REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0032
Revision:	0
Date sent:	25/02/2020
Acknowledgement required by:	17/03/2020
Agreement of Resolution Plan Required by:	17/03/2020
TRIM Ref:	2020/33470
Related RQ / RO No. and TRIM Ref: (if any)**:**	
Observation title:	Inadvertent Flooding of the Reactor Pit
Lead technical topic: 9. Fault Studies	**Related technical topic(s):** 3. Control & Instrumentation 11. Human Factors 14. Mechanical Engineering 15. Probabilistic Safety Analysis 19. Severe Accident Analysis 20. Structural Integrity

Regulatory Observation

Background

The UK HPR1000 employs an In-Vessel Melt Retention (IVMR) by Ex-Reactor Vessel Cooling (ERVC) severe accident mitigation strategy. In the unlikely event of a severe accident involving core melting, the reactor pit of the UK HPR1000 is designed to be flooded under gravity using the passive injection of water from a dedicated tank. This submerges the Reactor Pressure Vessel (RPV) with the objective of removing sufficient heat to maintain its integrity and contain the molten core debris. Longer term cooling is achieved by using Containment Heat Removal System (EHR [CHRS]) pumps to inject water from the In-containment Reactor Water Storage Tank (IRWST).

In the UK HPR1000 design the RPV is designated as a High Integrity Component (HIC) as the consequences of failure of this component are deemed intolerable. As part of the HIC claim the RP has chosen to pursue an avoidance of fracture demonstration that will claim that the likelihood of failure of this component is so low it can be discounted from the design basis. For these types of arguments ONR expects that the component be tolerant of defects. To achieve this, ONR expects that evidence is available to demonstrate the necessary level of integrity for the most demanding design basis situations identified. This includes a consideration of a detailed design loading specification covering both normal operations and fault and accident conditions (including internal and external hazards) within the design basis.

A failure of isolation of either the active or passive injection water sources has the potential for inadvertent flooding of the reactor pit. It is ONR's opinion that this flooding has the potential to induce a thermal shock on the RPV and hence challenge its structural integrity. Inadvertent flooding of the reactor pit is currently not considered in the UK HPR1000 design basis. Whilst thermal shock analysis has been performed for severe accidents [1], consequence analyses of inadvertent flooding as a design basis accident has not been provided to ONR.

ONR has raised a number of Regulatory Queries on this matter [2 to 6]. In response, the RP has credited failure probabilities of multiple low classification systems, structures and components (SSCs) in order to exclude inadvertent flooding from the design basis. In response to RQ-UKHPR1000-0410 [6], the RP stated that a common cause failure of valves should be considered and that "*the elimination of the CCF factor or other design improvement in passive injection line will be performed to make sure that risk of inadvertent reactor pit flooding is ALARP*."

In the absence of unmitigated consequence analyses, it is unclear whether the extant prevention, protection and mitigation measures are appropriately designed and classified. However, on the assumption that inadvertent flooding of the reactor pit results in RPV failure, ONR considers that this is not appropriate to assign multiple lower class components to fulfil such a safety function where the consequence of failure are high. In addition, ONR considers that the extant design may not fulfil the RP's design basis rules when considering spurious opening of valves (e.g. a design basis fault should be protected by a Class 1 safety system).

To date, the safety case submission made by the RP are incomplete and inconsistent regarding the risks posed by inadvertent flooding of the reactor pit. ONR considers that a systematic and holistic approach should be adopted to the development of a suitable and sufficient safety case for such events that considers the consequences of the reactor pit flooding during normal operations and the likelihood of such an event. This should ultimately demonstrate that the design the EHR (CHRS) is adequate to reduce risks to As Low As Reasonably Practicable (ALARP).

Relevant Legislation, Standards and Guidance

The ONR Safety Assessment Principles (SAPs) [7] expect that a safety case should be accurate, objective and demonstrably complete for its intended purpose. A safety case should set out the argument for why risks are ALARP, and to achieve this, a safety case should identify the facility's hazards by a thorough and systematic process. A number of the SAPs are relevant to this RO, including the SC (Safety cases) and FA (Fault Analysis) SAPs. Of particular note are SAPs EMC.3 and EMC.7 and associated paragraphs:

Engineering principles: integrity of metal components and structures: highest reliability components and structures	Evidence	EMC.3
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.		

Engineering principles: integrity of metal components and structures: design	Loadings	EMC.7
The schedule of design loadings (including combinations of loadings) for components and structures, together with conservative estimates of their frequency of occurrence should be used as the basis for design against normal operation, fault and accident conditions. This should include plant transients and tests together with internal and external hazards.		

Further information can be found in the associated Technical Assessment Guides (TAGs) [8].

In addition, relevant international guidance includes [9 to 11].

Regulatory Expectations

In resolution of this RO, ONR expects that the requesting party delivers a suitable and sufficient safety case to demonstrate that the risks associated with inadvertent flooding of the reactor pit during normal operations are reduced to ALARP.

It is important to note that the RP should choose its approach to making such a safety case, given there are different ways in which the objectives above can be achieved. The RP may wish to demonstrate that:

- the RPV can tolerate the consequences of the identified fault sequences to a high degree of confidence; or
- the RP may wish to demonstrate that the UK HPR1000 design is sufficient to prevent, protect against or mitigate fault sequences that can lead to challenging the integrity of the RPV; or
- a combination of the above arguments.

ONR considers that the following aspects should be considered by the RP in producing their safety case, as appropriate:

- Fault identification – the requesting party should systematically identify all Postulated Initiating Events (PIEs) related to inadvertent flooding of the reactor pit, including those from spurious C&I and common cause failures. The RP should apply its methodology for identification of PIEs and the bounding and grouping process as appropriate.
- Fault frequency – the fault frequency should be determined, and a justification for the frequency should be provided. The justification should not solely rely on the current PSA models.
- Assessment of consequences – consequential failure of the RPV and other equipment due to the initiating events identified should be considered. The level of detail required in the RPs assessment of consequential failure should depend on the approach to its safety case.
- Identification of protection, prevention and mitigation – all safety functions and the corresponding SSCs (including human actions) credited in the prevention, protection or mitigation of faults identified should be identified and appropriately categorised and classified, respectively, using the RP's design principles. This should not be limited to the extant design, but should consider any further safety functions required.
- Deterministic demonstration of fault tolerance – the relevant design basis fault sequences should be identified and it should be demonstrated that adequate prevention, protection and mitigation exists to prevent identified challenge to the integrity of the RPV. The assessment should consider the expectations of SAPs FA.6 and FA.7 as appropriate.
- Identification of further risk prevention, protection or mitigation – the RP should consider whether the identified risks have been reduced to ALARP. In doing so, the RP should consider independence of levels of defence in depth, and the balance of risk between levels of defence in depth, ensuring that one safety measure does not adversely affect the reliability of another to operate when required.
- Relevant updates to the PSA – The PSA should be updated to reflect the outcome of this work.The initiating event frequency for RPV rupture should include inadvertent reactor pit flooding if appropriate.
- Ultimately, ONR expects the RP to demonstrate that risks have been reduced to ALARP. This should be a multi-stranded argument including, as appropriate, deterministic and probabilistic arguments (FA.1).

References

[1] *The Thermal Shock Analysis of RPV While Triggering IVR Condition*, GHX00100011PLX44GN, Rev A, CGN, September 2019. CM9 Ref. 2019/281317
[2] Response to RQ-UKHPR1000-0168. CM9 Ref. 2019/57315
[3] Response to RQ-UKHPR1000-0224. CM9 Ref. 2019/100762
[4] Response to RQ-UKHPR1000-0232. CM9 Ref. 2019/149084
[5] Response to RQ-UKHPR1000-0307. CM9 Ref. 2019/215308
[6] Response to RQ-UKHPR1000-0410. CM9 Ref. 2019/245542
[7] Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1, Office for Nuclear Regulation, 2020. www.onr.org.uk/saps/saps2014.pdf
[8] Nuclear Safety Technical Assessment Guides. www.onr.org.uk/operational/tech_asst_guides/index.htm
[9] *Deterministic Safety Assessment for Nuclear Power Plants – Specific Safety Guide - SSG-2*, Revision 1, IAEA, 2009. www.iaea.org
[10] *Safety of new NPP designs*, WENRA, March 2013. www.wenra.org
[11] *Practical Elimination Applied to New NPP Designs – Key Elements and Expectations*, WENRA, September 2019. www.wenra.org

Regulatory Observation Actions

RO-UKHPR1000-0032.A1 – Demonstate that the risks associated with inadvertent reactor pit flooding during normal operations are reduced to ALARP

In response to this Regulatory Observation Action, GNS should:

- Provide a suitable and sufficient safety case related to inadvertant flooding of the reactor pit.

• In responding to this Action the RP should consider the expections and relevant guidance described in the RO, and ultimately provide a justification that the risks associated with inadvertent reactor pit flooding have been reduced to ALARP. **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:	