|  |  |  |
| --- | --- | --- |
| **GDA Regulatory Observation** | | |
| **REGULATOR TO COMPLETE** | | |
| **RO unique no.:** | RO-BWRX300-001 | |
| **Revision:** | 1.0 | |
| **Date sent:** | 20 June 2025 | |
| **Acknowledgement required by:** | 11 July 2025 | |
| **Resolution Plan Agreement Required by:** | 8 August 2025 | |
| **Record Reference:** | ONRW-2126615823-7689 | |
| **Related RQ / RO No. and CM9 Ref:** (if any)**:** | RQ-01743  RQ-01756  RQ-01903  RQ-01961 | |
| **Observation title:** | Demonstration of independence and diversity in the BWRX-300 I&C architecture | |
| **Lead technical topic:**  Control & Instrumentation | **Related technical topic(s):**  Security  Fault studies  PSA | |
| **REGULATORY OBSERVATION:** | | |
| This regulatory observation (RO) does not contain any export-controlled information.  **Background**  GE-Hitachi Nuclear Energy International LLC (UK Branch), the requesting party (RP) for the BWRX-300 Generic Design Assessment (GDA), has adopted a plant level defence-in-depth concept comprising several defence lines (DL) and claimed independence[[1]](#footnote-2) and diversity[[2]](#footnote-3) between DL3 and DL2 systems and between DL3 and DL4a systems to defend against common cause failures[[3]](#footnote-4) (CCF) (ref. ‎[1]). The RP has presented an instrumentation and control (I&C) architecture aligned with the defence-in-depth concept, including (ref. ‎[2]):   * A Safety Class (SC) 1 C10 Primary Protection System (PPS) in DL3, * A SC2 C20 Diverse Protection System (DPS) in DL4a, * SC3 systems in DL2, such as C30 Anticipatory Protection System (APS) and C31 Reactor Control System (RCS).   The RP initially considered using hardwired analogue technology for the C20 DPS (ref. ‎[3], for information). However, as the BWRX-300 I&C continued to develop, the concept of the C20 DPS evolved to use a diverse digital platform. The RP has described the decision making to adopt digital technology over hardwired technology in the response to RQ-01756 (ref. ‎[4]). The RP identified a variety of constraints of analogue hardwired technology, such as physical space, power consumption, and heat loading, which led the RP to conclude that digital technology was preferable. Consequently, PSR Chapter 7 (ref. ‎[2]) describes an all-digital I&C architecture. The specific digital technologies considered for use within C10 PPS and C20 DPS are described in more detail in the RP’s response to RQ-01743 (ref. ‎[5]), making use of a mixture of different digital technologies, such as microprocessors and hardware description language (HDL) programmed devices (HPD), within each system.  Independence between systems, components or channels can be undermined by common dependencies resulting in potential for CCFs. Factors affecting and compromising independence can include the conceptual design, programming languages, practice, coding style, tools used for implementation and physical separation (ref. ‎[7]). Diversity supports claims of independence by ensuring systems and components have different attributes to reduce the possibility of CCF. Independence can also be undermined by common cybersecurity vulnerabilities. Secure by design (SbD) is an important principle ensuring security and safety are well integrated and seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design.  Relevant good practice (RGP) is a UK regulatory concept used to reduce the time and effort in commonly-encountered circumstances where there is well-established good practice and where a detailed, first-principles demonstration that risks have been reduced as low as reasonably practicable (ALARP) is not needed (ref. ‎[8]). Dutyholders (and RPs) are free to choose an alternative approach to RGP, providing they have satisfied the legal requirement of reducing the risk to ALARP (ref. ‎[8]). The RGP I consider relevant to this RO is set out in the relevant legislation, standards and guidance section.  All nuclear reactors currently operating or under construction in the UK have two independent protection systems, a main or primary protection system and a diverse protection system. This is necessary to ensure that adequate levels of risk control are achieved for these designs, reflecting the consequences of failure. For these designs, a non-software-based line of defence makes a significant contribution to the demonstration of adequate independence and diversity. In addition, ONR has assessed a number of reactor designs through previous GDAs (ref. ‎[9], ‎[10], ‎[11], ‎[12]). In each GDA, the reactor vendor analysed the options and changed the design to select a software-based primary protection system and a non-software-based diverse protection system.  While a non-software-based line of defence has been a key aspect of demonstrations of independence between I&C protection systems for existing or under-construction UK nuclear power stations, new reactor designs may place different demands on I&C based protection systems depending on the reactor technology and specific implementation. The RP is currently pursuing an approach using all-digital I&C protection systems, and therefore this RO seeks further clarity as to how the RP intends to demonstrate an adequate level of risk control for CCFs between the PPS and DPS, and that a case can be made in the future that the risks arising from the RP’s proposed approach are reduced so far as is reasonably practicable.  In response to RQ-01961 (ref. ‎[13]), the RP has described how the adequacy of diversity is assessed. The RP has used the semi-quantitative scoring methodology described in NUREG/CR-7007 (ref. ‎[14]) as an indication that the C20 DPS platform is adequately diverse from the C10 PPS platform (ref. ‎[15]). A final diversity assessment of the SC1 C10 PPS, SC2 C20 DPS and SC3 systems in DL2 will be performed at a later design stage in accordance with the I&C failure mode and hazards analyses (FMHA) plan (ref. ‎[16]).  The RP presents cybersecurity aspects of the security case within PSR Chapter 25 (ref. ‎[17]), which is undergoing assessment at GDA Step 2 led by ONR’s cybersecurity assessor. The RP describes the integration of cybersecurity with the I&C design lifecycle in PSR Chapter 7 (ref. ‎[2]). In the response to RQ-01903 (ref. ‎[18]), the RP explained how a preliminary cyber security assessment was produced for the digital DPS platform (provided for information (ref. ‎[19])) after the evolution from an analogue to digital platform. The RP also explained that the verification and validation steps applied at a later design stage would ensure that all requirements are achieved, including cybersecurity and diversity requirements.  From the submissions received and discussions held to date during GDA step 2, I consider that the RP might be downselecting credible options before it has demonstrated its preferred design solution can achieve the relevant safety and security expectations. In addition, there does not appear to be a clear plan which ensures that the BWRX-300 I&C design develops in a way which ensures claims of independence and diversity will be met.  **Relevant Legislation, Standards and Guidance**  ONR publishes Safety Assessment Principles (SAPs) (ref. ‎[20]) and Security Assessment Principles (ref. ‎[21]) to assist inspectors in judging whether, in their opinion, the designer’s or dutyholder’s safety and security case has satisfactorily demonstrated that the requirements of the law can be or have been met. The principles are not intended to be a compliance checklist, and priority should be given to achieving an overall balance of safety and security. Notwithstanding this, the SAPs themselves should be met so far as is reasonably practicable. ONR also publishes a set of Technical Assessment Guides (TAGs) to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions. ONR’s SAPs and TAGs are goal setting in nature, with the overall objective of supporting inspectors to judge whether reducing risks to ALARP is achieved.  The following SAPs and TAGs are particularly relevant to the potential shortfalls described above:   * SAP SC.4 *Safety case characteristics* provides guidance that *“to demonstrate that risks have been reduced to ALARP, the safety case should:*  1. *identify and document all the options considered for risk prevention or reduction;* 2. *provide evidence justifying the criteria used in decision making or option selection;* 3. *justify the options chosen in terms of meeting relevant good practice, and discard any options as being either less effective than the chosen option(s) or grossly disproportionate.”*  * NS-TAST-GD-046 (TAG 46) (ref. ‎[22]) provides the following guidance:   + Paragraph 17 – *“Where diverse safety systems are required to implement category A safety functions and one is computer based, one of the other safety systems should be provided using a non-computer based system (EKP.3, EDR.2 and EDR.3).”*   + Paragraph 155 – *“Demonstrating that two complex computer based protection systems are "independent" and “diverse” (i.e. will not tend to fail on the same demands) and hence that the reliability claims for each can be multiplied together remains an open question despite significant research. Hence, where a high level of risk reduction is required that is greater than the accepted common cause cut-off limit for a single computer based safety system (i.e. 1 × 10-4 pfd for a computer based safety system where the consequence in the event of failure of the safety system could potentially involve large releases of radioactive material) then ONR’s current expectation is that a simple hardware based secondary safety system should be provided.”*   + Paragraph 156 – *“However, the use of two diverse computer based safety systems to implement a safety function requiring high reliability (e.g. such as a reactor protection system comprising primary and secondary systems) may be acceptable, provided the guidance in SAP ERL.1 paragraph 191 is followed.”* * SAP ERL.1 *Form of claims* provides guidance (paragraph 191) that “*where reliability data is unavailable, the demonstration should be based on a case-by-case analysis and include:*  1. *a comprehensive examination of all the relevant scientific and technical issues;* 2. *a review of precedents set under comparable circumstances in the past;* 3. *where warranted, e.g. for complex items, an independent third-party assessment; and* 4. *periodic review of further developments in technical information, precedent and relevant good practice.”*  * TAG 46 (ref. ‎[22]) paragraph 157 provides further guidance in relation to SAP ERL.1 – “*With regard to the implementation of SAP ERL.1 in the context of diverse computer based systems important to safety the case should include*:   + *application of relevant good design practice (e.g. functional and equipment diversity),*   + *adoption of appropriate nuclear standards (e.g. IAEA SSG-39, IEC 61513, IEC 60880, IEC 62138 and IEC 62340) for the production and assessment of diverse computer based systems,*   + *an independent assessment of all factors that could lead to common cause failure,*   + *examination and implementation of relevant research.”*   The following SyAP is also relevant to this RO:   * KSyPP.1 *Secure by design*, which outlines a hierarchy of controls (most effective listed first); elimination, substitution, passive engineering, active engineering, operational/human factors. * CNS-TAST-GD-11.4.1 *Secure By Design* (ref. ‎[23]) provides further guidance in relation to KSyPP1:   + Paragraph 23 – *“SyAPs describes SbD as an approach that seeks to reduce security vulnerabilities within a given design (a large project such as a new nuclear power plant or smaller one such as a new storage facility) rather than attempting to secure or mitigate them post design. Emphasis is placed upon eliminating or reducing risk to design out the requirement for protection measures. An RP, or later a dutyholder, has the flexibility on how they achieve security outcomes so to meet regulatory expectations. ONR should be prepared to assess all claims made by an RP, developer or dutyholder as to how risks are managed.”*   + Paragraph 30 – “*The expectation is that engineers and designers would understand the plant vulnerabilities and collectively seek engineering solutions to eliminate or reduce the risk. SyAPs refers to ‘inherent security’ that describes how safety measures may deliver security benefit or might be strengthened to reduce risk further. This might be referred to as designing-out security vulnerabilities and is the first part of any SbD approach.*”   The following SAPs are also generally relevant to this RO:   * EDR.2 Redundancy, diversity and segregation * EDR.3 Common cause failure * EKP.3 Defence in depth * ERC.2 Shutdown systems * ESS.1 Provision of safety systems * ESS.18 Failure independence * ESS.21 Reliability * ESS.27 Computer-based safety systems   The following guidance is relevant to the potential shortfalls described above:   * BS EN IEC 62859:2020 (ref. ‎[24]) 5.2 a) states, “*Cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realisation. It shall not compromise the effectiveness of the diversity and defence-in-depth features implemented by the I&C architecture*.” * BS EN IEC 62859:2020 (ref. ‎[24]) 5.2 e) states, “*When two architecture designs offer equivalent level of safety, priority should be given to the most secure one. Unnecessary complexity shall be avoided as it is detrimental to both safety and cybersecurity.”* * BS EN IEC 62859:2020 (ref. ‎[24]) 5.3.2 b) states, “*Any cybersecurity measures considered for inclusion in the design shall be assessed for their potential to introduce a fault leading to CCF between systems diversified for safety reasons. Where such risks are found, alternative means of achieving adequate cybersecurity shall be implemented as necessary.*” * Annex 3, of the Chief Nuclear Inspector’s annual report on Great Britain’s nuclear industry - October 2024 (ref. ‎[25]) includes a case study related to the EPR design in the UK and states *“truly diverse systems would use different development methods and technology. ONR advised that it would be challenging to justify that the original design was adequate to ensure the required levels of safety, and that using a different technology such as a hardwired back-up system had the potential to significantly reduce the risk of common cause failure. Hardwired systems are not computer-based, and therefore do not use software. They are a fundamentally diverse technology to software-based systems.”* * The ONR report, ONR’s Regulatory influence on the EPR Design in the UK (ref. ‎[26]), also refers to the hardwired backup in the design, stating *“In the decade since GDA, another significant benefit of the hardwired backup system has been realised. Hardwired systems are resilient to a cyber-attack and will prevent escalation of a fault in the unlikely event that the computer-based systems are compromised. This alone would be a compelling case for the system, given the elevated cyber threat levels today.”* * IAEA SSG-39 (ref. ‎[27]), paragraph 4.39 states, “*when diverse I&C systems are provided, the diverse systems should not be subject to the same errors in specification, design, fabrication or maintenance.*” * BS EN 62340:2010 (ref. ‎[28]) 7.1.2 states, “*The principle of independent I&C systems aims at limiting the influence of CCF to one I&C system only. An analysis shall be performed to identify common mechanisms which could jeopardize the independence of such I&C systems. The identified common mechanisms should be eliminated or shall be shown to have adequate mitigation.*” * Regulator Task Force on Safety Critical Software (TF SCS), Licensing of safety critical software for nuclear reactors (ref. ‎[7]) states,   + Common position 1.12.3.2 *“The decision to use diversity, the type of diversity, the objectives for its use in each case (for example protecting against a particular hazardous condition), or the decision not to use diversity shall be documented and justified.”*   + recommended practice 1.12.4.1 *“where diverse safety systems are required, and one is computer-based, consideration should be given to implementing the second one using a simple non-computer-based system.”* * US NRC BTP 7-19 Guidance for evaluation of defense in depth and diversity to address common-cause failure due to latent design defects in digital instrumentation and control systems (ref. ‎[29]) in relation to the use of NUREG/CR-7007 states, *“while this NUREG describes a method for quantitatively assessing the amount of diversity in a system, this method has not been benchmarked and should not be used as the sole basis for justifying adequate diversity.”*   **Regulatory Expectations**  ONR would not necessarily expect a fully substantiated demonstration of independence and diversity in Step 2 of GDA. It is also recognised that the RP may still be making design choices or making decisions on when to provide equivalent or similar submissions to other regulators for BWRX-300 projects progressing on different timescales.  ONR is also not necessarily asking for ‘bespoke’ submissions solely for the UK. We share the RP’s aspirations to have standard design in multiple countries, supported as much as possible by common documentation.  We are seeking assurances, through a resolution plan agreed in Step 2, on how the RP plans to address the RO actions identified below. Through either existing planned work or new work packages, a description of suitable activities to address the points identified is sought, along with timescales, standards and guidance that will be applied, and criteria that will be used to inform the design and the RP’s “success criteria”.  **References**   1. GE-Hitachi, NEDC-34165P BWRX-300 UK GDA Chapter 3 – Safety Objective & Design Rules for SSCs, Rev A, 27 November 2024, ONRW-2019369590-15124 2. GE-Hitachi, NEDC-34169P BWRX-300 UK GDA Chapter 7 - Instrumentation and Control, Rev A, 27 November 2024, ONRW-2019369590-15125 3. GE-Hitachi, 005N9751 BWRX-300 General Description, Revision F, December 2023, ONRW-2019369590-7908 4. GE-Hitachi, M250047 Submission of BWRX-300 UK GDA Step 2 RQ-01756 Response, 25 March 2025, ONRW-609516046-1198 5. GE-Hitachi, M250037 Submission of BWRX-300 UK GDA Step 2 Regulatory Query (RQ)-01743 Full Response, 28 March 2025, ONRW-609516046-1261 6. IAEA, IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition, https://www-pub.iaea.org/MTCD/Publications/PDF/IAEA-NSS-GLOweb.pdf 7. Regulator Task Force on Safety Critical Software (TF SCS), Licensing of safety critical software for nuclear reactors, Common position of international regulators and authorised technical support organisations, 2024 revision, <https://www.onr.org.uk/publications/regulatory-reports/other-reports/licensing-of-safety-critical-software-for-nuclear-reactors/> 8. ONR, NS-TAST-GD-005 Technical Assessment Guide on Regulating duties to reduce risks to ALARP, Issue 12, 2 September 2024, https://www.onr.org.uk/media/aavhpg4c/ns-tast-gd-005.docx 9. ONR, Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPRTM Reactor https://www.onr.org.uk/media/documents/gda/reports/step-four/technical-assessment/ukepr-ci-onr-gda-ar-11-022-r-rev-0.pdf 10. ONR, Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor, December 2011, https://www.onr.org.uk/media/documents/gda/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf 11. ONR, Step 4 Assessment of Control and Instrumentation for the UK Advanced Boiling Water Reactor, December 2017, https://www.onr.org.uk/media/documents/gda/uk-abwr/step4/onr-nr-ar-17-017.pdf 12. ONR, Step 4 Assessment of Control and Instrumentation for the UK HPR1000 Reactor, January 2022, https://www.onr.org.uk/media/documents/gda/uk-hpr1000/step-4/onr-nr-ar-21-005.pdf 13. GE-Hitachi, M250170 Submission of BWRX-300 UK GDA, Regulatory Query (RQ)-01961 Response, 2 May 2025, ONRW-609516046-1721 14. United States Nuclear Regulatory Commission, NUREG/CR-7007 Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, February 2010, https://www.nrc.gov/docs/ML1008/ML100880143.pdf 15. GE-Hitachi, 008N1105 Safety Class 2 H20 Diverse Protection System Platform Suitability Assessment, Revision A, December 2023, ONRW-609516046-1724 16. GE-Hitachi, 007N5107 BWRX-300 I&C Failure Mode and Hazards Analyses Plan, Revision B, July 2024, ONRW-609516046-1754 17. GE-Hitachi, NEDC-34197P BWRX-300 UK GDA Chapter 25 – Security Annex, Revision A, November 2024, ONRW-2019369590-14914 18. GE-Hitachi, M250144 Submission of BWRX-300 UK GDA, GEH Response to RQ-01903, 29 April 2025, ONRW-609516046-1606 19. GE-Hitachi, 008N5815 BWRX-300 C20 Diverse Protection System Cyber Security Assessment Report, Revision A, May 2024, ONRW-609516046-1600. 20. ONR, Safety Assessment Principles for Nuclear Facilities, Rev 1, January 2020, <https://www.onr.org.uk/media/pobf24xm/saps2014.pdf> 21. ONR, Security Assessment Principles for the Civil Nuclear Industry, Version 1, 2022 Edition https://www.onr.org.uk/media/g05fszjn/security-assessment-principles.pdf 22. ONR, NS-TAST-GD-046 Technical Assessment Guide on Computer Based Safety Systems, Issue 7, December 2023, <https://www.onr.org.uk/media/3def2aat/ns-tast-gd-046.docx> 23. ONR, CNS-TAST-GD-11.4.1 Technical Assessment Guide on Secure by Design, Issue 1.1, January 2023, https://www.onr.org.uk/media/hr0lnkol/cns-tast-gd-1141.docx 24. BS EN IEC 62859:2020, Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity 25. ONR, Chief Nuclear Inspector’s Annual Report on Great Britain’s Nuclear Industry 2023/24, October 2024, https://onr.org.uk/media/l3ihfyrw/onr\_cni\_report\_2024.pdf 26. ONR, ONR’s Regulatory influence on the EPR Design in the UK, Issue 1, 4 October 2024, 2024/40704, https://www.onr.org.uk/media/qr2ifif4/onrs-regulatory-influence-on-the-epr-design-in-the-uk.docx 27. International Atomic Energy Agency (IAEA), Specific Safety Guide (SSG) 39 Design of Instrumentation and Control Systems for Nuclear Power Plants, 2016, <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf> 28. BS EN 62340:2010 Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF) 29. United States Nuclear Regulatory Commission, Branch Technical Position 7-19, Guidance for evaluation of defense in depth and diversity to address common-cause failure due to latent design defects in digital safety systems, Revision 9, May 2024 | | |
| **REGULATORY OBSERVATION ACTIONS** | | |
| **RO-BWRX300-001 A1 – 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 required by '*to be determined by the RP’s Resolution Plan*'. | | |
| **RO-BWRX300-001 A2 – 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 required by '*to be determined by the RP’s Resolution Plan*' | | |
| **RO-BWRX300-001 A3 – 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.   Our expectation is for the RP to capture this information in an appropriate report. This may be a report specific to this Action, or it may be integrated or referenced within an overarching document addressing wider aspects of independence and diversity, or elsewhere as the RP sees fit.  Resolution required by '*to be determined by the RP’s Resolution Plan*' | | |
| **RO-BWRX300-001 A4 – 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 required by '*to be determined by the RP’s Resolution Plan*' | | |
| **REQUESTING PARTY TO COMPLETE** | | |
| **Actual Acknowledgement date** (dd/mm/yy)**:** | |  |
| **RP stated Resolution Plan agreement date** (dd/mm/yy)**:** | |  |

1. Independence - the ability to perform a required function unaffected by the operation or failure of other equipment and from the effects resulting from the initiating event (ref. ‎[6]). [↑](#footnote-ref-2)
2. Diversity - the presence of two or more independent systems or components to perform an identified function, where the systems or components have different attributes so as to reduce the possibility of CCF (ref. ‎[6]). [↑](#footnote-ref-3)
3. CCF - a functional failure of multiple components due to a single specific event or cause (ref. ‎[1]). [↑](#footnote-ref-4)