REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0007
Date sent:	5th June 2014
Acknowledgement required by:	26th June 2014
Agreement of Resolution Plan Required by:	3rd July 2014
Resolution of Regulatory Observation required by:	*To be determined by the Hitachi-GE Resolution Plan*
TRIM Ref.:	2014/138778
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	Spurious C&I failures as design basis initiating events
Technical area(s) Fault Studies	**Related technical area(s)** C&I

Regulatory Observation

Summary

Modern nuclear power plant (NPP) control and instrumentation (C&I) systems such as those proposed for the UK Advanced Boiling Water Reactor (ABWR) are complex and have a large number of outputs controlling a wide range of both safety and non-safety functions. ONR has requested Hitachi-GE undertake wide ranging analyses of spurious failures in its proposed C&I systems for the UK ABWR to ensure that such failures are either bounded by existing design basis analyses or, if not, to propose design changes to keep the faults within the design basis acceptance criteria.

Background

Traditionally, design basis analyses consider major single failure events or single system common cause failure events together with consequential damage. Even in probabilistic safety analyses (and closely allied beyond design basis and severe accident analyses), once the accident sequence involves four or five independent failures, the predicted frequencies become so low that analysis of the failure scenario is screened out from further consideration. However, the large computer based control and instrumentation (C&I) systems proposed for modern nuclear power plants (NPPs) have the potential to cause complex failure modes through the very large number of spurious failure states which could seriously challenge the three main safety functions of criticality, cooling and confinement. Crucially, multiple failures within the computer based C&I systems are not necessarily independent and therefore cannot be screened out on frequency grounds.

It is therefore relevant good practice in the UK to consider the failure of both plant control systems and safety protection systems within the design basis.

It is ONR's view that the failure of a Class 2 or Class 3 plant control system is a frequent fault (i.e. $>10^{-3}$ /yr). A common cause failure of Class 1 protection systems is considered an infrequent fault (i.e. $>10^{-5}$ /yr). The bases for these event frequencies are derived from ONR's technical assessment guide on Safety Systems, T/AST/003 Issue 6 (http://www.onr.org.uk/operational/tech_asst_guides/tast003.pdf).

System Class	Failure Frequency/yr (*ff*)
Class 1	10^{-3}/yr ≥ *ff* ≥ 10^{-5}/y
Class 2	10^{-2}/yr ≥ *ff* > 10^{-3}/y
Class 3	10^{-1}/yr ≥ *ff* > 10^{-2}/y

In some cases, erroneous signals from the control system or spurious actuation of a safety system via the UK ABWR's safety system and logic controller (SSLC) may have benign consequences. In other instances, the fault sequence may already be bounded by a "traditional" design basis fault or adequately protected by the existing design basis safety measures. However, this needs to be demonstrated, potentially with additional transient analysis. Work already identified by Hitachi-GE to show diverse protection for frequent faults could provide the necessary demonstration of adequacy.

In other cases, major spurious C&I functional failures could result in new events and challenging fault sequences which may require new claims within the design basis safety case on defence-in-depth systems. There could also be a requirement for design changes or additional engineered provision to be provided. The need for any such changes needs to be established through a systematic review.

It is recognised that modern control systems for NPP have a large number of outputs with systems of 200 or more outputs controlling a wide range of diesels, pumps, valves, dampers, control rods and also alarms for action by the operators. For example a system with 100 outputs with the simplifying assumption that they are also simple two state functions will have approximately $1x10^{30}$ combinations of output states. The reality is that many of the controls will not be the simple 'on' or 'off' type but more complex making the possible arrangements of outputs states even larger.

To avoid the impossible requirement for a reactor designer to analyse the combinatorial explosion of output states for even moderately large control systems, ONR seeks demonstrably pessimistic spurious failure analyses of all major C&I systems to demonstrate the robustness of the engineering within the design basis. The basis of the approach is to group the large number of outputs into functional groups and then to undertake a very pessimistic analysis of a much smaller number of possible failed states.

It is expected that the analyses will assume that all redundant divisions and all redundant arrangements within a division of equipment are simultaneously affected.

Any claims on operators to diagnose and isolate a spurious failure should not be credited before 30 minutes have elapsed and appropriate human factors justifications given.

No claims should be made on the other protective functions in the control or protection system containing the failure. For example, an event initiated in the SSLC would mean that it should be considered unavailable to protect against the resulting fault sequence (i.e. both RPS and ECCS/ESF functionality should be assumed to be lost).

The response to Regulatory Observation should be provided in a number of topic reports or similar documents, with a view to being incorporated into the PCSR at an appropriate time. The fault schedule will need to be revised to include any new initiating events. Any new claims or requirements on systems will need to be cascaded through to other parts of the safety case (notably C&I sections). The safety classification of the systems providing protection against the considered C&I failures needs to be clearly identified.

Regulatory Observation Actions

RO-ABWR-0007.A1: Identification of the major output functions in the UK ABWR control and protection systems

Hitachi-GE is required to identify the major output functions for the control and protection systems proposed for the UK ABWR. Amongst the systems considered are expected to be the Class 1 SSLC (including the neutron monitoring system), the Class 2 hardwired protection system (including the alternative rod insertion system), the Class 2 plant control system and the Class 3 auxiliary control system.

Resolution required by: To be determined by the Hitachi-GE Resolution Plan

RO-ABWR-0007.A2: Demonstration of protection against a failure in the Class 1 SSLC

Hitachi-GE is required to demonstrate that the UK ABWR can be brought to a sustainable safe state following a spurious failure in the Class 1 SSLC. Amongst the failures considered are expected to be:

- A spurious reactor trip initiated in the SSLC, with the SSLC assumed not to be available following the spurious initiation.
- A spurious containment isolation initiated in the SSLC, with the SSLC assumed not to be available following the spurious initiation.
- A spurious actuation of a safety system initiated by the Emergency Core Cooling System / Engineered Safety Features (ECCS/ESF) (e.g. LPFL, ADS, HPCF, RCIC), with the SSLC assumed not to be available following the spurious initiation.
- Any frequent design basis initiating event and the correct performance of the Reactor Protection System, but where the ECCS/ESF fails to function or initiates an inappropriate response.

The work in response to Action 1 may identify additional major functional failures to consider. Pre-existing transient analysis may provide the necessary demonstrations or new analysis may be required. The appropriate deterministic rules and acceptance criteria should be assumed.

Resolution required by: To be determined by the Hitachi-GE Resolution Plan

RO-ABWR-0007.A3: Demonstration of protection against a failure in the Class 2 hardwired protection system

Hitachi-GE is required to demonstrate that the UK ABWR can be brought to a sustainable safe state following a spurious failure in the Class 2 hardwired protection system.

The work in response to Actions 1 and 2 may demonstrate that there are no additional failures in the Class 2 hardwired protection system which are not effectively bounded by the analyses of failures in the SSLC. However, this needs to be systematically reported.

Resolution required by: To be determined by the Hitachi-GE Resolution Plan

RO-ABWR-0007.A4: Demonstration of protection against a spurious control system failure

Hitachi-GE is required to demonstrate that the UK ABWR can be brought to a sustainable safe state following a major functional failure in the Class 2 and Class 3 control systems. The failures to consider will have been identified through Action 1 but it is expected failures in the Rod Control & Information System, Recirculation Flow Control System, Feedwater Flow Control System, and the Turbine Control System are likely to be amongst those considered. Such failures should be considered frequent faults and therefore a main and a diverse means of protection should be demonstrated.

Resolution required by: To be determined by the Hitachi-GE Resolution Plan

REQUESTING PARTY TO COMPLETE	
Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	