 CGN EDF General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0030	Rev.: 1	Page: 1 / 7
		GDA-REC-GNSL-006969	

REGULATORY OBSERVATION Resolution Plan

RO Unique No.:	RO-UKHPR1000-0030
RO Title:	Justification For The Use Of Automatic Diagnosis
Technical Area(s)	Human Factors
Revision:	0
Overall RO Closure Date (Planned):	01-12-2020
Linked RQ(s)	NA
Linked RO(s)	NA
Related Technical Area(s)	C&I, PSA, Fault Studies
Other Related Documentation	NA

Scope of Work

Background

ONR has requested via RQ-UKHPR1000-0160 (Ref. 1) and RQ-UKHPR1000-0167 (Ref. 2) that the requesting party 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 requesting party 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 the operating team and a safety engineer to detect and protect against AD failures by advising incorrect fault responses that could potentially hazard the plant. On this basis, the requesting party 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 supports 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

 <p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0030</p>	Rev.: 1	Page: 2 / 7
	GDA-REC-GNSL-006969	

to safety’.

The purpose of this RO is to help the requesting party 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.

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.

Deliverable Description

The scope of work is defined in RO-UKHPR1000-0030 as four actions. This plan describes how the requesting party will address each action.

RO-UKHPR1000-0030.Action 1 – Identify the safety function/s that the AD system directly or indirectly supports

In response to this action the requesting party will undertake a number of assessment activities and prepare a report that presents the following information:

1. A description of how the AD system works, including;
 - Technological aspects
 - Operational aspects
 - Where the AD System sits in the I&C architecture
2. An assessment on the effect the AD system has on the overall safety case and how this will be

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0030	Rev.: 1	Page: 3 / 7
		GDA-REC-GNSL-006969	

recognised during Step 4 of the GDA process.

3. Possible failure mechanisms of the AD system and consequences will be performed. It will identify and document credible failures of the AD system, how each failure is revealed to the operator and the required operator action in response to the failure.
4. An assessment of the impact of each credible failure on operator behaviour taking account of human factors phenomena related to the use and failure of operator assist systems.
5. Based on 3, consider the impact of the AD failure mode on operators' ability to deliver their role in achieving safety functions.
6. Derive an estimate of the probability of AD failure. Assess the operators' ability to detect the AD failure and support delivery of the safety function using other means. For example a clear indication of the fault on an alternative HMI.
7. Identify the safety functions that are supported by the AD system by identification of the design basis accidents that make a claim on AD supported operator initiated safety measures and the transition to severe accident states. Identify the safety category of those functions.

The "Concept of Operations" has been updated based on the utilisation of the AD system and submitted on 30/06/2020. The related Human Reliability Assessment (HRA) documents will also be consistent with the updated "Concept of Operations".

A new document "Justification of the AD Safety Classification" will be submitted on 31/08/2020. Furthermore, detailed human factor phenomena related to the use and failure of AD will be summarised in the document "AD System Design Analysis Report" which will be submitted on 30/09/2020.


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

In response to this action, the requesting party will derive and justify the safety classification for the AD system. Classification of the AD system will take account of:

1. The safety function(s) the AD system supports and their associated categorisation.
2. Relevant supporting or auxiliary systems.
3. The role of the AD system and operator in delivering these safety functions.
4. The probability of the AD system being required to support delivery of the safety function
5. Whether AD failure can directly initiate a fault or exacerbate the consequences an existing fault e.g. as a result of misdiagnosis.
6. The time available for AD supported operator response (detection and recovery) and the duration for which AD and operator response will be required.

The document "Justification of the AD Safety Classification" will be submitted on 31/08/2020.

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

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0030	Rev.: 1	Page: 4 / 7
		GDA-REC-GNSL-006969	

In response to this action, the requesting party will develop a verification and validation plan for the AD system. This V&V plan will be split into two main activities:

Develop of a technology qualification plan commensurate with the AD's safety classification, including both verification and validation activities. The activities in the plan will

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

Develop a plan regarding the verification and validation from a human-technology perspective. The activities in the plan will

1. Demonstrate that the AD system interface is operable under normal and fault conditions. By providing evidence that HBSC can be diagnosed reliably without AD or with an incorrect AD result.
2. Demonstrate that reasonably foreseeable failures of the AD system can be protected against or are suitably mitigated by reference to the possible failure mechanisms of the AD system and consequences described in A1.
3. Demonstrate that the AD system reliably operates in concert with the rest of the main control room design under normal and fault conditions. This will be achieved both through the HBSC assessment programme and the MCR validation programme.
4. Demonstrate that in the event of AD failure, the alternative diagnostic approach is suitable by HBSC assessment.

A new document "Qualification Plan of the AD System" will be submitted on 15/09/2020.

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

A new report "AD System Design Analysis Report" will be produced which will report the outcome of the analyses completed under Actions 1 to 3. This will describe:

1. the operation of the AD system,
2. the credible failure modes of the AD system and their impact on operator response,
3. The safety functions supported by the AD system and their categorisation
4. The classification of the AD system
5. Verification and Validation activities and the results of these where they are available during GDA
6. Identify and list all the safety case documents related to AD system and make an update plan of those documents during Step 4 of the GDA process if necessary

The report will provide a suitable and sufficient documented risk assessment to justify that the AD system

 <p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0030</p>	Rev.: 1	Page: 5 / 7
	GDA-REC-GNSL-006969	

meets the reliability requirements associated with its classification and that it does not decrease the likelihood of safety functions being achieved as a result of AD failure and associated operator errors related to misdiagnosis.

“AD System Design Analysis Report” will be submitted on 30/09/2020.

Impact on the GDA Submissions

GDA Submission Document	Related ROAs	Schedule for Submission
Concept of Operations, Rev. E	ROA1	30/06/2020
Justification of the AD Safety Classification, Rev. A	ROA1, ROA2	31/08/2020
Qualification Plan of the AD System, Rev. A	ROA3	15/09/2020
AD System Design Analysis Report, Rev. A	ROA4	30/09/2020

Timetable and Milestone Programme Leading to the Deliverables

See attached Gantt Chart in APPENDIX A.

Reference

 <p>General Nuclear System</p>	<p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0030</p>	Rev.: 1	Page: 6 / 7
		HPR/GDA/GNS/0000XX	

APPENDIX A RO-UKHPR1000-0030 Gantt Chart

Task and Schedule	2020												2021	
	31-Jan	29-Feb	31-Mar	30-Apr	31-May	30-Jun	31-Jul	31-Aug	30-Sep	31-Oct	30-Nov	31-Dec	31-Jan	28-Feb
RO Action 1														
Development of deliverable-[Concept of Operations]	█	█	█	█	█	█								
Submission of deliverable-[Concept of Operations]							▲							
Development of deliverable-[Justification of the AD Safety Classification]	█	█	█	█	█	█	█							
Submission of deliverable-[Justification of the AD Safety Classification]								▲						
RO Action 2														
Development of deliverable-[Justification of the AD Safety Classification]	█	█	█	█	█	█	█							
Submission of deliverable-[Justification of the AD Safety Classification]								▲						
RO Action 3														
Development of deliverable-[Qualification Plan of the AD System]	█	█	█	█	█	█	█	█						
Submission of deliverable-[Qualification Plan of the AD System]									▲					
RO Action 4														
Development of deliverable-[AD System Design Analysis Report]	█	█	█	█	█	█	█	█						
Submission of deliverable-[AD System Design Analysis Report]									▲					
Assessment														
Regulatory Assessment	█	█	█	█	█	█	█	█	█	█	█	█		

