
 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001	Rev.: 1	Page: 1 / 8
		GDA/REC/GNS/003379	

REGULATORY OBSERVATION Resolution Plan	
RO Unique No.:	RO-UKHPR1000-0001
RO Title:	Diverse Actuation System Design Shortfalls
Technical Area(s)	Control & Instrumentation
Revision:	Rev 1
Overall RO Closure Date (Planned):	31/08/2019
Linked RQ(s)	-
Linked RO(s)	-
Related Technical Area(s)	<ul style="list-style-type: none"> - Electrical Engineering - Fault Studies - Internal Hazards - Probabilistic Safety Analysis - Security
Other Related Documentation	Refer to Appendix A
Scope of Work	
<p><u>Background</u></p> <p>The provision of nuclear safety functions to trip nuclear power plant reactors and initiate post trip cooling of the core (which continues to produce significant quantities of heat post trip) is a key role of Nuclear Power Plant Control and Instrumentation (C&I) equipment. As the reference plant for the UK HPR1000, the Hua-long Pressurized Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) adopts two C&I systems to perform these functions – the Reactor Protection System (RPS) and the Diverse Actuation System (KDS [DAS]).</p> <p>A number of aspects of the HPR1000 (FCG3) KDS [DAS] design do not align with UK Relevant Good Practice (RGP). ONR has raised RO-UKHPR1000-0001 to highlight the gaps.</p> <p><i>ONR expectations are for the UK HPR1000 DAS or Secondary Protection System (SPS) design and safety case to provide a suitable and sufficient justification that ONR expectations and relevant good practice can be satisfied regarding:</i></p> <ul style="list-style-type: none"> <i>i) DAS/SPS classification;</i> <i>ii) DAS/SPS ability to meet relevant good practice with respect to the single failure criterion;</i> <i>iii) DAS/SPS implementation technology, to include consideration of failure to safety,</i> 	

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001	Rev.: 1	Page: 2 / 8
		GDA/REC/GNS/003379	

diversity and common cause failure (CCF).

Based on the relevant ONR Safety Assessment Principles (SAPs) ^[1], standards such as IEC61513 ^[2] and IEC61226 ^[3] mentioned in the Regulatory Observation (RO), and other RGP, suitable and sufficient modification of the KDS [DAS] design will be developed. This resolution plan provides a response to each of the three gaps and draws up a plan to address them.

Scope of work


The KDS [DAS] modification for the UK HPR1000 will consider the requirements of IEC 61513, IEC 61226, IAEA SSG-30 ^[4], IAEA SSG-39 ^[5], the principles provided in relevant ONR SAPs, e.g. EKP.2, ESP.3, ECS.2, EDR.1, EDR.3, EDR.4, ESS.1, ESS.18, ESS.21, ESS.27, etc., and other relevant important standards, e.g. IEC 60980 ^[6], IEC 61225 ^[7] and IEC 60780-323 ^[8].

A top-down approach will be adopted to identify the activities needed for the KDS [DAS] modification. The modification is mainly related to the following technical disciplines:

- Control & Instrumentation
- Electrical Engineering
- Fault Studies
- Human Factors
- Internal Hazards
- Mechanical Engineering
- Probabilistic Safety Analysis
- Security

Prior to the tasks performed within the C&I discipline, upstream tasks will be undertaken to define the system role and function scope of the KDS [DAS] in accordance with the high level design principles, the development of fault analysis and task analysis.

Two topic reports will be developed respectively for the closure of this RO. The first report titled '*Safety Requirements of the KDS [DAS]*', which specifies the system role, the system classification, the system design principles, the design requirements (e.g. the general requirements for the technology used for the KDS [DAS]) and the reference list of codes and standards, will be provided as the response to RO Action 1 & 2. The second report titled '*Simple Hardware Based Platform Technical Research Summary Report*', which presents the output of the investigation of simple hardware technologies, lists a number of potential technologies which could be used for the KDS [DAS] and describes the methodology for selection of the KDS [DAS] technology, will be provided as the response to RO Action 3.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001	Rev.: 1	Page: 3 / 8
		GDA/REC/GNS/003379	

The activities in completing the integrated design modification may continue beyond the planned closure date of this RO. The remaining activities identified in the two reports will be tracked by the GNS Commitment Tracker, which will also be used to record and manage the progress of commitments and to ensure that the safety case can be updated accordingly.

The process of design modification will follow the GNS procedure of Design Change Control which is yet to be formally issued, but will be in place before the end of GDA Step 2. A design change proposal for this modification will be raised at the appropriate time in the GDA project (likely to be in step 3).

Please note that, subject to regulatory agreement, this resolution plan may be updated in future.

Deliverable Description

It is proposed that the responses to RO Action 1 and Action 2 will be combined into a single report, i.e. *Safety Requirements of the KDS [DAS]*.

RO-UKHPR1000-0001.Action 1

The RO action states that:

In response to this Regulatory Observation Action, GNS should:

Taking into account:


- *ONR expectations;*
- *relevant good practice; and*
- *the nuclear safety significance of the UK HPR1000 Diverse Actuation System/Secondary Protection System.*

Provide a suitable and sufficient justification for the classification of the DAS/SPS in UK HPR1000.

Resolution Plan

It is noted that it is stated in IAEA-SSG-30: *Any function that is designed to provide a backup of a function categorised in safety category 1 and that is required to control design extension conditions without core melt should be categorised as safety category 2.* In addition, it is understood that the SPS has been classified as at least a class 2 system in previous UK projects for similar designs and is considered as UK RGP.

Compared with the current KDS [DAS] design for HPR1000 (FCG3) as described in the Preliminary Safety Report (PSR) ^[9], the KDS [DAS] proposed for UK HPR1000 will be re-classified, according

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001	Rev.: 1	Page: 4 / 8
		GDA/REC/GNS/003379	

to:

- Methodology of Categorisation and Classification for UK HPR1000^[10]; and
- System role of the KDS [DAS].

The functional role of the KDS [DAS] will be determined, and then the system will be classified according to the methodology for categorisation and classification of systems.

In response to RO Action 1, the report entitled ‘*Safety Requirements of the KDS [DAS]*’ will be provided to present the design principles of the KDS [DAS]. Detailed information about classification of the KDS [DAS] in UK HPR1000 will be specified in the report. The report will include:

- Codes and Standards.
- System role in the C&I Defence in Depth (DiD) structure.
- Function categorisation and system classification.
- General design principles of the KDS [DAS], including Single Failure Criterion (SFC), independence, hazard-protection, failure to safety, etc.
- Requirements for the KDS [DAS] platform technology.

RO-UKHPR1000-0001.Action 2

The RO action states that:

In response to this Regulatory Observation Action, GNS should:

Taking into account:

- *the GNS response to A1;*
- *ONR expectations; and*
- *relevant good practice.*

Provide a suitable and sufficient justification of the ability of the DAS/SPS in UK HPR1000 to meet relevant good practice with respect to the single failure criterion and/or other relevant engineering principles (e.g. failure to safety).

Resolution Plan

SFC in NS-TAST-GD-003^[11] and in related standards such as IEC 61266 will be taken into account. In addition, RGPs regarding SFC and other relevant engineering principles (e.g. failure to safety,

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001	Rev.: 1	Page: 5 / 8
		GDA/REC/GNS/003379	

independence, etc.) will be considered, notably from previous GDAs.

Detailed information covering compliance with the SFC and other relevant engineering principles will be included in the design principles, which will be presented in the report ‘*Safety Requirements of the KDS [DAS]*’ (as defined in Action 1).

After the RO closure, a further assessment will be carried out to establish the KDS [DAS] architecture (e.g. number of trains). This work will be referenced by the design change proposal.

RO-UKHPR1000-0001.Action 3

The RO action states that:

In response to this Regulatory Observation Action, GNS should:

Taking into account:

- *ONR expectations; and*
- *relevant good practice regarding the potential vulnerability to common cause failure of complex programmable technology in combination with software-based technology.*

Provide a suitable and sufficient justification for the implementation technology proposed for the DAS/SPS in UK HPR1000.


Resolution Plan


The design of complex hardware technology has many similarities with the design of software for computer based safety systems. It is challenging to demonstrate diversity between software technology and complex hardware technology. For the purpose of achieving diverse functions, simple hardware technologies were adopted in previous UK projects.


For RO Action 3, investigation will be undertaken to complete a feasibility analysis on existing simple hardware technologies. From the feasibility analysis, the list of potential technologies which could be used for the KDS [DAS] will be derived and presented. A detailed methodology, to select the specific technology for the KDS [DAS], will also be presented.

A report titled ‘*Simple Hardware Based Platform Technical Research Summary Report*’, which describes simple hardware technologies as potential options for the KDS [DAS], will be provided. The report will include:

- A survey and feasibility analysis of simple hardware technologies.
- A list of potential technologies to be used in the KDS [DAS].

 <p>General Nuclear System</p>	<p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001</p>	Rev.: 1	Page: 6 / 8
		GDA/REC/GNS/003379	
<p>– A methodology for selection of the platform technology for the KDS [DAS].</p> <p>Further work related to detailed design of the system will be undertaken following the closure of this RO. This will be included in the design change proposal.</p>			
<p>Impact on the GDA Submissions</p>			
<p>The PCSR V0^[12] delivered for formal GDA Step 3 assessment is based on the existing KDS [DAS] design and as such provides an updated baseline for the gap that this RO resolution plan will address. The updated information will be incorporated into PCSR V1 to be submitted at the end of Step 3 and PCSR V2 to be submitted at the end of Step 4.</p>			
<p>Timetable and Milestone Programme Leading to the Deliverables</p>			
<p>See attached Gantt Chart in APPENDIX A.</p>			
<p>References</p>			
[1]	SAP	Safety Assessment Principles for Nuclear Facilities	ONR 2014
[2]	IEC 61513	Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirements for Systems	IEC 2011
[3]	IEC 61226	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Classification of Instrumentation and Control Functions	IEC 2009
[4]	IAEA SSG-30	Safety Classification of Structures, Systems and Components in Nuclear Power Plants	IAEA 2014
[5]	IAEA SSG-39	Design of Instrumentation and Control Systems for Nuclear Power Plants	IAEA 2016
[6]	IEC 60980	Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations	IEC 1989
[7]	IEC 61225	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Requirements for Electrical Supplies	IEC 2005

 General Nuclear System		REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001		Rev.: 1	Page: 7 / 8
				GDA/REC/GNS/003379	
[8]	IEC 60780-323	Nuclear Power Plants - Electrical Equipment of Safety System - Qualification	IEC	2016	
[9]	HPR/GDA/PSR /0008	Preliminary Safety Report Chapter 8 Instrumentation & Control, Rev. 000	GNS	2017	
[10]	GHX00100062DOZJ03GN	Methodology of Safety Categorisation and Classification	CGN	2018	
[11]	NS-TAST-GD-003	Nuclear Safety Technical Assessment Guide - Safety Systems	ONR	2017	
[12]	HPR/GDA/PCSR /0008	Pre-Construction Safety Report Chapter 8 Instrumentation & Control, Rev. 000	GNS	2018	
Rev.	Author	Scope/Reason of Revision	Date	Page	
1	██████████	According to the updating RO, the associated quotation and the description of relevant engineering principles have been modified.	November 2018	1, 2, 4~6	
	██████████	Add the updating references.	November 2018	4, 6, 7	

 <p>General Nuclear System</p>	<p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0001</p>	Rev.: 1	Page: 8 / 8
		GDA/REC/GNS/003379	

APPENDIX A RO-UKHPR1000-0001 Gantt Chart

	Apr-18	May-18	Jun-18	Jul-18	Aug-18	Sep-18	Oct-18	Nov-18	Dec-18	Jan-19	Feb-19	Mar-19	Apr-19	May-19	Jun-19	Jul-19	Aug-19	
RO Action 1 and Action 2																		
Development of deliverable - [Safety Requirements of the KDS [DAS]]	█																	
Submission of deliverable - [Safety Requirements of the KDS [DAS]]									▲									
RO Action 3																		
Development of deliverable - [Simple Hardware Based Platform Technical Research Summary Report]	█																	
Submission of deliverable - [Simple Hardware Based Platform Technical Research Summary Report]												▲						
Assessment																		
Regulators Assessment	█																	
Target RO Closure Date																		▲