BWRX-300 UK Generic Design Assessment
Response to Regulatory Observation (RO)

REGULATORY OBSERVATION Resolution Plan	
RO Unique No.:	BWRX300-001
RO- Title:	Demonstration of independence and diversity in the BWRX-300 I&C Architecture
Technical Area(s)	Instrumentation & Control
Revision:	0
Overall RO Closure Date (Planned):	October 30, 2026
Linked RQ(s)	RQ-01743 RQ-01756 RQ-01903 RQ-01961
Linked RO(s)	N/A
Related Technical Area(s)	Security Fault Studies PSA
Other Related Documentation	N/A

Scope of Work

Background

The GE-Hitachi Nuclear Energy International LLC (GEH) BWRX-300 SMR design has adopted a plant level defence-in-depth concept comprising several defence lines (DL) and claimed independence and diversity between DL3 and DL2 systems, and between DL3 and DL4a systems to defend against common cause failures (CCFs).

As stated in the RO from ONR, the submissions received from GEH and discussions held to date during GDA Step 2 have not provided sufficient confidence to the Office for Nuclear Regulation (ONR) that GEH has considered all credible options for the technology selection of the Diverse Protection System. In addition, the ONR has stated it does not see a clear plan to ensure the BWRX-300 Instrumentation and Control (I&C) design develops the claims of independence and diversity will be met.

The ONR have consequently outlined four actions in RO-BWRX300-001 which seek to provide further confidence to ONR. This resolution plan outlines how GEH intend to respond to these actions and the information provided as part of completion of the resolution plan will be assessed by ONR to close out the Regulatory Observation (RO).

Scope of Work

To address this RO, the RP will perform the following:

- *Delivery plan encompassing the resolution plan items specified in Action 1 for Actions 2, 3, and 4.*
- *The delivery method for Actions 2, 3 and 4 will be detailed in the delivery plan.*

Deliverable Description
RO-BWRX300-001 – ACTION 1 – Provide a delivery plan In response to this RO Action, the RP should: Provide a delivery plan, supporting the RO Resolution Plan, which provides further details as to how the RP intends to satisfy the objectives of each RO action. Regulatory Expectations In response to this Action, we are seeking further detail beyond that which is provided in the RO Resolution Plan which explains how the RP intends to address each RO Action. The intent is for this plan to be shared with ONR within GDA Step 2, such that the RP and ONR can share confidence that the activities defined will successfully achieve the relevant objectives. Our expectation is that a response to this Action should consider the following aspects, amongst any other matters considered relevant by the RP: • the activities necessary, • the scope of the activities and which I&C systems are considered, • the standards and guidance which will be applied, • the timing of each activity in relation to design baselines and other key engineering milestones, • any criteria that will be used to inform the design and the RP's "success criteria". The term "delivery plan" is used here as a general term to refer to more detailed planning. The RP may determine the most appropriate form to capture this planning and provide it to ONR, be it a separate detailed delivery plan, one or a series of Forward Action Plans, or another format. **Resolution Plan for RO-BWRX300-001.A1** In response to RO Action 1 (A1), the RP will produce a "delivery plan". For each action (A2, A3 and A4) the delivery plan will consider: • The objective, scope (including specific I&C systems) • Proposed solutions • Key activities, tasks, timeline, and associated design baselines • Delivery strategy (method and approach) with success criteria • Applicable codes and standards The RP expects to perform A1 within the scope of Step 2 GDA timescales to support ONR's I&C assessment report forecasted September 2025.

RO-BWRX300-001 - ACTION 2 – Diversity attributes supporting independence claims within the I&C architecture

In response to this RO Action, the RP should:

Capture in an appropriate report how the BWRX-300 I&C architecture incorporates specific diversity attributes, resulting in identifiable design decisions and features, which allow a credible demonstration to be made that the nuclear safety risks arising from CCF as a result of loss of independence between I&C systems have been reduced, so far as is reasonably practicable. This report should show how these attributes, decisions and features will be supported by claims and arguments in a future safety case.

Regulatory Expectations

In response to this Action, we are seeking clarity as to how the RP intends to identify and establish the sufficiency of the attributes, design decisions and features which support the overarching design goal of diversity, such that there is earlier confidence that the final confirmatory diversity analysis which the RP intends to perform at a later design stage is likely to be successful.

ONRs expectation is for a deterministic approach to be taken, identifying potential CCFs and specific design features (e.g. simplicity, technology choices, architectural choices) which eliminate these where possible, or where this is not possible, to demonstrate that it is not reasonably practicable to introduce features to reduce risks further. Whilst we are not seeking the full demonstration at GDA Step 2, I was seeking to understand the overarching approach and the considerations informing I&C architecture decisions.

Our expectation is that a response to this Action should consider the following aspects, amongst any other matters considered relevant by the RP:

- The high-level identification and grouping of potential CCFs which may affect multiple I&C systems claimed to be independent and diverse.
- What attributes, design decisions and features, including types of diversity, are credited to reduce or mitigate the CCFs identified to a level which supports a claim of independence.
- The combined effectiveness of the measures identified, including the effectiveness of the method chosen to deliver any particular type of diversity, and why this is sufficient in the context of the CCF against which they are credited.
- What sources of evidence are available to underpin these decisions and what assumptions have been made.
- What industry standards and guidance are available and relevant, and how these are applied.

Resolution Plan for RO-BWRX300-001.A2

In response to RO Action 2 (A2), the RP will cover the following topics in a format detailed within the delivery plan as outlined in RO-BWRX300-001.A1

The topics considered are:

- The high-level identification and grouping of potential CCFs that may affect multiple I&C systems claimed to be independent and diverse.
- The attributes, design decisions, and features, including types of diversity, credited to reduce or mitigate the identified CCFs to a level where I&C system independence will reduce risks SFAIRP (So Far As Is Reasonably Practicable).
- The combined effectiveness of the measures identified, including the effectiveness of the method chosen to deliver any particular type of diversity, and why this is sufficient in the context of the CCF against which they are credited.
- Sources of evidence to underpin these decisions
- Assumptions that have been made.
- Applicable codes and standards

RO-BWRX300-001 – ACTION 3 – Cybersecurity supporting independence within the I&C architecture

In response to this RO Action, the RP should:

Capture in an appropriate report the activities and assessments which will result in identifiable design decisions and features which support a credible demonstration to be made that the nuclear safety risks arising from common cyber security vulnerabilities undermining independence between I&C systems have been adequately mitigated.

Regulatory Expectations

In response to this Action, we are seeking clarity as to how the RP intends to apply SbD principles to identify and establish the sufficiency of features and measures which support a credible demonstration that any common cybersecurity vulnerabilities in the I&C architecture are removed or mitigated such that they cannot undermine the overarching design goal of independence. The intent is to provide early confidence that the final verification and validation activities, which the RP intends to perform at a later design stage to confirm cybersecurity requirements are met, are likely to be successful. Whilst we are not seeking the full demonstration at GDA Step 2, I was seeking to understand the overarching approach and the considerations informing I&C architecture decisions.

Our expectation is that a response to this Action should consider the following aspects, amongst any other matters considered relevant by the RP:

- The threat capabilities described within the UK DBT.
- The outcomes set out in the SyAPs and SyAPs Annexes.
- The cybersecurity activities and assessments which contribute to the demonstration of independence.
- The high-level identification and grouping of potential common cybersecurity vulnerabilities which may affect multiple I&C systems claimed to be independent and diverse.
- The design choices and features of the I&C architecture provided for safety purposes and their effectiveness in relation to the common cyber-security vulnerabilities identified.
- Any additional measures, beyond that already required for nuclear safety purposes, which are credited to remove or mitigate common cyber-security vulnerabilities identified to a level to support a claim of independence.
- The combined effectiveness of the measures in the context of the common cybersecurity vulnerability against which they are credited.
- What sources of evidence are available and what assumptions have been made.
- What industry standards and guidance are available and relevant, and how these are applied.

Resolution Plan for RO-BWRX300-001.A3

In response to RO Action 3 (A3), the RP sets out how Secure by Design (SbD) principles are being applied to identify and establish the sufficiency of features and measures which support a credible demonstration that common cybersecurity vulnerabilities within the I&C architecture and inter-connected systems are either removed or mitigated so as not to compromise the overarching design goal of independence and diversity.
The RP adopts a cross-disciplinary approach to achieve this, ensuring the integration of cybersecurity into the design and layout of the BWRX-300. This approach is informed by the "threat–design–outcome" relationship and includes identifying and crediting inherent security benefits across plant systems, broader network architecture and design, and passive safety systems, while managing conflicting requirements.
Secure by Design is applied pragmatically. Where practicable, risks are designed out. Where elimination is not practicable, the design incorporates cybersecurity controls to mitigate the associated risks. This approach is supported by progressive and repeatable formal design reviews that will continue throughout the design maturity lifecycle covering country or site-specific detailed design, construction, commissioning, and operations. Further detail on the RP's SbD implementation is provided in Section 25.1 of Chapter 25, Rev B (NEDC-34197P).

Alignment with the UK DBT and ONR SyAPs

The RP has referenced, within the Forward Action Plan (NEDC-34274P, Rev 2) Action PSR25-403, that the Licensee/DevCo responsible for the UK detailed design beyond GDA Step 2 must ensure cybersecurity defences are aligned with the UK DBT and ONR SyAPs SNI

Annexes (Annex H to J Tables). This alignment ensures that common cybersecurity vulnerabilities are identified and addressed appropriately within the I&C plant design.

Cybersecurity Activities and Assessment

Cyber security activities and assessments supporting the demonstration of independence including high-level identification and grouping of vulnerabilities across independent and diverse I&C system, the RP outlines its methodology in Chapter 25 (NEDC-34197P), Section 25.9.1.
The Cyber Security Program Plan (CSyPP) describes how systems are identified and classified, and how cybersecurity controls are applied based on a cyber risk assessment methodology. This methodology encompasses both digital and non-digital systems and the assessment process is based on NUREG CR-6847, which complies with CSA, NEI, and specified IEC standards as defined in the process documentation. Assessments have been completed and submitted previously to ONR for review which show evidence for the process as described. Noted in the Forward Action Plan (NEDC-34274P Rev 2), PSR25-343.
For activities beyond GDA Step 2, the Licensee/DevCo will continue to evolve this approach through the Cyber Security Assessment Process (CSyAP) and the Defensive Cyber Security Architecture (DCSA) by aligning to a relevant international standard for OT cyber security such as the IEC 62443 series, and industry best practice guidance from NIST CSF 2.0 or NIST SP 800-82 ensure independence of systems. These frameworks will support refinement of system interoperability requirements, including interfaces between I&C platforms, while ensuring SbD, independence and diversity principles remain integral across the development lifecycle. Detailed information on how this will be achieved, will be captured in the future delivery plan.

Design Features and Future Enhancements

To address common cybersecurity vulnerabilities within the I&C architecture, the RP is planning a revision to the Defensive Cyber Security Architecture document (007N5118 r0). This updated version will include enhanced guidance on common-cause cybersecurity failures and align with the provisions of IEC 62859 Section 5.3.
As noted within Chapter 25 Section 25.9.5, the I&C network architecture is based on recognized good practice from IEC 61513:2011 and IEC 62859, to enhance the I&C architecture features to mitigate common cyber-security vulnerabilities identified. The Forward Action Plan (NEDC-34274P, Rev 2) PSR25-343, PSR25-401 & PSR25-402 notes future actions to be undertaken beyond GDA Step 2 by the future Licensee/DevCo such as the revision of the I&C architecture, enhancement to role-based access control and other controls to mitigate common cyber security vulnerabilities.

The collective actions noted above and detailed within the delivery plan, would be adopted by a future licensee or DevCo beyond GDA Step 2 and integrated with UK specific or site-specific activities with the aim to ensure system interoperability, independence and diversity, reinforcing SbD to meet UK specific threats and mitigation or removal of common cyber security vulnerabilities without adversely impacting fundamental operations.

RO-BWRX300-001 – ACTION 4 – Justification of I&C technology selection
In response to this RO Action, the RP should:

Capture in an appropriate report a suitable and sufficient justification for the technology type(s) selected for the I&C systems within the BWRX-300 I&C architecture with a view that this will support claims and arguments in a future safety and security case.

Regulatory Expectations

Our expectation is that a response to this action should consider the following aspects, amongst any other matters considered relevant by the RP:

- The potential technology options available to support the delivery of I&C safety functions.
- The criteria that inform the selection of platform technologies and their relative importance to safety and security should be set out and justified. It should be noted that some criteria may have commercial impact which may be relevant to note but are not expected to be priority criteria informing decision making.
- The outcome of any further assessment or characterisation of potential CCFs and common cybersecurity vulnerabilities (e.g., arising from Action 2 or Action 3).
- The evidence and assumptions which have been used to inform decision making. Where assumptions or approximate calculations are made, it should be clear as to their basis.
- Where any particular criteria are shown to dominate decision making, consideration should be made as to whether this is appropriate.
- Deterministic claims of independence and diversity arising from the BWRX-300 Safety Strategy.
- Relevant good practice and OPEX regarding the potential vulnerability to CCF of digital technology and the potential for common cybersecurity vulnerabilities.
- The ability to deterministically demonstrate resistance to common hazards and failure types.
- The ability to deterministically demonstrate the absence of, or sufficient mitigation of, common cybersecurity vulnerabilities such that reasonably foreseeable cyber-security risks do not compromise safety case claims of independence.

Resolution Plan for RO-BWRX300-001.A4

In response to RO Action 4 (A4), the RP will cover the following topics in a format detailed within the delivery plan as outlined in RO-BWRX300-001.A1.

The topics considered are:

• The technology options • The technology selection criteria, their relative importance to safety and security and justification • Where relevant, the effect of the outcomes from A.2 and/or A.3 • The basis of any evidence and assumptions made to inform the decision making • Justification of any overwhelming decision-making criteria • Linkage to the claims of independence and diversity from the Safety Strategy • Use of codes, standards and guidance relating to the vulnerability of digital technology to CCFs • Use of codes, standards and guidance relating to common cybersecurity vulnerabilities • Analysis of the I&C systems resistance to common hazards and failures, • Analyse the absence or sufficient mitigation of common cybersecurity vulnerabilities within I&C architecture and systems.
Impact on GDA submissions
None
Timetable and Milestone Programme Leading to the Deliverables
The RP expects to perform A2-A4 after GDA Step 2 with the specific timescales and detailed delivery information outlined in the delivery plan specified in RO-BWRX300-001.A1. A2-A4 are intended to be completed in time to support the site-specific pre-construction safety report (ssPCSR). See Appendix A
References
N/A

Appendix A: RO-BWRX300-001 Schedule

Activities	Steps	2025							2026									
		June	July	August	September	October	November	December	January	February	March	April	May	June	July	August	September	October
ONR Issue RO																		
RP Acknowledgement of RO																		
Issuance of Resolution Plan																		
RO Action 1																		
Deliverable: Delivery Plan for Actions 2, 3, & 4	Production																	
	Submission																	
RO Action 2*																		
Deliverable: To be detailed in the delivery plan	Production																	
	Submission																	
RO Action 3*																		
Deliverable: To be detailed in the delivery plan	Production																	
	Submission																	
RO Action 4*																		
Deliverable: To be detailed in the delivery plan	Production																	
	Submission																	
ONR Assessment Report																		
Target RO Closure Date																		

***Note:** Actions 2-4 delivery timescales are only estimates and may be superseded by timescales given within the delivery plan.