REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0053
Date sent:	7th May 2015
Acknowledgement required by:	29th May 2015
Agreement of Resolution Plan Required by:	11th June 2015
Resolution of Regulatory Observation required by:	*To be determined by the Hitachi-GE Resolution Plan*
TRIM Ref.:	2015/155573
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	UK ABWR Probabilistic Safety Analysis (PSA) – level 1 and level 2 PSA for internal events during operation at power - System Analyses
Technical area(s) 4. PSA	**Related technical area(s)** 5. Fault Studies 6. Control & Instrumentation 7. Electrical Power Supply 11. Mechanical Engineering 13. Human Factors

Regulatory Observation

Summary

During Step 3 of GDA, ONR has undertaken an assessment of the methodologies used by Hitachi-GE for the UK ABWR Probabilistic Safety Analysis (PSA) system analyses. This assessment has identified areas that need enhancement to meet regulatory expectations and international good practice. The main objective of this Regulatory Observation (RO) is to state ONR's expectations related to the system analyses for the UK ABWR PSA (for internal initiating events during operation at power) and request Hitachi-GE to address the shortfalls identified by ONR's review.

Background and Regulatory Expectations

ONR's assessment of the UK ABWR PSA system analyses (Ref.1) performed during Step 3 of GDA has mainly addressed analysis methods and scope. The aim of this review was to ascertain whether Hitachi-GE's approach to the systems analyses and documentation are appropriate to support the objectives of the UK ABWR PSA and meet ONR's expectations laid-out in the PSA Technical Assessment Guide (TAG).

It can be noted that the UK ABWR PSA system analyses provides many of the key elements needed for a comprehensive modern standards PSA. ONR's assessment has identified areas that need enhancement to meet regulatory expectations and international good practice. A high level summary of some of the review findings has been provided below. More information is provided in Ref. 2.

<u>Scope and Completeness of the Systems Analyses:</u>

- The system descriptions and fault tree models do not provide a characterisation of the systems, structures and components (SSCs) operation during accident conditions (e.g. accident conditions may introduce system trips or failures during the course of an accident). For example, Ref.2 provides examples that could impact the modelling of the safety relief valves (SRVs) and reactor core isolation cooling system (RCIC) in the PSA. In addition, equipment survivability under adverse environment is not discussed in the system description nor is it modelled in the PSA fault trees.
- The system boundary diagrams are generally adequate; however, in some cases system connections or components included in the diagrams are not part of the system model. For example, the swing battery chargers in the direct current system (DC) are not modelled but appear in the system diagram.

Further information is required to clarify whether: (1) if the system boundary diagrams should be edited to clarify what is in the "system boundary"; or, (2) if the model needs to be expanded to encompass additional components or interfaces. ONR expectation is that the system boundary for the PSA model should be derived appropriately and clearly defined in the system diagrams within the PSA system analyses. The PSA model should be extended to include all the relevant components and systems connections. When justified, components in the diagram that are not explicitly modelled should be documented.

- The current listing of human error probabilities (HEPs) appears to be limited especially for the pre-initiators HEPs (e.g. miscalibration and misalignments, including those that could be common to multiple trains). The review in Ref. 2 has identified some examples of potentially missing HEPs (post-initiator and pre-initiator HEPs).
- The review in Ref. 2 has identified missing inter and intra system common cause failure (CCF), structural failures, failure modes and functions. For example the UK ABWR PSA does not include explicit modelling of the vapour suppression system functions or the high pressure nitrogen gas supply system (HPIN) that are potentially very important for the ABWR. It is ONR expectation that the UK ABWR PSA will be reviewed to address these omissions.
- The review in Ref. 2 has identified dependencies missing with no apparent justification (e.g. potential dependencies between the RCIC successful operation for 24h and suppression pool cooling conditions do not appear to be modelled in the PSA).
- One of the ABWR PSA Step 2 safety claims is the commitment to use the PSA to support the design development during GDA, which is in line with ONR expectations. Decisions made as part of the PSA modelling affect how the PSA may be effectively used for this purpose. For example, the more systems not modelled and the more conservative biases introduced, the less effective the PSA becomes as a tool to identify the benefits associated with plant or procedural changes that could reduce risk. The review in Ref. 2 has identified examples of systems that have been omitted from the PSA without a robust justification.
- The modelling of the containment isolation failure in the Level 2 PSA does not fully address CCF and latent failures modes.

<u>System Analyses Methodologies:</u>

- The review has found a lack of clarity and justification regarding the characterisation of the digital control and instrumentation (C&I) failure modes, CCFs, human interface failures, software failure, reliability data, etc.
- The PSA does not include support system initiator fault trees e.g., loss of service water, loss of turbine building service water system (TSW), loss of circulating water, loss of reactor building service water system (RSW), loss of intake, etc. ONR expectation is that the supporting initiators would be included in the PSA using a fault tree model to derive the initiating event frequency and the subsequent dependency on its failures in line with international good practice. In addition, CCF of separate trains of the same support systems should be modelled as separate initiating events (RO-ABWR-0042).
- The review has identified that some of the "latent" failure modes probabilities in the PSA are calculated assuming a 24 hours mission time duration instead of considering the standby exposure period (e.g. test period). Further information is provided in Ref.2. ONR expectation is that the PSA is reviewed to correct the modelling as necessary.
- Certain pumps or trains of standby systems are always assumed in operation. This creates an asymmetry in the calculated importance measures. It is ONR expectation that the PSA mode does not have asymmetries artificially built in. This is important to ensure the suitability of the PSA to support a number of applications such as risk monitoring (during operational stages) and those applications based on evaluation of the results of importance analysis (during GDA and beyond GDA).

<u>System Analyses Documentation:</u>

- The review has found that the impact of an initiating event on the system is not explicitly discussed as part of the system analysis. It is acknowledged that there are other resources provided as part of the PSA documentation that attempt to capture some of these effects. Nevertheless, it is appropriate that the system analyses explicitly cite those principal effects caused by initiators as they affect the system

availability.

- Hitachi-GE has provided elements of the dependency analysis in a number of diverse locations. ONR considers that a single location that addresses all of the dependencies could be extremely useful to the PSA team, reviewers, and as a communication tool.
- The review has found that the documentation regarding the use of house events, flags, and mutually exclusive files (MEX) is not available and should be provided (e.g. including the objectives satisfied by each of these modelling tools).
- A clear documentation of recovery actions credited in the PSA model is not available.

References:

1. System Analysis for Internal Event Level 1 PSA at Power, GA91-9201-0003-00183, Rev. 3.
2. Topical Report on UK ABWR GDA System Analysis (internal Events At-Power), ABWR-02-STEP3, April 2015.

Regulatory Observation Actions

RO-ABWR-0053.A1: Hitachi-GE is requested to revise and improve the completeness and scope of the systems analyses that support the UK ABWR level 1 and level 2 PSA model for internal initiating events at power, taking into consideration the following:

1. The UK ABWR PSA and documentation should reflect the system operation during accident conditions. Example of aspects that ONR considers should be explicit in the documentation and the PSA model are:
   - System operation modes and alignments;
   - Justification of any operator intervention given adverse environmental effects (if relevant);
   - Operability given the trip set-points limits;
   - Survivability of all system components;
   - Operability given adverse environmental effects impacting equipment survivability.
2. The UK ABWR PSA documentation should clearly identify all the relevant system components and system connections that are to be modelled. When relevant and justified, documentation of any component in the system diagrams that is not modelled and the reason why should be provided.
3. The UK ABWR PSA should include, with suitable justification, a complete list of pre-initiator HEPs and supporting analyses.
4. The UK ABWR PSA should include, with suitable justification, a complete list of inter and intra system CCF and supporting analyses. The documentation should also include a justification for the CCFs groups. When similar components of different systems are not included in the same CCF group a justification should be provided.
5. The UK ABWR PSA should include all relevant structural failures of components when subjected to unusual accident conditions and supporting analyses.
6. The UK ABWR PSA should include a complete and justified list of failure modes for each component.
7. The UK ABWR PSA should include a complete and justified list of system functions for each system.
8. The UK ABWR PSA should be reviewed to address the specific shortfalls identified in Ref.2 .
9. The UK ABWR PSA should explicitly include hardware failures that contribute to the human failure events.
10. The UK ABWR PSA should include additional systems needed to ensure that the PSA accurately reflects the UK ABWR risk profile, including HPIN system and other examples provided in Ref 2.
11. The UK ABWR PSA should include additional post-initiator errors (and adequate supporting analyses) to ensure that the PSA accurately reflects the UK ABWR risk profile.
12. Hitachi-GE should provide a description of how and for which sequences available portable equipment could be claimed in the PSA.

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

RO-ABWR-0053.A2: Hitachi-GE is requested to revise and improve the modelling and documentation of dependencies in the UK ABWR level 1 and level 2 PSA model for internal initiating events at power, taking into consideration the following:

1. The UK ABWR PSA model should include all reasonably foreseeable spatial, functional, support system, common cause and human dependencies. Example of dependencies that ONR considers should be considered in the UK ABWR PSA are provided in Ref.2

2. When room cooling and support systems dependencies are not included in the PSA, Hitachi-GE should provide analyses and justification to demonstrate that there are no dependencies.

3. The UK ABWR PSA documentation should clearly address all of the PSA dependencies in a single location.

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

RO-ABWR-0053.A3: Hitachi-GE is requested to revise and improve the C&I model and documentation in the UK ABWR level 1 and level 2 PSA model for internal initiating events at power, taking into consideration the following:

1. Hitachi-GE should provide a suitable justification for the C&I system boundaries and components modelled in the PSA.

2. Hitachi-GE should identify and justify the C&I failure modes considered in the PSA using a C&I failure mode and effect analyses (FMEA) or equivalent analyses. This should include but not be limited to the identification and justification of potential pressure and level instrumentation failures and CCFs, software failures, human interface failures, and CCFs.

3. Hitachi-GE should provide the technical basis for the C&I modelling assumptions including claims on any fault tolerant features of the C&I.

4. Hitachi-GE should provide the technical basis for the C&I data and associated uncertainty.

5. Hitachi-GE should provide an evaluation of the impact of C&I data uncertainties and modelling assumptions on the risk. Hitachi-GE should provide a plan to reduce these uncertainties and the effect on the PSA results of key assumptions, when further information on the design becomes available.

6. Hitachi-GE should revise the PSA model to explicitly model relevant indicators/alarms. Analyses should include an assessment of potential misleading indications resulting from the impact of fault and severe accident conditions on the instrumentation that, for example, could delay initiation of recovery or mitigation actions by the operator.

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

---

RO-ABWR-0053.A4: Hitachi-GE is requested to revise the UK ABWR level 1 PSA internal initiating events at power model, taking into consideration the following:

The UK ABWR PSA model and documentation should be revised to include fault trees of the support systems initiators.

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

RO-ABWR-0053.A5: Hitachi-GE is requested to revise and improve the modelling of latent failure

modes in the UK ABWR level 1 and level 2 PSA model for internal initiating events at power, taking into consideration the following:

Hitachi-GE should update the PSA model and documentation to model latent failure modes in line with relevant good practice. This should include both standby failure modes and pre-initiator (Type A) failure modes.

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

---

RO-ABWR-0053.A6: Hitachi-GE is requested to revise and improve the system analyses documentation for the UK ABWR level 1 and level 2 PSA model for internal initiating events at power, taking into consideration the following:

1. The documentation should address the shortfalls against ONR's expectations in the PSA TAG and international good practice identified in Ref.2
2. The documentation should be reviewed to explicitly include a suitable and sufficient discussion of the impact of each initiating event on the systems.
3. The documentation should be completed to include a suitable and sufficient description of use of house events, flags, and MEX files including the objectives satisfied by each of these modelling tools.
4. The documentation should be revised to ensure that the documentation of recovery actions credited in the PSA model is complete and clear.
5. Hitachi-GE should provide an explanation of how model asymmetries will be considered on the evaluation of the results of importance analysis and a commitment date to correct model asymmetries artificially built in the PSA.

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:	