REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-UKHPR1000-0001
Revision:	Rev 1
Date sent:	13/11/18
Acknowledgement required by:	04/12/18
Agreement of Resolution Plan Required by:	08/01/19
TRIM Ref:	2018/35038
Related RQ / RO No. and TRIM Ref: (if any)**:**	
Observation title:	Diverse Actuation System Design Shortfalls
Lead technical topic: 3. Control & Instrumentation	**Related technical topic(s):** 7. Electrical Engineering 9. Fault Studies 12. Internal Hazards 15. Probabilistic Safety Analysis 18. Security

Regulatory Observation

Background

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. Within the UK two C&I systems perform these functions – a Primary Protection System (PPS) backed up by a second system known as a Diverse Actuation System (DAS) or Secondary Protection System (SPS).

In line with ONR SAPs [1] and Relevant Good Practice as defined by international standards [e.g. 2], the implementation platforms for the PPS and DAS/SPS are of diverse design. The PPS is typically implemented using software-based/microprocessor technology and the DAS/SPS is implemented using simple electronic hardware-based technology. In those designs which are operational or which have received a Design Acceptance Certificate (DAC) [8, 9, 10] the PPS is a Class 1 system which meets the single failure criterion, and the DAS is a Class 2 (or Class 1) system. For some designs, a DAS may also meet the single failure criterion and/or other relevant engineering principles (e.g. failure to safety).

The UK HPR1000 Preliminary Safety Report [4] and information presented by GNS at Level 4 meetings [Refs 5, 6] have described a UK HPR1000 DAS/SPS with the following characteristics:

1) Designed to address Nuclear C&I Class 3 requirements
2) A system not designed to meet the single failure criterion
3) A system platform based on complex programmable hardware

These aspects of the design do not meet UK regulatory expectations, and relevant good practice, and are considered to be a significant shortfall. This RO has therefore been raised to ensure that these gaps are resolved in a satisfactory and timely manner for UK HPR1000 GDA.

Relevant Legislation, Standards and Guidance

The following SAPS [1] are of particular relevance to this RO:

- EKP.2 Fault tolerance
- ESP.3 Defence in depth
- ECS.2 Safety classification of structures, systems and components
- EDR.1 Failure to Safety
- EDR.3 Common Cause Failure
- EDR.4 Single failure criterion
- ESS.1 Provision of safety systems
- ESS.18 Failure independence
- ESS.21 Reliability
- ESS.27 Computer-based safety systems

In addition, the following international standards are of particular relevance:

- IAEA-SSG39 – Design of instrumentation and control systems for nuclear power plants [7]

- IEC 61513 – Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems [2]

- IEC61226 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions [3]

The above references provide detailed principles and guidance covering categorisation, single failure tolerance and common cause failure. Of particular note is IEC 61226, which states that backup protection functions (such as those allocated to a DAS/SPS) should be Category B, and IEC61513 which assigns a Class 2 allocation to systems performing Category B functions.

Regulatory Expectations

In summary, ONR expectations are for the UK HPR1000 DAS/SPS design and safety case to provide a suitable and sufficient justification that ONR expectations and relevant good practice can be satisfied regarding –

i) DAS/SPS classification
ii) DAS/SPS ability to meet relevant good practice with respect to the single failure criterion
iii) DAS/SPS implementation technology, to include consideration of failure to safety, diversity and CCF

References

[1] ONR Safety Assessment Principles – Rev 0, 2014

[2] IEC 61513 - Nuclear power plants – Instrumentation and control important to safety – General Requirements for Safety

[3] IEC61226 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

[4] PSR - HPR-GDA-PSR-0007 Preliminary Safety Report

[5] Contact Record ONR- NR-CR-17-327

[6] Contact Record ONR-NR-CR-17-485

[7] IAEA-SSG39 - Design of Instrumentation and Control Systems for Nuclear Power Plants

[8] EPR Step 4 C&I Report
http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ukepr-ci-onr-gda-ar-11-022-r-rev-0.pdf

[9] AP1000 Step 4 C&I Report
http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf

[10] ABWR Step 4 C&I Report
http://www.onr.org.uk/new-reactors/uk-abwr/reports/step4/onr-nr-ar-17-017.pdf

RO-UKHPR1000-0001.A1 – DAS/SPS Classification

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.

RO-UKHPR1000-0001.A2 – DAS/SPS Single Failure Criterion

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)..

RO-UKHPR1000-0001.A3 – DAS/SPS Implementation Technology

In response to this Regulatory Observation Action, GNS should:

Taking into account:

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

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

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:	