


 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 1 / 10
		GDA-REC-GNS-005202	

REGULATORY OBSERVATION Resolution Plan	
RO Unique No.:	RO-UKHPR1000-0017
RO Title:	Demonstration of independence between C&I systems
Technical Area(s)	Control & Instrumentation
Revision:	Rev. 0
Overall RO Closure Date (Planned):	2021-03-31
Linked RQ(s)	-
Linked RO(s)	-
Related Technical Area(s)	<ul style="list-style-type: none"> - Civil Engineering - Electrical Engineering - Fault Studies - Internal Hazards - Mechanical Engineering - Probabilistic Safety Analysis
Other Related Documentation	Refer to Appendix A
Scope of Work	
<p><u>Background</u></p> <p>Defence in Depth (DiD), achieved through the provision of multiple independent barriers against faults progression and potentially significant failures, plays a key role in the Instrumentation and Control (usually for I&C in China, C&I in the UK) architecture in nuclear power plants.</p> <p>A number of aspects of I&C design have been identified which do not currently meet ONR's expectations regarding independence between I&C systems. RO-UKHPR1000-0017 has been raised by ONR to highlight a number of potential shortfalls including the following:</p> <ul style="list-style-type: none"> • Shared equipment between I&C systems important to safety; • Component Interface Module (CIM) design scheme; • Signal Pre-processing Module (SPM) design scheme; • Separation and segregation of I&C systems; • Independence of I&C architecture design such that the risk of failures affecting multiple systems and compromising delivery of safety functions is reduced to as low as reasonably practicable (ALARP). 	

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 2 / 10
		GDA-REC-GNS-005202	

Based on the relevant ONR Safety Assessment Principles (SAPs), Reference [1], standards such as IEC 61513, Reference [2], and IEC 60709, Reference [3], and other Relevant Good Practice (RGP), this resolution plan provides response to each of the five Regulatory Observation (RO) actions and sets out the plan to address them.

Scope of work

A top-down approach will be adopted for the demonstration of independence between I&C systems. The demonstration of independence is mainly related to the following technical disciplines:

- Civil Engineering
- Electrical Engineering
- Fault Studies
- Internal Hazards
- Mechanical Engineering
- Probabilistic Safety Analysis

Each potential shortfall will be justified and addressed, with the following considerations:

- For shared equipment between I&C systems important to safety, I&C components shared in different defence lines, including sensors and actuators, will be identified and justified.
- For the CIM design scheme, a CIM improvement will be developed to demonstrate the risk of Common Cause Failure (CCF) is ALARP.
- For the SPM design scheme, an SPM improvement will be developed to demonstrate the risk of CCF is ALARP.
- The measures for separation and segregation of I&C systems will be enhanced and a demonstration will be made that the risk of failure propagation and the risk of CCFs due to internal plant hazards is ALARP.
- For independence of I&C architecture design, the justification of shared components, ALARP analysis of the CIM and the SPM, and justification for the separation and segregation, will be systematically integrated and set out in the I&C architecture design.

To address this RO, the following documents will be updated or developed:

- *Independence analysis of I&C systems*, which will identify the shared components for Action 1.
- *Optioneering Analysis Report for CIM Improvement*, which will address the requirements of Action 2.
- *Optioneering Analysis Report for SPM Improvement*, which will address the requirements of Action 3.
- *Basis of Safety Case (BSC) of Overall I&C Architecture and Independence analysis of I&C systems*, which will address the requirements of Action 4.
- *BSC of Overall I&C Architecture and BSC of Protection System*, which will be developed as the response to Action 5.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 3 / 10
		GDA-REC-GNS-005202	

Deliverable Description

RO-UKHPR1000-0017.A1 – Justification of shared equipment

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should provide a suitable and sufficient justification for the sharing of equipment between C&I systems important to safety. This justification should include, but not be limited to, consideration of the following:

- *Identification of which equipment is shared between C&I systems at different defence in depth levels and which safety functions are performed by that equipment;*
- *Justification that C&I systems and components fulfilling safety functions are independent from the systems and components involved in the initiating events against which they protect;*
- *Justification of the sharing of equipment between C&I systems important to safety; and*
- *Identification and justification of the use of common support systems between C&I systems at different levels of defence in depth and in different divisions within the same level of defence in depth.*


Resolution Plan

IEC 62340, Reference [4], states that *Independent I&C systems shall not use shared components or services if the postulated failure of these shared components or services can cause a coincident failure of the independent I&C systems (e.g. a common power supply)*. Compared with the current overall I&C architecture design for the UK HPR1000, there are some shared components of different defence lines, e.g. CIM, SPM.

In response to RO Action 1, the report '*Independence analysis of I&C systems*' will be updated to analyse and identify the shared components (e.g. sensors, CIM, SPM, supporting system) between I&C systems (e.g. RPS [PS] and PSAS, RPS [PS] and KDS [DAS]), which will include:

- 1) Analysis of mitigation by I&C functions in different protection lines for each Postulated Initiating Event (PIE) from the Fault Schedule;
- 2) Comprehensive identification of the I&C components shared in different defence lines, including sensors and actuators;
- 3) Identification of common support systems;
- 4) Justification of the shared sensors and actuators between I&C systems important to safety.

The justification of the shared CIM and SPM is addressed in actions 2 and 3.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 4 / 10
		GDA-REC-GNS-005202	

RO-UKHPR1000-0017.A2 – Justification of CIM design scheme

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should provide a suitable and sufficient justification for the role of the CIM in delivery of safety functions for multiple C&I systems. The justification should consider the following:

- *Explanation of the role of the CIM in delivery of safety functions and description of the design scheme;*
- *The architecture and implementation technology of the CIM;*
- *Demonstration that the risk of failure of the CIM affecting multiple C&I systems in different layers of defence simultaneously is reduced ALARP; and*
- *Demonstration that the risk of failure of the CIM affecting multiple divisions within a C&I system simultaneously is reduced ALARP.*

Resolution Plan


IEC 61513, Reference [2], states that *Independence includes provisions to prevent adverse interaction between subsystems of the system or with other systems which might result from abnormal operation or from failure of any component in either subsystem or system, including from common-cause failure.*

The CIM serves as the interface with the plant components. The CIM manages the priority of different component control signals from different I&C systems using priority logic, and then sends the signal with the highest priority to a controlled component such as a motor operated valve, pump motor, or solenoid operated valve. As the CIM acts as the common interface to I&C systems in different DiD levels, the failure of the CIM could result in a loss of relevant I&C systems, either for one division or across multiple divisions.

The requirements of the CIM are provided in the report ‘*Component Interface Module (CIM) Requirement Specification*’, Reference [5]. However, the current design scheme of the CIM for the UK HPR1000 is based on CPLD technology, so that it’s difficult to sufficiently demonstrate that the risk of the CIM failure, which can simultaneously affect multiple I&C systems in different DiD levels and multiple divisions within the RPS [PS], has been reduced to ALARP.

In response to RO Action 2, the report ‘*Optioneering Analysis Report for CIM Improvement*’ will be provided, in which the method of ALARP demonstration will be used and the following will be included:

- 1) Description of the role of the CIM in delivery of safety function;
- 2) Identification and evaluation of options for implementation technology and design scheme of the CIM;
- 3) Recommended implementation technology and design scheme (e.g. the architecture) of the CIM;

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 5 / 10
		GDA-REC-GNS-005202	

- 4) Demonstration that the risk of concurrent failure of the CIM is reduced to ALARP, considering the extent to which the requirements of the fault analysis and PSA can be met by the I&C design.

RO-UKHPR1000-0017.A3 – Justification of SPM design scheme

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should provide a suitable and sufficient justification for the role of the SPM in delivery of safety functions for multiple C&I systems.

The justification should consider the following:

- *Explanation of the role of the SPM in delivery of safety functions and description of the design scheme;*
- *The architecture and implementation technology of the SPM;*
- *Demonstration that the risk of failure of the SPM affecting multiple C&I systems in different layers of defence simultaneously is reduced ALARP ; and*
- *Demonstration that the risk of failure of the SPM affecting multiple divisions within a C&I system simultaneously is reduced ALARP.*

Resolution Plan


IEC 61513, Reference [2], states that *Independence includes provisions to prevent adverse interaction between subsystems of the system or with other systems which might result from abnormal operation or from failure of any component in either subsystem or system, including from common-cause failure.*

The SPM serves as the interface with the plant sensors. The SPM implements the power supply to sensors, conditioning of the signal (resistance, mV, etc.) to 4mA-20mA, signal filtering, signal multiplication and distribution to I&C systems which need it, and electrical isolation between I&C systems. As the SPM acts as the common interface to I&C systems in different DiD levels, the failure of the SPM could result in a loss of relevant I&C systems, either for one division or across multiple divisions.

Based on the assessment of the current SPM design scheme, it is difficult to sufficiently demonstrate that the risk of the SPM failure, which can simultaneously affect multiple I&C systems in different DiD levels and multiple divisions within the RPS [PS], has been reduced to ALARP.

In response to RO Action 3, the report '*Optioneering Analysis Report for SPM Improvement*' will be provided, in which the method of ALARP demonstration will be used and the following will be included:

- 1) Description of the role of the SPM in delivery of safety function;
- 2) Identification and evaluation of options for implementation technology and design scheme of the SPM;

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 6 / 10
		GDA-REC-GNS-005202	

- 3) Recommended implementation technology and design scheme (e.g. the architecture) of the SPM;
- 4) Demonstration that the risk of concurrent failure of the SPM is reduced to ALARP, considering the extent to which the requirements of the fault analysis and PSA can be met by the I&C design.

RO-UKHPR1000-0017.A4 – Separation and segregation of I&C systems

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should provide a suitable and sufficient justification for the approach to separation and segregation of C&I systems to protect against consequential physical effects caused by faults and normal actions within other systems and internal plant hazards. The justification should consider the following:

- *Protection against failures in redundant divisions of the same system;*
- *Protection against failures of systems within the same division;*
- *Resilience against common cause failures caused by internal plant hazards including but not limited to EMC, fire, extreme temperatures and flooding within a system;*
- *Resilience against common cause failures caused by internal plant hazards including but not limited to EMC, fire, extreme temperatures and flooding, across levels of defence in depth; and*
- *Demonstration that the risk of failure propagation between systems, and between redundant parts of the same system, and the risk of common cause failures due to internal plant hazards, has been reduced ALARP.*

Resolution Plan

IAEA SSG-39, Reference [6], states that *Hazards that should be considered include internal hazards and external hazards, failures of plant equipment and I&C failures or spurious operation due to hardware failure or software errors.* According to the requirements, *I&C systems and components should be protected against the effects of other internal hazards in accordance with the guidance of NS-G-1.11.*

The relevant claims, arguments and evidence to address the approach to separation and segregation of I&C systems have so far not met the ONR's expectation for demonstration that the risk of failure propagation between systems and the risk of common cause failures due to internal plant hazards has been reduced to ALARP.

In response to RO Action 4, two reports '*Independence analysis of I&C systems*' and '*BSC of Overall I&C Architecture*' will be updated, in which the arguments and evidence will be developed and enhanced to demonstrate that the separation and segregation of the I&C architecture is sufficient, and that the risk of failure propagation and the risk of CCFs due to internal hazards has been reduced to ALARP.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 7 / 10
		GDA-REC-GNS-005202	

RO-UKHPR1000-0017.A5 – Justification of architecture design

The RO action states that:

In response to this Regulatory Observation Action, General Nuclear System Limited should provide a suitable and sufficient justification of how the UK HPR1000 C&I architecture provides sufficient independence such that the risk of failures affecting multiple systems and compromising delivery of safety functions is reduced ALARP. The justification should consider the following:

- *How the regulatory expectations outlined in this Regulatory Observation are met;*
- *How the UK HPR1000 safety analysis supports the justifications being made; and*
- *How the design of the UK HPR1000 C&I architecture reduces the risk of common-cause failures affecting multiple systems, or multiple divisions within systems, ALARP.*


The justification that risks have been reduced ALARP should demonstrate the options that were considered in the design of the UK HPR1000 C&I architecture, why the selected option(s) achieve the optimum safety benefit and why measures to further reduce risks are not reasonably practicable.

The demonstration of adequate independence, redundancy, separation and segregation of SSCs has the potential to require design modifications. In response to this RO the requesting party should provide justification that the risks associated with the UK HPR1000 C&I architecture and layout have been reduced ALARP.

Resolution Plan

IAEA SSG-39, Reference [6] states that *The overall I&C architecture should not compromise the concept of defence in depth and the diversity strategies of the design of the plant and The overall I&C architecture should neither compromise the independence of safety system divisions, nor the independence of the different levels of the defence in depth applied at the plant.* The provided BSC documents set out the demonstration of Defence in Depth, safety classification, Single Failure Criterion, diversity, etc., but do not adequately address independence.

Compared with the current overall I&C architecture design for the UK HPR1000, as described in the ‘*BSC of Overall I&C Architecture*’, Reference [7] and ‘*BSC of Protection System*’, Reference [8], it is acknowledged that the demonstration of independence of shared components, the ALARP analysis of common equipment and the justification for separation and segregation have so far not met ONR’s expectations. To address this, updated reports, i.e. ‘*BSC of Overall I&C Architecture*’ and ‘*BSC of Protection System*’ (RPS [PS] as an example system) will be provided to systematically integrate and set out the justification of shared components, the ALARP analysis of the CIM and the SPM, as well as the justification for the approach to

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 8 / 10
		GDA-REC-GNS-005202	

separation and segregation of I&C systems which are addressed in actions 1-4. This will include justification of the independence between those I&C systems that initiate faults and all I&C systems providing protection for those faults.

Impact on the GDA Submissions

The submissions that are impacted by this resolution plan include:

- *Independence analysis of I&C systems*
- *Optioneering Analysis Report for CIM Improvement*
- *Component Interface Module (CIM) Requirement Specification*
- *Optioneering Analysis Report for SPM Improvement*
- *Signal Pre-processing Module (SPM) Requirement Specification*
- *BSC of Overall I&C Architecture*
- *BSC of Protection System*
- *Pre-Construction Safety Report Chapter 8 Instrumentation and Control*

Timetable and Milestone Programme Leading to the Deliverables

See attached Gantt Chart in APPENDIX A.

Reference

- [1] ONR, Safety Assessment Principles, Revision 0, November 2014.
- [2] IEC, Nuclear power plants - Instrumentation and Control Important to Safety - General Requirement for Systems, IEC 61513, 2011.
- [3] IEC, Nuclear power plants - Instrumentation and Control Important to Safety - Separation, IEC 60709, 2004
- [4] IEC, Nuclear power plants - Instrumentation and Control Important to Safety - Requirements for Coping With Common Cause Failure (CCF), IEC 62340, 2007
- [5] CGN, Component Interface Module (CIM) Requirement Specification, GHX06002027DIYK03GN, Revision B, August 2019.
- [6] IAEA, Design of Instrumentation and Control Systems for Nuclear Power Plants, SSG-39, 2016.
- [7] CGN, BSC of Overall I&C Architecture, GHX06002001DIYK01GN, Revision C, May 2019
- [8] CGN, BSC of Protection System, GHX06002002DIYK03GN, Revision B, April 2019

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017	Rev.: 0	Page: 9 / 10
		GDA-REC-GNS-005202	

PREVIOUS REVISIONS RECORD

Rev.	Author	Scope/Reason of Revision	Date	Page

 <p>General Nuclear System</p>	<p>REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0017</p>	Rev.: 0	Page: 10 / 10
		GDA-REC-GNS-005202	

APPENDIX A RO-UKHPR1000-0017 Gantt Chart

Tasks	Steps	2019			2020												2021		
		Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
RO Action 1																			
Deliverable: Independence analysis of I&C systems, Rev B	Development																		
	Submission																		
RO Action 2																			
Deliverable: Optioneering Analysis Report for CIM Improvement, Rev A	Development																		
	Submission																		
RO Action 3																			
Deliverable: Optioneering Analysis Report for SPM Improvement, Rev A	Development																		
	Submission																		
RO Action 4																			
Deliverable 1: BSC of Overall I&C Architecture, Rev D	Development																		
	Submission																		
Deliverable 2: Independence analysis of I&C systems, Rev C	Development																		
	Submission																		
RO Action 5																			
Deliverable 1: BSC of Overall I&C Architecture, Rev D	Development																		
	Submission																		
Deliverable 2: BSC of Protection System, Rev C	Development																		
	Submission																		
Regulator assessment																			
Target RO closure Date																			