# REGULATORY OBSERVATION

## REGULATOR TO COMPLETE

| | |
|---|---|
| **RO unique no.:** | RO-UKHPR1000-0013 |
| **Revision:** | 0 |
| **Date sent:** | 03/09/19 |
| **Acknowledgement required by:** | 24/09/19 |
| **Agreement of Resolution Plan Required by:** | 28/02/20 |
| **CM9 Ref:** | 2019/209367 |
| **Related RQ / RO No. and CM9 Ref:** (if any)**:** | RQ-UKHPR1000-0226 (CM9 Ref. 2019/157632) |
| **Observation title:** | Modelling of computer based system reliability in the PSA |
| **Lead technical topic:**<br><br>15. Probabilistic Safety Analysis | **Related technical topic(s):**<br><br>3. Control & Instrumentation |

## *Regulatory Observation*

**Background**

ONR expects the safety case for new reactors to include a suitable and sufficient Probabilistic Safety Analysis (PSA) that adequately represents the design of the facility, that is realistic and that uses relevant data that is suitably underpinned. To this end, ONR is seeking to gain confidence in GNS' plan and approach for the modelling of computer based system reliability in the PSA for the UK HPR1000 generic design assessment (GDA).

Despite a number of engagements on this topic, GNS has yet to present a complete and coherent methodology for how and the plan for when the modelling of reliability of computer based safety systems will be justified and incorporated into the PSA. This is an important issue because the level of risk represented by computer based systems in the design may be significant and until the analysis has been performed it will continue to be unknown. While the response to RQ-UKHPR1000-0226 has provided some useful information, the approach outlined seemed to be somewhat complex and there was little consideration of:

- Identification of computer based systems and components to be modelled in the PSA.
- Explanation of how these will be modelled in the PSA.
- Justification of the source of data to be used in estimating the computer based system reliability and demonstration that it is suitably underpinned.
- Justification of the relevant standards applied and how the methodology follows industry-accepted practices.
- Explanation how dependencies (between systems and between components and subsystems within the same system) will be identified and explicitly addressed by the analysis
- Justification of how the analysis gives due consideration to the factors that could lead to common cause failures of computer based systems.

This regulatory observation has therefore been raised to:

- Explain ONR's regulatory expectations regarding the scope and content;
- Ensure that the Requesting Party (RP) provides a suitable and sufficient methodology explaining how computer based system reliability will be modelled in the PSA in a manner that meets ONR's regulatory expectations; and
- Ensure that the requesting party provides a realistic plan for when this work will be completed during the GDA.

**Relevant Legislation, Standards and Guidance**

ONR Safety Assessment Principal (SAP) FA.13 expects that the PSA model presents an adequate

representation of the facility.

| Fault analysis: PSA | Adequate representation | FA.13 |
|---|---|---|
| The PSA model should provide an adequate representation of the facility and/or site. | | |

Of particular relevance to this regulatory observation is SAPs paragraph 657, which states:

> 657. When models are used for the calculations of input probabilities, for example in human errors or failures of computer-based systems (including software errors), common cause failures, or the failures of structures, then the methodologies used should be justified, and should account for all key influencing factors.

Further guidance is provided in the ONR technical assessment guide on PSA, NS-TAST-GD-030 [3], in particular the following passages:

Section 4.5, paragraph 3 sub-paragraph iv:

*"The methodology used for the estimation of probabilities of failure of computer-based systems should meet industry accepted practices. The analysis of the software reliability should identify and take into account the influencing factors that affect the quality of the software. If the software system has been separated into parts that are treated individually in the reliability analysis, the dependencies between the various parts should be addressed explicitly. Any self-checking facilities built in the system should be taken into account in an adequate manner. The dependencies between diverse software systems should be dealt with explicitly."*

Table A1-2.6.2:

*"When models are used for the calculations of input probabilities, for example in human errors or failures of computer-based systems (including software errors), common cause failures, or the failures of structures, then the methodologies used should be justified, and should account for all key influencing factors."*

Appendix 4 of the ONR technical assessment guide on computer based safety systems, NS-TAST-GD-046 [4] provides guidance on the estimation of computer based system reliability for PSA purposes.

**Regulatory Expectations**

ONR expects: that the RP should demonstrate that the reliability of computer based systems has been modelled appropriately in the PSA during the UK HPR1000 GDA, in a manner that meets regulatory expectations described above; that the RP's PSA topic lead maintains oversight of the SQEP individuals from the RP's C&I design team who model the computer based systems in the PSA; and, that the methodology used to model computer based systems is integrated sufficiently into the overall Level 1 PSA methodology (Ref. 5).

The scope of this modelling should proportionately include any systems wherein computer based systems are expected to significantly contribute to the overall risk profile of the plant. As a minimum the following systems are expected to be considered:

- RPS
- SAS
- PSAS
- KDA.

ONR expects that the modelling of computer based system reliability in the PSA should demonstrate that:

- Factors influencing the quality and integrity of software are considered in the estimation of reliability.
- Where a software system is being separated into individual parts (for example consideration of operating system software and application software as separate entities), the analysis should explicitly address dependencies between the various parts.
- SMART components are considered, including sensors, actuators and those included in support systems.
- The PSA gives due consideration to the factors that could lead to common cause failures of computer

based systems.

- Where claims are made that separate parts of a computer based system are not subject to dependent failures, these claims should be suitably justified and underpinned.
- Dependencies between software systems that are claimed as independent and/ or diverse should be explicitly addressed.
- Estimations of the reliability of computer based system software should be justified by suitably underpinned data.

**References**

[1] Response to RQ-UKHPR1000-0226. CM9 Ref. 2019/157632
[2] *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 0, Office for Nuclear Regulation, 2014. www.onr.org.uk/saps/saps2014.pdf
[3] *Nuclear Safety Technical Assessment Guide, Probabilistic Safety Analysis*, NS-TAST-GD-030 Revision 5, Office for Nuclear Regulation, 2016. www.onr.org.uk/operational/tech_asst_guides/index.htm
[4] *Nuclear Safety Technical Assessment Guide, Computer Based Safety Systems*, NS-TAST-GD-046 Revision 5, Office for Nuclear Regulation, 2019. www.onr.org.uk/operational/tech_asst_guides/index.htm
[5] *Methodology of Internal Events Level 1 PSA* , GHX00650027DOZJ02GN, Revision A, GNS, 2018, CM9 Ref. 2018/139577

## *Regulatory Observation Actions*

**RO-UKHPR1000-0013.A1 – Provide a methodology and approach for the modelling of computer based system reliability in the PSA and demonstrate that it meets regulatory expectations**

In response to this Regulatory Observation Action, GNS should provide a methodology and approach to modelling computer based systems within the generic UK HPR1000 PSA so that the level of risk arising from computer based systems is adequately understood and demonstrated that it meets regulatory expectations.

ONR considers that the response to this Action should:

- Identify the computer based systems and components that will be modelled in the PSA;
- Explain how these will be modelled in the PSA;
- Justify the source of data that will be used to estimate computer based system reliability and demonstrate that it is suitably underpinned;
- Justify relevant standards applied and how the methodology follows industry-accepted practices.
- Explain how dependencies (between systems and between components and subsystems within the same system) will be addressed by the analysis; and
- Describe and justify how the analysis gives due consideration to the factors that could lead to common cause failures of computer based systems.

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

**RO-UKHPR1000-0013.A2 – Perform adequate PSA modelling of computer based system reliability**

In response to this regulatory observation action, the requesting party should:

- Implement the methodology and approach for the PSA based modelling of computer based systems as detailed in the response to Action 1. In responding to the Action the RP should consider staging the response such that ONR is provided with sufficient information to demonstrate the adequacy of the methodology, alongside a forward plan for completion of the full scope of activities necessary.

**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:** | |