REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0023
Revision:	0
Date sent:	18/11/19
Acknowledgement required by:	09/12/19
Agreement of Resolution Plan Required by:	20/12/2019
TRIM Ref:	2019/297976
Related RQ / RO No. and TRIM Ref: (if any)**:**	RQ-UKHPR1000-0471
Observation title:	Demonstration of Diverse Protection for frequent faults
Lead technical topic: 9. Fault Studies	**Related technical topic(s):** 3. Control & Instrumentation 7. Electrical Engineering 10. Fuel & Core 11. Human Factors 14. Mechanical Engineering 15. Probabilistic Safety Analysis

Regulatory Observation

Background

The Requesting Party (RP) for the UK HPR1000 (General Nuclear Systems, GNS) has committed (Reference 1) to providing diverse safety systems for protection against frequent faults, consistent with UK good practice for a design basis safety case. The demonstration will be summarised within a fault schedule, an early version of which has been submitted to ONR (Reference 2).

As part of its design basis assessment, the RP has identified a number of Design Basis Conditions (DBCs) and categorised them according to their predicted frequency of occurrence. The RP has defined DBC-2 events as DBCs with a frequency greater than $1x10^{-2}$ per year. DBC-3 events are defined as DBCs with a frequency between $1x10^{-4}$ and $1x10^{-2}$ per year. Recognising the definition within ONR's SAPs, the RP has defined frequent faults as those with an initiating fault frequency exceeding $1x10^{-3}$ per year. Therefore the RP intends to demonstrate diversity in the delivery of safety functions for all DBC2 events and some DBC3 events.

GNS has to date submitted a number of documents to achieve this:

- A fault schedule which identifies candidate diverse lines of protection (Reference 2) for DBC-2 and DBC-3 faults;
- A report to identify most onerous fault sequences for demonstrating diverse protection (Reference 3);
- A report which summarises the transient analysis that has been conducted for these bounding cases (Reference 4) to validate the candidate diverse lines within the Fault Schedule.

However Reference 4 concludes that there are a number of areas for which further work is required to demonstrate diverse protection for some sequences. These areas are described in Reference 4 as:

a) Investigation on the following isolation functions:

1) Boron dilution isolation valve on RCV [CVCS] malfunction mitigation;
2) Containment isolation;
3) MSIV closure on SGTR (one tube) mitigation.

b) Categorisation & classification for the following safety functions:

1) Spent fuel pool makeup by ASP: currently category 3;
2) SBODG: currently category 3.

c) Amendment of diverse lines in Fault Schedule
1) The diverse protection candidate for reactor trip in SB-LOCA: “Containment pressure high 1” to be replaced by “Hot leg pressure low 1”;
2) Amendment derived from the investigations above.

ONR anticipates that a range of options will be considered by the RP to address each of the identified issues to ensure that the design is consistent with relevant good practice and that the risks are reduced As Low as Reasonably Practicable (ALARP). However, Reference 4 does not give sufficient explanation of these issues for ONR to understand the nature of the shortfalls nor does it provide a plan to address these.

This Regulatory Observation has therefore been raised to ensure that there is a robust demonstration that diverse protection has been provided for frequent faults and that risks have been reduced ALARP.

Relevant Legislation, Standards and Guidance

A nuclear power plant design should have demonstrable defence in depth in the delivery of safety functions and diversity is a key part of this demonstration. There is an expectation that levels of defence in depth are independent, as far as is practicable, as stated in IAEA SSR2-1 Requirement 7 and ONR’s SAPs EKP.3 (para 149 and 153).

Diverse, independent safety measures provide defence against common cause failures of the primary protection systems. SAPs EDR.3 states that Common Cause Failures (CCFs) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.

Supporting paragraphs give additional guidance to Inspectors on the limits of claims that should be made for CCFs:
SAPs para 185. In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by ONR of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis.

SAPs para 187. Where required reliabilities cannot be achieved due to CCF considerations, the safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.

In the UK, it is considered good practice to regard any fault sequence with a frequency greater than 1×10^{-7} per year to be within the design basis (SAPs FA.6). Given that SAP EDR.3 limits the reliability claim that may be placed on any safety system to be no better than 1×10^{-5} per demand, this means that for any initiating frequency greater than 1×10^{-2} per year (and in practice for most initiating frequencies greater than 1×10^{-3} per year) a diverse safety system, qualified to an appropriate standard, is required to be provided for each safety function.

The functional capability of the diverse system needs to be demonstrated using design basis analysis techniques with appropriate safety margins included to cover for uncertainties. GNS has developed a methodology (Reference 5) which states that functions which provide a diverse backup to a Category 1 function in a frequent fault are Category 2 functions and that these should be delivered by a Class 2 System Structure or Component (SSC). This is consistent with the expectation in ONR TAG 094 (Categorisation of Safety Functions and Classification of Systems, Structures and Components) that the diverse protection against failure of a Class 1 SSC that delivers a Category A safety function would be Class 2.

Regulatory Expectations

ONR’s regulatory expectation is that diverse protection for safety functions is provided for all frequent design basis faults and that a robust argument is provided to demonstrate that risks have been reduced As Low as Reasonably Practicable.

References

[1] Fault Schedule Production Methodology. GHX00600172DRAF02GN, Revision B, dated June 2018.

[2] Early Version of Fault schedule. GHX82036001DRAF03GN, Revision B dated December 2018.
[3] Bounding Case Selection for Diverse Protection Line Demonstration. GHX00600277DRAF02GN, Revision B, dated April 2019.
[4] Transient Analysis Report for Diverse Protection Line Demonstration. GHX00600141DRAF02GN Revision A, dated August 2019.
[5] Methodology of Safety Categorisation and Classification. GHX00100062DOZJ03GN Revision B, dated June 2018.

Regulatory Observation Actions

RO-UKHPR1000-0023.A1 – Confirm the list of frequent design basis faults

In response to this Regulatory Observation Action, GNS should:

- Confirm the list of design basis initiating events for which diverse protection is required, consistent with its design basis rules.

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

RO-UKHPR1000-0023.A2 – Identify which two safety systems are provided for each required safety function for the events identified in A1 and provide evidence that demonstrates the adequacy of each safety system.

In response to this Regulatory Observation Action, GNS should:

- Confirm the main and diverse safety systems, and any required support systems, that are claimed against each fault identified in A1.
- Provide sufficient information to demonstrate that these systems can be considered independent from each other and the initiating events.
- Confirm the safety classification and required reliability (probability of failure on demand) of each of these systems.
- Provide evidence (or reference to existing submissions) that demonstrates the ability of each of these systems to deliver the required safety functions.
- Provide evidence (or reference to existing submissions) that demonstrates that the systems will acheive the required reliability.

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

RO-UKHPR1000-0023.A3 – Provide additional information for any areas where additional work is needed to demonstrate diverse protection for frequent faults.

In response to this Regulatory Observation Action, GNS should provide sufficient information to explain the nuclear safety significance of any shortfalls against the safety case claims for diverse protection:

- Identify each relevant fault sequence and the safety functions for which the GNS has not been able to demonstrate diverse protection.
- Explain the current level of diversity within the delivery of the safety functions with reference to system diagrams as appropriate.
- Explain the nature and safety significance of any shortfalls against the expectations described above.

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

RO-UKHPR1000-0023.A4 – Provide evidence that a range of options has been considered to address the issues described in response to A3 and that risks have been reduced ALARP.

In response to this Regulatory Observation Action, GNS should:

- Consider whether there are any modifications to the design or operation of the plant that are reasonably practicable to implement.
- Demonstrate the adequacy of any proposed modifications to deliver the required safety functions.
- Provide a clear justification that the risks associated with the chosen design are reduced ALARP, consistent with GNS deterministic design rules, probabalistic risk targets and relevant good practice.

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:	