/at-power testing to be carried out. This list should clearly identify the safety classification of each piece of equipment. Where the safety classification does not align with the safety function classification the specifically installed equipment is supporting a justifcation should be provided. In addition failure modes associated with the equipment and processes supporting testing and maintenance which could override safety functions should be identified. An explanation should be provided of how these potential failures will be captured in the probabalistic safety analysis (PSA) and where relevant the deterministic fault studies analyses.
3. An explanation and justification of the coverage of the tests carried out. Where "overlapping" testing is applied (e.g. testing of detection instrumentation at a different frequency than the logic solving and fault terminating equipment) to make an overall safety justifcation then this is captured in the PSA and explicitly explained in the PSA documentation. The explanation should include a justification of the

coverage of the tests which should clearly identify what failure mode is being tested and how.

4. A justification for the frequency of testing. This should demonstrated that any assumptions are linked to the Probabalistic Safety Assessment.
5. Explanation and justification of the claim (made during C & I Technical Workshops) that the safety systems under test which are not in maintenance can respond to a demand placed upon them. This should include a justification of the transition from test mode to operating mode for the Safety System Logic and Control system and should clearly explain and justify how testing impacts on the availability of the systems assumed in the PSA. This should include the failure of any test and maintenance override being returned to the service position.

All of the above points should take into account any changes that have been made to the UK ABWR safety case and design in particular the changes in the design of SSLC HMI and the delivery of the Surveillance Test Prompt functionality.

An important outcome of this RO will be the agreement with ONR that the methodology for testing and maintenance of safety systems is considered holistically by all disciplines and that the safety case supports the overall safety claims on the UK ABWR design. In addition, that assumptions made in individual discipline areas are captured by other disciplines in particular the coverage and frequencies of testing are included in the probabilistic safety analysis. Other ONR Specialist Assessors will also take into consideration Hitachi-GE's response to this RO.

As the testing and maintenance of safety systems has a major impact on the overall through-life operation of any NPP ONR would expect to see Hitachi-GE have clearly set out the operational requirements of the UK ABWR to the prospective licensee.

This Regulatory Observation is linked to the RO on Safety System Logic & Control (SSLC) Class 1 HMI (RO-ABWR-0032)

Regulatory Observation Actions

RO-ABWR-0062.A1

Hitachi-GE are to develop suitable documentation that describes and substantiates the methodology to testing and maintenance of safety systems. It is expected that the documentation will follow the claims, arguments and evidence approach and this will include the identification and justification of the cases where the system / part system under test can re-aligne itself in response to a demand during testing.

Resolution required by:- December 2015

RO-ABWR-0062.A2

Hitachi-GE should confirm to ONR that the proposed methodology for testing and maintenance of safety systems has been included in the safety case for all related topic areas; e.g. mechanical and electrical engineering, and that it has been correctly accounted for (modelled in) the PSA and related fault studies.

Resolution required by:- January 2017

RO-ABWR-0062.A3

Hitachi-GE should confirm that the methodology for testing and maintenance has been clearly communicated to the prospective licensee of the UK ABWR.

Resolution required by:- February 2016

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	