REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0030
Revision:	1
Date sent:	23/01/2020
Acknowledgement required by:	20/02/2020
Agreement of Resolution Plan Required by:	21/02/2020
TRIM Ref:	2020/19270
Related RQ / RO No. and TRIM Ref: (if any)**:**	N/A
Observation title:	Justification For The Use Of Automatic Diagnosis
Lead technical topic: Human Factors	**Related technical topic(s):** C&I Fault Studies PSA

Regulatory Observation

Background

ONR has requested via RQ-UKHPR1000-0160 (Ref. 1) and RQ-UKHPR1000-0167 (Ref. 2) that GNS provide a suitable and sufficient risk assessment of the use of Automatic Diagnosis (AD) system on the UKHPR1000 design. ONR do not consider that a suitable and sufficient risk assessment has been provided so far.

The GNS position is that the AD system has no safety (or safety related) function so therefore does not require a safety justification. This is at odds with the AD system being part of a safety classified control and instrumentation system, the Class 3 Plant Standard Automation System (PSAS). This claim appears largely predicated on the use of a safety engineer to detect and protect against AD failures by advising incorrect fault responses that could potentially hazard the plant. On this basis, GNS has not provided a (suitable and sufficient) justification for its use.

ONR does not consider this position aligns with internationally recognised good practice. ONR definitions (which are aligned with IAEA) for Safety, and Safety Related, systems are clear that any systems "important to safety" should be classified as either Safety or Safety Related. Safety related is defined as "An item important to safety that is not part of a safety system".

The AD system directs operator actions in response to a plant fault and can thus be considered to support the delivery of the fundamental safety functions (control of reactivity, removal of heat from the core; and confinement of radioactive material). On this basis, ONR consider this system meets the definition: 'important to safety'.

The purpose of this RO is to help GNS to understand the GB regulatory requirements and expectations and to help it meets its legal duties by:

- Providing a suitable and sufficient justification to support the current claim that the AD system is not a Safety or Safety Related System; and
- If this cannot be substantiated, providing a suitable and sufficient safety justification for its use within the UK HPR1000 design and safety case.

Relevant Legislation, Standards and Guidance

The relevant SAPs (Ref. 3) and TAGs comprise the following.

EKP.2 (Fault tolerance) requires that the sensitivity of the facility to potential faults should be minimised. The consequence of failure of the AD has not been presented yet. Any failure, process perturbation or mal-operation in a facility should produce a change in plant state towards a safer condition, or produce no significant response. If the change is, however, to a less safe condition, then systems should have long time constants so that key parameters deviate only slowly from their desired values. It is conceivable that an AD fault could advise a course of action that could hazard the plant.

EKP.4 (Safety Function) requires that the safety function(s) to be delivered within the facility should be identified by a structured analysis.

EKP.5 (Safety measures) requires that safety measures should be identified to deliver the required safety function(s).

ECS.1 (Safety Categorisation) requires that: safety functions, both during normal operation and in the event of a fault or accident, should be identified and categorised based on their significance. This applies to prevention, protection, and mitigation.

ECS.2 (Safety Classification of SSCs) requires that: The SSC needed to the deliver the safety functions should be identified and classified based on their significance. Classification should take account of: category of the safety function; likelihood that the item will be called upon; potential for failure to initiate/exacerbate a fault; and the grace-time before being called upon and duration of any demand.

ERC.1 (Design and Operation of Reactors) requires that the design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor." AD likely has a role in the delivery of this.

ECS.3 (Codes and Standards) requires that SSC should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards. This should be done commensurate to the SSC class. Should AD be identified to be a safety / safety related system, then it is important that this SAP is considered.

EHF.3 (Identification of Actions Impacting Safety) requires a systematic approach to the identification of human actions that can impact safety for all permitted modes and all fault and accident conditions identified in the safety case, including severe accidents. Actions taken in response to AD direction have the potential to impact safety.

ESS.27 (Computer-based safety systems) requires that where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design.

NS-TAST-GD-046 (Rev 5) Computer Based Safety Systems (Ref. 4) provides guidance on the use, and safety assessment of computer based safety systems.

NS-TAST-GD-094 (Rev 1) - Categorisation of Safety Functions and Classification of Structures, Systems and Components (Ref. 5) provides guidance to ONR inspectors on the factors that should be considered when classifying Structures, Systems, Components, and Operator Actions.

Regulatory Expectations

In response to this RO, ONR expects the requesting party to:

- Identify the safety functions that AD either directly or indirectly supports and assign these an appropriate category.
- Based on the safety function/s, assign a suitable classification of the AD (and supporting) systems.
- Develop a verification and validation plan for the AD system, including both the technology and the human machine interface elements.
- Document the above in the safety case demonstrating the suitability of the AD system.

In addressing this RO, ONR expect that the responses provided will demonstrate that all relevant technical disciplines have provided inputs as necessary.

References

[1] ONR, (November 2018) RQ-UKHPR1000-0160 – Human Factors – The Verification, Validation and Use of Automatic Diagnosis on the UK HPR1000 Reactor Design
[2] ONR, ONR, (December 2019) RQ-UKHPR1000-0167 – Human Factors – Repeat RQ – The Verification, Validation and Use of Automatic Diagnosis on the UK HPR1000 Reactor Design
[3] ONR, (November 2014), Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 0, ONR,
[4] ONR, NS-TAST-GD-046 (Rev 5) Computer Based Safety Systems
[5] ONR, NS-TAST-GD-094 (Rev 1) - Categorisation of Safety Functions and Classification of Structures, Systems and Components

Regulatory Observation Actions

RO-UKHPR1000-0030.A1 – Identify the safety function/s that the AD system directly or indirectly supports

In response to this Regulatory Observation Action, GNS should:

- Provide a discription of how the AD system works; including both technology and operator aspects, e.g. how does it work under normal and fault conditions and who does what and when (conduct of operations).
- Analyse and document the failure modes of the AD system. Given the likely very high dependence between AD failing and the operator following a fault response based upon a potentially incorrect diagnosis, it is important to consider both the AD failure AND the consequent operator actions.
- Analyse and document the human factors phenomena associated with the failure of operator assist systems, and how these contribute to the consequences associated with AD failure.
- Based on an understanding of the failure modes and relevant human factors phenomena, carry out and document a consequence analysis.
- Analyse and document the likihood of failure of the AD system; to include both the technology and human elements of the system.
- On the basis of the above analysis, derive and categorise the safety function, or functions for the AD system being clear the extent to which the function/s is required to prevent, protect or mitigate.

RO-UKHPR1000-0030.A2 – Based on the safety function/s, assign a suitable safety classification for the AD system

In response to this Regulatory Observation Action, GNS should:

- Based upon the response to Action 1, justify the safety classification assignment of the AD system, taking account of:
    - The safety category assigned to the functions that the AD system supports.
    - Any supporting or auxiliary systems.
    - The role of the operator.
    - The likelihood of the AD system being called upon for prevention, protection or mitigation purposes.
    - The consequences of failure, e.g.: could its failure become a hazard in its own right, either as an initiating event or as a post fault failure.
    - Time factors; e.g. how long does the operator have to detect and recover from AD failure.

RO-UKHPR1000-0030.A3 – Develop a verification and validation plan for the AD system, including both the technology and the human machine interface elements

In response to this Regulatory Observation Action, GNS should:

- Based on the safety classification of the AD derived under Action 2, develop a qualification plan for the technology commensurate with its safety classification. This should include both verification and validation activities. Where appropriate, it should consider the need to:

- Demonstrate that the technology enabling the AD system, should, as a minimum, meet relevant good practice.
- Demonstrate that the AD system cannot detrimentally effect physically or functionally linked systems.
- Demonstrate that the AD system can meet the necessary reliability targets.

- Provide a plan, appropriate to the safety classification derived under Action 2, describing the verification and validation of the AD system from a human-technology perspective. It should consider the need to:
  - Demonstrate that the AD system interface needs to be operable under normal and fault conditions.
  - Demonstrate that reasonably foreseeable failures of the AD system can be protected against or are suitably mitigated.
  - Demonstrate that the AD system reliably operates in concert with the rest of the main control room design under normal and fault conditions.
  - Demonstrate that in the event of total AD failure, the alternative diagnostic approach is suitable.

RO-UKHPR1000-0030.A4 – Produce a suitable and sufficient safety justification for the AD system as part of the overall UK HPR1000 safety case

In response to this Regulatory Observation Action, GNS should:

- Based upon the responses to Actions 1 to 3, produce a suitable and sufficient safety justification for the AD system. ONR would expect this justfication to build upon the responses provided under this RO, and suitably link to the overall UK HPR1000 safety case.

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:	