REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0069
Date sent:	24th June 2016
Acknowledgement required by:	15th July 2016
Agreement of Resolution Plan Required by:	*To be determined by Hitachi-GE resolution plan*
Resolution of Regulatory Observation required by:	*To be determined by Hitachi-GE resolution plan*
TRIM Ref.:	2016/254208
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	HMI: Strategy, Application and Cognitive Issues
Technical area(s) 4. PSA 5. Fault Studies 6. Control & Instrumentation 13. Human Factors	**Related technical area(s)** 17. Security 18. Severe Accident Analysis

Regulatory Observation

Summary

ONR Safety Assessment Principle (SAP) EHF.3 directs an assessment of whether human actions that can affect safety have been identified. In addition, SAP EHF.5 sets out an expectation for the proportionate analysis of tasks contributing positively or negatively to the fulfilment of safety functions. SAPs ESR.1 and EHF.7 direct the assessment of whether such HMIs are ‘suitable and sufficient’. Taken together, these SAPs provide principled criteria for ONR inspectors to assess the suitability and sufficiency of user interfaces to support the users’ tasks that may be required to support safety.

It is a fundamental functional requirement that those personnel in nuclear power plant control rooms, who are responsible for controlling and monitoring that nuclear plant, should have the necessary information to do so available to them through human-machine interfaces (HMIs). Because operators base their understanding and the majority of their decisions on this information, it must be reliably understood if they are to maintain their situation awareness of the plant state and suitably intervene where necessary. In part, this understanding is assured in design by developing user interfaces on HMIs that are clear in the design of their content and match user’s’ expectations in the methods used for presenting and coding the required information. ONR is generally satisfied that the Hitachi-GE application of human factors (HF) engineering specifications to deliver clear layouts and information coding meets recognised good practice in alignment with the principles of EHF.7. However, such HF engineering specifications do not, by themselves, assure the required understanding and situation awareness. Therefore, ONR is also pleased that Hitachi-GE intend, as a part of verification and validation, to undertake analysis of usability via trials of user interface designs that result from the application of the HF Engineering Specification, in alignment with EHF.5. Nevertheless, the use of such interfaces can be vulnerable to causes of cognitive errors that can compromise the desired levels of understanding and situation awareness that are not easily addressed by the application of engineering specifications. Our concern is focused on the extent to which these other causes are being addressed by the Hitachi-GE design within the HF assessment processes that we know about.

From the commencement of GDA Step 4, ONR HF, C&I and PSA inspectors have sought to assess HMI design methods, by means of documentation and discussions with Hitachi-GE. However, Hitachi-GE has not yet delivered sufficient information to date to provide regulatory confidence that Hitachi-GE’s design strategies, design analytical processes and acceptance criteria for HMIs, will be sufficient to demonstrate in Step 4 that for all operator interactions with the different user interfaces available in the MCR and elsewhere, the sources for potential cognitive unreliability or avoidable cognitive workload will be controlled by user interface designs, so that risks are as low as reasonably practicable (ALARP). Overall therefore on the evidence seen to date, we consider that Hitachi-GE HF Engineering Guidelines, integrated programme of HF design support and analysis activities, and the currently proposed HF assessment trials during the interface verification and validation phase are unlikely to ensure that the ALARP principle is met. In particular, we would wish to see HF analysis during the HF design input phase to HMI, especially where human-computer interaction (HCI) occurs. This would provide early awareness of any potential workload or cognition issues. Accordingly, ONR considers that the issues described under the headings given below also need to be addressed. However, it should be noted that at the present time ONR has no evidence to suggest that the operational characteristics of the UK ABWR plant are complex relative to other designs of nuclear power plant. Therefore, the scope of this RO is confined strictly to our concerns about the use of HMIs and any potential they might have, when being used, to induce cognitive workload or cognitive error that can be avoided by HMI or HCI design.

Strategy for Use of User Interfaces after an Initiating Event.
ONR expect there to be a clearly designed strategy in place for operators to effectively use multiple HMIs in the Main Control Room. We consider this necessary so that operators refer to the most reliable available interface to obtain necessary data and to manage contingent failures of one or more of those HMIs.

ONR has been unable to find a clear description of the design intent for the use of the different HMIs, alone or in combination, in the Main Control Room (MCR) to address plant failures or failures of any particular HMI system. We have looked in:

i. Basis of Safety Cases on Overall Human-machine Interfaces , GA91-9201-0002-00109

ii. Basis of Safety Cases on Main Control Room Human-machine Interface GA91-9201-0002-00060

iii. Functionality of Class 1 HMI for the SSLC GA91-9201-0003-00577

iv. Human Factors Concept of Operations GA91-9201-0001-00034

v. Allocation of Function Report GA91-9201-0001-00040

vi. Human Reliability Analysis Report GA91-9201-0001-00041

vii. Baseline Human factors Assessment report GA91-9201-0001-00032

By completion of Step 4, ONR would expect to see a clear demonstration that the chosen Hitachi-GE strategy for HMI use would be effective in practice. This would support a demonstration that the levels of human reliability required by the safety case in following that strategy are likely to be achieved in practice. We would expect that the analysis, undertaken during the HF design input phase, which would lead to such a demonstration could impact upon the design of HMIs to achieve the best practicable usability. We would also expect reference to this analysis to be included in the Human Based Safety Claims that support the safety case. To make such a demonstration in accordance with the SAPs we would expect to see:

a) A clear design concept for the use of each independent user interface which states: its functional purpose, the types of actions to be undertaken at that interface and the levels of human reliability needed to meet the safety functional categorisation and safety system classification of that interface.

b) A demonstration that the failures of each user interface will be made very obvious to users and reliably recognised, so that HMI users will reliably move to alternative HMIs as defined by the strategy.

c) A demonstration that sequences of tasks needed to address scenarios of significance to nuclear safety can be undertaken without undue task sequence interruption being caused by moving to a different physical interface location.

d) A demonstration that alternative HMIs will provide information that is sufficient in functional terms for the tasks required to control or mitigate plant faults.

e) A demonstration that the alternative HMIs defined by the strategy for HMI use will provide information designed in such a way that it minimises the risk of cognitive error occurring.

MCR Operator Distraction and Workload
Our concern about distraction and workload centres on the psychological corollaries of both the requirement to undertake the testing of protection and standby safety systems via the Class 1 interface and by the currently prescribed Japanese frequency of test. Therefore, we are pleased to note that Hitachi-GE is undertaking a

study to establish a reliability-based inter-test interval which we would expect could reduce the currently prescribed frequency. However, we are concerned by the potential for distraction by such testing which we understand is intended to be undertaken by MCR-based, or possibly other personnel brought into the MCR (Although we do note that Hitachi-GE have clearly stated that the UK ABWR Concept of Operations does not include such extra personnel within the MCR as this is contrary to current UK control room Conduct of Operations). It is well-established, by psychological experiment, that logical reasoning involves sub-vocalisation and that this can be interfered with by other speech that can be heard by the thinker –particularly if that other speech contains similar content or meaning. Therefore, we expect that the potential for the disruption of thought processes by verbal technical discussions by others in proximity to MCR operators (if there are to be any) should be demonstrated to be minimised by design and tolerable or eliminated.

We are also concerned that a requirement upon MCR personnel to undertake these secondary testing tasks on the Class 1 interface could distract the attention by operators from their primary task of monitoring the continuing plant state and nuclear safety. Therefore, we would expect that any requirement to undertake secondary tasks should be demonstrated to be tolerable in two ways. First, in terms of the resulting cognitive workload and re-direction of attention away from the primary task; and secondly by the ability, through interface design and automation, to rapidly revert to the primary task because such secondary tasks as may be required can be rapidly closed out and made safe.

We recognise that some aspects of task design such as operational role assignment lie within the remit of the operating organisation and are therefore out of scope for GDA. However, we have some expectations for those aspects of task design which are influenced by systems and user interface design. The design should support assumed tasks such that the design seeks both to optimise cognitive workload, reduce the risk of distraction and ensure that MCR-based tasks fall within the competence of MCR personnel. These expectations are:

a) Wherever possible, tasks are done elsewhere which are not an integral part of monitoring the reactor and balance of plant for changes in phenomena that do affect, or could affect reactor safety.

b) MCR operators should not be responsible for logging and managing the rectification of network, instrumentation and other C&I faults. Neither should they be involved in the identification, procurement and setting to work of maintenance personnel to address such faults. (However, it is important to note that where the impact of such faults affects the validity of information that is relevant to MCR roles then this effect on indication validity should be made clear at that indication in the MCR and at other centralised locations.)

c) In all cases, tasks assigned to MCR staff should be those in which they are competent and relevant to their overall understanding of plant conditions in relation to nuclear safety. Accordingly, in operation, we would expect that any tasks assigned to MCR staff, additional to plant monitoring and control, should be prioritised and in accordance with their potential beneficial influence on nuclear safety. Therefore, we would expect that, in the MCR, the design of user interface systems at the GDA stage should not impose any requirements to undertake tasks that would be contrary either to those priorities or the possible staffing methods that will be established before operation to meet them.

Cognition Demands Stemming from User Interfaces

ONR are pleased to note that a process for alarm population definition and design of dynamic alarm management during an event is being undertaken by Hitachi-GE to minimise the display of unnecessary alarms. This should assist in reducing cognitive workload in respect of alarm handling. However, ONR require a clear demonstration that user understanding of a situation seen via alarms is maximised because unnecessary alarms have been eliminated in those scenarios of significance to nuclear safety. Therefore, we are concerned that we have not seen information about the Hitachi-GE proposed design assessment processes intended to ensure that cognitive workload engendered by interacting with other HMI is minimised.

Minimisation of cognitive workload, or cognitive burden, induced by an HMI is important to ensure that operators are able to concentrate on assimilating the presented data and hence understand the plant state and maintain situation awareness. This is of particular concern for HCI. Whilst HCI may present information more elegantly than previous generations of user interface, it is acknowledged in some HCI literature that the design of such interfaces requires reference to theories and principles in cognitive science and cognitive psychology to ensure interface usability and error-minimised operation. Therefore, careful task and interface assessment attention is needed to identify potential sources of cognitive workload induced by HCI design and to establish any risks to task performance that could be engendered by them.

We would expect a demonstration of cognitive workload minimisation in an HCI to rely on HCI trials that specifically attend to cognitive elements and consider the following:

a. Observation methods and measurements that address the concept of cognitive workload induced by HCI; measures include, for example, attention to ease of use and interface transparency. These measures would be obtained by observational measures of behaviour that may be symptomatic uncertainty or other cognitive challenges for users and by debriefing methods that explore trial subject experiences of cognitive challenge.

b. The success of such HF assessment critically relies upon the chosen methods, a belief by observers that such phenomena can occur and the skills to observe them or retrospectively elicit them from trial subjects when they do occur.

Regulatory Observation Actions

RO-ABWR-0069 . A1

*Hitachi-GE is asked to consider the matters identified in this RO and provide a Resolution plan by ****Date to be specified*****

Where Hitachi-GE plan that required submissions will be provided within documentation that ONR already expects to receive as part of the Step 4 submissions process, then that documentation and the time of its delivery should be explicitly identified in the Resolution Plan.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A2

Hitachi-GE is expected to provide an adequate documented explanation and justification of the strategy to be employed in managing interface systems that can impact upon operations undertaken by MCR staff and, as necessary, other staff in post fault operation. This justification should address the concerns expressed under the corresponding heading "Strategy for Use of User Interfaces after an Initiating Event" of this RO.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A3

In addition to Action # 2, Hitachi-GE should provide a submission which sets out which interface systems are the basis for claims upon human reliability made within the PSA. If such claims require the operator to abandon a faulted interface on a claimed system in order to use an interface on another claimed system, then the human reliability of fault detection and transfer needs to be qualitatively demonstrated and any quantification of such claims clearly justified. The documentation should also explain the role of the Class 1 and any other back-up HMI(s), if any, in that strategy.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A4

Hitachi-GE should undertake and report on a study that establishes predicted levels of cognitive workload and distraction for MCR operators and supervisor based upon the design proposals current at the time of writing this RO (April 2016). This should be based on a clearly stated method agreed with ONR. Specifically, this should examine the cognitive workload and distraction during routine operations and during post initiating event operations to the extent practicable at GDA.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A5

Hitachi-GE should confirm that information on abnormal equipment status that does not fall within the assumed UK ABWR MCR operator's competence or responsibility will be directed to another location. Such confirmation should include justification that any equipment status information that is directed to the MCR operator is suitable and relevant for them to receive.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A6

Hitachi-GE should provide a submission, which explains what processes they will use to ensure that cognitive performance, and challenges to it engendered by HMI design (particularly HCI), will be reliably identified and addressed to ensure ALARP solutions are implemented in user interface design.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A7

Hitachi –GE should provide a submission explaining what steps they will take to ensure that both identified and reasonably foreseeable cognitive errors that may be induced by HMI design will be correctly evaluated for human reliability and incorporated in the PSA models.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

RO-ABWR-0069. A8

For those plant processes and systems affecting nuclear safety, Hitachi-GE should provide a submission which details their methods for determining:
a) The alarm population of relevance to nuclear safety to be presented within the MCR;
b) The dynamic and administrative management processes that reduce the number of alarms presented to MCR personnel.
Hitachi-GE should also illustrate the effectiveness of their method for assessing alarms in reducing the cognitive burden to ALARP for MCR personnel during fault scenarios.

Resolution required by: ***To be determibed by the Hitachi-GE Resolution Plan***

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	