REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0052
Date sent:	6th May 2015
Acknowledgement required by:	28th May 2015
Agreement of Resolution Plan Required by:	28th May 2015
Resolution of Regulatory Observation required by:	*to be determined by Hitachi-GE Resolution Plan*
TRIM Ref.:	2015/167963
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	Mechanical Engineering - Design Process - SSCs' Detailed Design
Technical area(s) 11. Mechanical Engineering	**Related technical area(s)** 12. Structural Integrity 7. Electrical Power Supply 6. Control & Instrumentation 15. Radwaste & Decommissioning

Regulatory Observation

Summary

This mechanical engineering regulatory observation is cross cutting. It is being raised to ensure the UK ABWR Structures, Systems and Components (SSCs) detailed designs reduce risks So Far Is Reasonably Practicable (SFAIRP) to secure an As Low As Reasonably Practicable (ALARP) design basis.

Assessment Observation

During the third Step 3 mechanical engineering technical workshop; Jan 2015; the Requesting Party (RP) explained that its design process arrangement does not require a hazard identification review (for example a Failure Mode Effects Analysis (FMEA)) to be undertaken for its mechanical engineering SSCs as part of its detailed design scope. The RP's design process arrangement is based on consideration of:

1) operational experience;
2) empirical testing; and
3) analytical methods.

I consider that:

1) an SSC supplier will develop the concept design and detailed design specifically to suit its manufacturing capability;
2) undertaking a hazard identification review of its SSC (for example a FMEA) as part of the detailed design phase:
   a) demonstrates the adoption of a robust design process;
   b) aids demonstration and consideration to the following:
      i) failure to safety (SAP EDR.1);
      ii) common cause failure (SAP EDR.3); and
      iii) single failure criterion (SAP EDR.4).
3) provides supporting arguments and the audit trail to the demonstration that a SSC design has been:
   a) adequately optioneered;
   b) hazards are understood; and
   c) risks have been reduced SFAIRP to secure an ALARP design.

I judge the following Safety Assessment Principles (SAPs) to be pertinent to this topic:

1) ECS.3 – Codes and standards - SSCs that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards;

2) EDR.1 – Failure to safety – due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate;

3) EDR.3 – Common cause failure - should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability; and

4) EDR.4 – Single failure criterion - during any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.

I consider this regulatory observation to be cross-cutting and of interest to:

1. Structural integrity;

2. Electrical;
3. Control and instrumentation; and
4. Decommissioning and radwaste.

To conclude, I consider the RP design process arrangement:

1) is not aligned with UK legislation or RGP;
2) it doesn't reduce the risks SFAIRP; thus doesn't secure an ALARP design basis; which is a requirement of UK legislation (Health & Safety at Work etc. Act 1974); and
3) does not enable a GDA to be concluded without this regulatory observation being adequately addressed in an auditable manner.

Regulatory Expectations

It is my regulatory expectation that the RP:

1) develops and implements a robust and auditable lifecycle design process arrangement to demonstrate each SSC important to safety:
   a) reduces its risks SFAIRP to secure an ALARP design basis;
   b) meets the expectations of the ONR's SAPs; and
   c) meets the expectations of UK relevant good practice.
2) generates an auditable trail to its safety claims, supporting arguments and design basis substantiation evidence.

Regulatory Observation Actions

RO-ABWR-0052.A1

Generate a resolution plan that will:

a) present its detailed strategy to demonstrate SSCs important to safety are aligned with UK legislation and are optioneered to be ALARP;
b) define and scope the planned activities;
c) include a controlled programme identifying: planned activities; deliverables; milestones; timescales and resource requirements; and
d) provide the audit trail to demonstrate each UK ABWR SSC hazards and risks have been reduced SFAIRP and demonstrate each SSC is ALARP.

Resolution required by: to be determined by Hitachi-GE Resolution Plan

---

RO-ABWR-0052.A2

Provide progress updates to ONR through the planned GDA engagements.

Resolution required by: to be determined by Hitachi-GE Resolution Plan

RO-ABWR-0052.A3

Make available to ONR, activity deliverables, conclusions and recommendations.

Resolution required by: to be determined by Hitachi-GE Resolution Plan

---

RO-ABWR-0052.A4

If appropriate:

a) raise design changes; and
b) update the UK ABWR safety case, system designs and substantiation.

Resolution required by: to be determined by Hitachi-GE Resolution Plan

---

RO-ABWR-0052.A5

Make available any appropriate updated documents and substantiation for ONR assessment.

Resolution required by: to be determined by Hitachi-GE Resolution Plan

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