REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0046
Revision:	1
Date sent:	19/05/20
Acknowledgement required by:	09/06/20
Agreement of Resolution Plan Required by:	31/08/20
CM9 Ref:	2020/103176
Related RQ / RO No. and CM9 Ref: (if any)**:**	See reference list.
Observation title:	Demonstration that the Risks to HIC Components from Internal Hazards are Reduced to ALARP
Lead technical topic: 12. Internal Hazards	**Related technical topic(s)** 2. Civil Engineering 8. External Hazards 9. Fault Studies 14. Mechanical Engineering 15. Probabilistic Safety Analysis 18. Security 20. Structural Integrity

Regulatory Observation

Background

It is ONRs expectation that a safety case demonstrates the SSCs with highest reliability claims are not challenged by internal hazards such that the estimated likelihood of gross failure is very low or the safety case claims of gross failure can be discounted (Ref. 1).

The UKHPR1000 pre-construction safety report (PCSR) (Ref.2) claims the highest integrity components (HIC) have appropriate withstands against internal hazards. During step 3 analyses were undertaken by the requesting party (RP) to identify those areas where HIC could be impacted by internal hazards (IH) to demonstrate that the claims made are appropriately substantiated.

From the assessment of supporting reports analysing internal hazard effects on HIC (Ref.3, 4, & 5), and subsequent RP engagements (Ref. 6, 7, 8 & 9), ONR has identified that currently there is insufficient detail to provide assurance that the risks to HIC components from IH are as low as is reasonably practicable (ALARP).

ONR sampling has identified shortfalls in the completeness of the safety case for HIC; in particular there is a lack of evidence to support the assumptions and claims used in the analysis, both in terms of the methods used and the level of conservatism applied. Additionally, where IH challenges have been identified it is unclear what analysis has been undertaken to review the design in order to optimise plant layout to eliminate the internal hazard challenge to the HICs.

Relevant Legislation, Standards and Guidance

ONRs expectation is that the RP demonstrates that the integrity of SSCs with highest reliability claims are not challenged by internal hazards (Ref.9).

Paragraph 290 of the SAPs (Ref.1) states that where

(a) a metal component or structure performs a principal role in ensuring nuclear safety; and

(b) the estimated likelihood of gross failure needs to be very low or the safety case claims gross failures can be discounted.

Then evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations identified in the safety case [EMC.3]. In addition, the safety case should provide a detailed design hazard loading specification covering normal operation, faults and accident conditions. This should include plant transients and internal and external hazards [SAPs Para 295].

It is ONRs expectation that in the first instance the design of the plant layout is optimised to eliminate or minimise the effects of internal hazards. Furthermore the design and layout should be such that the number of components with a highest integrity claim is minimised and the effect of faults and accidents are prevented. These expectations are captured generally in SAP ELO.4 which states:

The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised. For example, the design and layout should:

- Minimise the direct effects of initiating events, particularly from internal and external hazards, on structures, systems or components;
- Not compromise the safety of the site, or its facilities, structures, systems and components;
- Minimise any interactions between a failed structure, system or component and other structures, systems or components;
- Ensure that site personnel are physically protected from direct and indirect effects of faults; and
- Facilitate access for necessary recovery actions and re-supply of essential stocks, materials, equipment and personnel following an accident.

Where the layout cannot eliminate the internal hazards the next level is to provide adequate mitigation through segregation and/or protection from hazard initiators. The following ONR SAP is highlighted:

ESS.18, Failure independence, No design basis event should disable a safety system. Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.

The analysis of design basis events should assume the event occurs simultaneously with the facility's most adverse permitted operating state and determine the need for segregation, diversity and redundancy of plant and equipment and the location of barriers to limit this impact.

The following ONR SAPs and supporting paragraphs are also highlighted:

EDR.2, Redundancy, diversity and segregation, Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components. It should be demonstrated that the required level of reliability for their intended safety function has been achieved.

EHA.5, Design basis event operating states, Analysis of design basis events should assume the event occurs simultaneously with the facility's most adverse permitted operating state (see paragraph 631 c) and d)).

EHA.6, Analysis, The effects of internal and external hazards that could affect the safety of the facility should be analysed. The analysis should take into account hazard combinations, simultaneous effects, common cause failures, defence in depth and consequential effects.

Paragraph 243 - The analysis should apply an appropriate combination of engineering, deterministic and probabilistic methods in order to:

- Understand the behaviour of the facility in response to the hazard; and
- Confirm high confidence in the adequacy of the design basis definition and the associated fault tolerance of the facility.

Paragraph 244 - The analysis should include hazard analysis to:

a) identify the potential impact of the hazard on the facility's structures, systems and components, and in particular its safety systems;
b) determine the need for segregation, diversity and redundancy of plant and equipment and the location of barriers to limit this impact; and
c) determine the safety functions (eg the withstand capability) to be provided by such barriers.

Paragraph 245 - The analysis should take into account that:

a) certain internal or external hazards may not be independent of one other and may occur simultaneously or in combinations that are reasonable to expect;
b) the initiating hazard, or its effects may persist as the fault sequence progresses (see paragraph 631 a).
c) an internal or external hazard may occur simultaneously with a facility fault, or when plant is out for maintenance;
d) there is significant potential for internal or external hazards to act as initiators of common cause failures, including loss of off-site power and other services;
e) the most severe internal and external hazards have the potential to threaten more than one level of defence in depth (see Principle EKP.3) at once;
f) internal hazards (eg fire) can arise as a consequence of faults internal or external to the site; and
g) the severity of the consequences of internal and external hazards will often be affected by aspects such as facility layout, interactions between structures, systems and components, and building size and shape.

Ultimately the safety case should present a robust justification that the risks to highest integrity components from internal hazards are as low as is reasonably practicable (ALARP).

SC.4, Safety case characteristics, A safety case should be accurate, objective and demonstrably complete for its intended purpose. Further guidance (SAPs Para 100) states that a safety case should:

a) explicitly set out the argument for why risks are ALARP; and
b) link the information necessary to show that risks are ALARP, and what will be needed to ensure that this can be maintained over the period for which the safety case is valid;
c) support claims and arguments with appropriate evidence, and with experiment and/or analysis that validates performance assumptions;
d) accurately and realistically reflect the proposed activity, facility and its structures, systems and components;
e) identify all the limits and conditions necessary in the interests of safety (operating rules); and
f) identify any other requirements necessary to meet or maintain the safety case such as surveillance, maintenance and inspection.

Regulatory Expectations

To address the shortfalls identified and given the guidance detailed above, ONR expects the requesting party to review the plant layout of HICs and provide a robust demonstration that risks to HICs associated with internal hazards have been reduced ALARP.
Where necessary, this demonstration should include consideration of different design options to prevent, protect or mitigate the effects on HICs from IH.

ONR recognises that the assessment of HIC components is still underway in the structural integrity topic area. The response to this RO should therefore be informed by the progression of work undertaken within the RP's structural integrity specialism. In particular the work associated with the consequence assessment for HIC candidates and the work undertaken in response to RO-UKHPR1000-0008 action 3 (Ref. 10) should be used to inform the wider IH aspects to address this regulatory observation.

References

1. ONR Safety Assessment Principles For Nuclear Facilities, 2014 Edition, January 2020
2. CGN, Pre-Construction Safety Report, Chapter 19 Internal Hazards, Rev 001, HPR/GDA/PCSR/0019
3. GHX84200015DOZJ03GN - High Energy Pipe Failures Safety Assessment Report for Reactor Building (Based on Bounding Cases) - Rev A - 16 September 2019, File Ref: 2019/268510
4. GHX84200018DOZJ03GN - High Energy Pipe Failures Safety Assessment Report for Fuel Building (Based on Bounding Cases) - Rev B - 3 October 2019, File Ref: 2019/285922
5. RQ 509, Internal Hazard queries on high energy pipe failures (bounding cases) for the reactor & fuel buildings, File Ref: 2019/375195
6. ONR-NR-CR-19-464- Internal Hazards Interaction No.9 Level 4 meeting 16th January 2020, File Ref: 2020/29526
7. ONR-NR-CR-19-531 – Internal Hazards Interaction No.10 Level 4 meeting 28th February, File Ref: 2020/74080
8. CGN Presentation - Discussion of HIC Equipment Substantiation against Internal Hazard Loads, File Ref: 2020/17622
9. ONR presentation, HIC Component expectations, 10th March 2020, File Ref: 2020/77899
10. ONR, Regulatory Observation, Justification of the Structural Integrity Classification of the Main Coolant Loop, RO-UKHPR1000-0008, 20th Dec 2018, File Ref: 2018/409445

Regulatory Observation Actions

RO-UKHPR1000-0046.A1 – Demonstration of optimisation of plant layout in respect to HIC.

In response to this Regulatory Observation Action, the RP should:

- Where IH sources have been identified to impact HICs, undertake a review of the plant layout and demonstrate that the IH sources have been eliminated where possible.

RO-UKHPR1000-0046.A2 – Present the safety case to cover the consequences of internal hazards on HIC

For those IH that could not be eliminated through optimisation of plant layout, the RP should :

- **Derive the Hazard loading for all HIC components**: Provide a robust demonstration that the identification and quantification of all remaining IH sources (those that could not be eliminated) that impacting HIC has been undertaken:
    - Demonstration that a robust hazard analysis has been undertaken, including justification of screening of sources, application of assumptions, analysis methods and the incorporation of appropriate conservatism.
- **Present the HIC withstand criteria:** To enable adequate assessment of HIC given the IH loadings this should include**:**
    - A justification of the methodologies and standards from which the criteria are derived; and
    - A clear justification of why the withstand criteria for the HIC are conservative.
- **Present the golden thread** for the safety case (claims, arguments and evidence) for those HICs against which an IH withstand claim has been made. This should include:
    - A clear presentation of the requirements for the HICs and / or any additional protective measures;
    - Substantiation of the withstand capability of HIC, against IH loads, which may involve multi-discipline consideration; and
    - Substantiation of any other claims made - for example any additional protection measures identified.

RO-UKHPR1000-0046.A3 – Present ALARP justifcation

- Demonstrate that the risk to HIC components from IH is reduced ALARP taking into consideration the work undertaken under RO-UKHPR1000-0008 action 3.

Resolution required by '*to be determined by General Nuclear System Resolution Plan*'

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