REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0017
Revision:	0
Date sent:	20/09/19
Acknowledgement required by:	11/10/19
Agreement of Resolution Plan Required by:	31/10/19
TRIM Ref:	2019/206775
Related RQ / RO No. and TRIM Ref: (if any)**:**	
Observation title:	Demonstration of independence between C&I systems
Lead technical topic: 3. Control & Instrumentation	**Related technical topic(s):** 2. Civil Engineering 7. Electrical Engineering 9. Fault Studies 12. Internal Hazards 14. Mechanical Engineering 15. Probabilistic Safety Analysis

Regulatory Observation

Background

A key expectation in the UK is that nuclear facilities should be designed so that defence in depth against potentially significant faults or failures is achieved through the provision of multiple independent barriers to fault progression. The overall control and instrumentation (C&I) architecture should incorporate independence between C&I systems, in support of the plant's approach to the concepts of defence in depth and diversity. Defence in depth within the overall C&I architecture should be achieved by multiple independent lines of defence such that failure of one system or component does not lead to the loss of multiple layers of defence.

The requesting party has submitted a number of documents whose purpose is to demonstrate that the independence, diversity and defence in depth implemented in the UK HPR1000 C&I architecture [Refs. 2 – 6] are adequate. While ONR's assessment of these submissions has found that the defence-in-depth model is broadly aligned to ONR's regulatory expectations (for example as defined in safety assessment principle (SAP) EKP.3 [Ref. 1]), a number of potential shortfalls have been identified which present a risk that common-cause failure (CCF) could simultaneously affect multiple systems across different levels of defence in depth, thus compromising the safety case claims and arguments regarding independence and defence in depth. From the evidence sampled to date, the following issues have been identified:

- Sensors and actuators are shared between the reactor protection system (RPS [PS]) and diverse actuation system (KDS [DAS]).
- Support systems (including but not limited to electrical systems and heating, ventilation and air conditioning (HVAC) systems) are common between C&I systems at different levels of defence in depth.
- Some measurement signals are shared by both the control system (PSAS) and the RPS [PS].
- The signal pre-processing module (SPM) acts as a common interface between all centralised C&I systems (ie the RPS [PS], KDS [DAS], PSAS, safety automation system (SAS) and severe accident system (KDA [SA I&C])) for distribution of output signals.

- The component interface module (CIM) acts as a common interface point, carrying out signal prioritisation and arbitration for all centralised C&I systems (ie the RPS [PS], KDS [DAS], PSAS, SAS and the KDA [SA I&C]).

- The RPS [PS] and KDS [DAS] are not physically separated and are therefore potentially vulnerable to internal hazards such as fire, flood, etc.

- There is no physical separation of cabling between C&I systems within the same division.

The submissions received to date do not provide adequate justification as to why the issues outlined above are acceptable, and how the independence between systems in the UK HPR1000 C&I architecture reduces the risk of common-cause failures affecting multiple systems as low as reasonably practicable (ALARP).

The issues identified above do not meet UK regulatory expectations and are considered to be a potential shortfall. This RO has therefore been raised to address these gaps and to confirm:

- that the UK HPR1000 C&I architecture will meet UK regulatory expectations in terms of independence and defence in depth;

- that the safety case provides suitable and sufficient justification that the levels of defence in depth and independence between C&I systems is adequate; and

- that the risk of CCF affecting multiple systems simultaneously is reduced ALARP.

Relevant Legislation, Standards and Guidance

There are a number of safety assessment principles (SAPs) [Ref. 7] that define expectations for the independence of C&I systems important to safety. These SAPs are identified below.

EKP.3 – Defence in depth
Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.

EDR.2 – Redundancy, diversity and segregation
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.

EDR.3 – Common cause failure
Common cause failure should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.

SAPs paragraph 187 supports SAP EDR.3 and is of particular relevance to this RO:
Where required reliabilities cannot be achieved due to CCF considerations, the safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.

EDR.4 – Single Failure Criterion
During any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.

SAPs paragraph 189 supports SAP EDR.4 and states expectations for applicability of the single failure criterion:
A system that is the principle means of fulfilling a Category A safety function should, other than in exceptional circumstances, always be designed to meet the single failure criterion. However, other systems which make a contribution to fulfilling the same safety function, but are independent of the principal system, do not necessarily need to meet the single failure criterion.

ESS.10 – Definition of Capability
The capability of a safety system, and of each of its constituent sub-systems and components, should be defined and substantiated.

ESS.11 – Demonstration of adequacy
The adequacy of the system to achieve its specified functions and reliabilities should be demonstrated for each safety system.

ESS.18 – Failure independence
No design basis event should disable a safety system.

SAPs paragraph 413 supports SAP ESS.18 and is of particular relevance to this RO:
Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.

ESS.20 – Avoidance of connections to other systems
Connections between any part of a safety systems and a system external to the facility (other than to safety system support and monitoring features) should be avoided.

ESS.21 – Reliability
The design of safety systems should avoid complexity, apply a failsafe approach and incorporate means of revealing internal faults at the time of their occurrence.

EES.5 – Cross-connections to other services
The ability of the essential services to meet the demands of the safety function(s) they support should not be undermined by making cross-connections to services provided for safety functions of a lower category.

A number of international standards also specify requirements and expectations with respect to independence. Of particular relevance are the following standards:

IAEA SSG-39 [Ref. 8] – in particular clauses 4.14 – 4.24 on independence, and clauses 4.25 – 4.35 on consideration of common cause failure.

IAEA NP-T-2.11 [Ref. 9] with regard to overall principles to be adopted in the C&I architecture design, including independence between lines of defence and interconnections of systems of different classes.

IEC 61513 [Ref. 10] – in particular clauses 5.2.2, 5.4.2.2, 5.4.2.6, 6.2.2.3.2 and 6.2.3.3.3.

IEC 60709 [Ref. 11] with regard to requirements for separation of C&I systems as a means to achieve independence. Of particular significance are section 5.4 on the independence of safety systems from control systems, and section 6 on requirements for separation of cabling.

Further guidance on the expectations of a number of international regulators with regard to independence can be found in the following MDEP common position documents:

MDEP Common Position No DICWG-09 [12] - Common Position On Safety Design Principles And Supporting Information For The Overall I&C Architecture

MDEP Generic Common Position No DICWG04 [13] - Common Position On Principle On Data Communication Independence

Regulatory Expectations

ONR expectations are for the design of the UK HPR1000 C&I architecture to meet regulatory expectations and relevant good practice, and that the safety case provides a suitable and sufficient justification that the design reduces risks ALARP with respect to the following:

- The independence of systems at different levels of defence in depth, such that a postulated failure of one system does not prevent other systems from correctly performing their safety function(s);
- The independence of systems across divisions, such that the risk of failures simultaneously affecting multiple divisions within a C&I system is reduced ALARP.

- Prevention of failure propagation from systems affecting other systems important to safety (for example failure of the primary protection system should not adversely affect the performance of the diverse protection system);
- Prevention of failure propagation between redundant divisions of systems;
- Delivery of safety functions not being compromised by the occurrence of the postulated initiating events for which they are required to function; and
- Prevention of common cause failures between layers of defence due to common internal plant hazards.

References

[1] HPR-GDA-PCSR-0008 - Pre Construction Safety Report - Chapter 08 - Instrumentation and Control - 2 October 2018 – CM9 2018/318229
[2] GDA-REC-CGN-003694 - Comparison of UK HPR1000 Overall I&C Architecture with IEC 61513 - 30 January 2019 – CM9 2019/27419
[3] GDA-REC-CGN-003695 - Defence in Depth and Diversity Analysis Report - 30 January 2019 – CM9 2019/27428
[4] GDA-REC-CGN-003697 - Independence Analysis of I&C Systems - 30 January 2019 – CM9 2019/27469
[5] GHX06002001DIYK01GN – Basis of Safety Case of Overall I&C Architecture – 20 May 2019 – CM9 2019/152717
[6] GHX00630003DIYK03GN – SAPS Conformance Assessment of I&C Systems Design – 20 May 2019 – 2019/152735
[7] ONR Safety Assessment Principles – Rev 0, 2014
[8] IAEA-SSG39 – Design of Instrumentation and Control Systems for Nuclear Power Plants
[9] IAEA NP-T-2.11 – Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants
[10] IEC 61513 – Nuclear power plants – Instrumentation and control important to safety – General Requirements for Safety
[11] IEC 60709 – Nuclear power plants – Instrumentation and control important to safety – Separation
[12] MDEP Common Position No DICWG-09 - Common Position On Safety Design Principles And Supporting Information For The Overall I&C Architecture
[13] MDEP Generic Common Position No DICWG04 - Common Position On Principle On Data Communication Independence

Regulatory Observation Actions

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

In response to this Regulatory Observation Action, GNS 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 componenents 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 required by '*to be determined by General Nuclear System Resolution Plan*'

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

In response to this Regulatory Observation Action, GNS 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 required by '*to be determined by General Nuclear System Resolution Plan*'

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

In response to this Regulatory Observation Action, GNS 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 required by '*to be determined by General Nuclear System Resolution Plan*'

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

In response to this Regulatory Observation Action, GNS 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 required by '*to be determined by General Nuclear System Resolution Plan*'

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

In response to this Regulatory Observation Action, GNS 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, seperation 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 required by '*to be determined by General Nuclear System Resolution Plan*'**	
REQUESTING PARTY TO COMPLETE	
Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	