Office for Nuclear Regulation

Civil Nuclear Reactor Build - Generic Design Assessment

Step 2 Assessment of the Control and Instrumentation of Hitachi GE's UK Advanced Boiling Water Reactor (UK ABWR)

Assessment Report ONR-GDA-AR-14-006
Revision 0
28th August 2014

Published 08/14

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

This report presents the results of my assessment of the Control and Instrumentation (C & I) of Hitachi General Electric Nuclear Energy Ltd (Hitachi-GE) UK Advanced Boiling Water Reactor (UK ABWR) undertaken as part of Step 2 of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA). ONR refers to an organisation or organisations submitting a design for GDA as the Requesting Party (RP).

The GDA process calls for a step-wise assessment of the RP's safety submission with the assessments getting increasingly detailed as the project progresses. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including a review of key nuclear safety, nuclear security and environmental safety claims with the aim of identifying any fundamental safety or security shortfalls that could prevent the proposed design from being licensed in Great Britain. Therefore, during GDA Step 2 my work has focused on the assessment of the key safety claims in the area of control and instrumentation to judge whether they are complete and reasonable in the light of our current understanding of reactor technology.

For C & I, I have interpreted safety claims to be those related to the adequacy of the architecture of the C & I systems to perform their function and that these systems are adequate to support Design Basis, beyond the Design Basis and Probabilistic claims made against them. In addition, that the systems meet the expectations of the appropriate standards and guidance and their design meets the high-level expectations of the established relevant good practice for Nuclear Power Plant design in the United Kingdom.

The standards I have used to judge the adequacy of the claims in the area of C & I have been primarily ONR's Safety Assessment Principles (SAPs), in particular SAPs EKP, ECS, EQU, EDR, ERL, ECM, EMT, EAD, ELO, EHA, ESS, ESR, EES, ECV, ERC and DC, and ONR's Technical Assessment Guides (TAG)s Safety Systems (NS-TAST-GD-003) and Computer Based Safety Systems, (NS-TAST-GD-046).

My GDA Step 2 assessment work has involved continuous engagement with the RP (Hitachi-GE) in the form of technical exchange workshops and progress meetings. In addition, my understanding of the ABWR technology, and, therefore, my assessment, has significantly benefited from visits to ABWRs, Hitachi Works and Omika Works.

My assessment has been based on the RP's Preliminary Safety Report (PSR) and its references relevant to C & I. The RP's preliminary safety case aspects related to control and instrumentation, as presented in those documents, can be summarised as follows:

- The C & I systems will be classified in accordance with the functions they perform and their safety significance.
- High-level design principles of segregation, independence, diversity, defence against common cause failures and defence in depth will be applied to the design of the C & I Systems.
- C & I systems will be designed to comply with relevant codes and standards.

During the early stages of my assessment a potential shortfall in the diversity between the Primary Protection System platform technology and other systems, was identified as a regulatory concern. Following extensive engagement with the RP, it has committed to modify the technology of the Primary Protection System to be diverse from other systems for the UK ABWR. It has also agreed to enhance the isolation of its primary protection system (known as the Safety System Logic and Control) from the other control systems and also provide additional isolation of the plant computer system (PCS) from more general nuclear power station computer networks.

During my GDA Step 2 assessment of the UK ABWR aspects of the safety case related to C & I, I have identified the following areas of strength:

- The RP has an adequate process in place to identify faults and classify the C & I systems that are required to support its claim relating to the overall safety of the UK ABWR.
- The high-level design of the C & I architecture will follow relevant good practice and has three diverse, independent and separate C & I platforms, which deliver primary and secondary protection and control functions.

Overall, I am satisfied that the high-level claims made by the RP are reasonable, complete, and can be adequately underpinned with sufficient arguments and robust evidence. I am also confident that the RP will be able to articulate reasonable claims in the PCSR.

During my GDA Step 2 assessment of the UK ABWR aspects of the safety case related to control and instrumentation I have identified the following areas that require follow-up:

- The demonstration of adequate production excellence of the Safety System Logic and Control (SSLC) design (this is the primary protection system).
  The design and development of this system to support its classification (Class 1) requirements will require production excellence processes proportionate with its classification. The RP has not fully developed its processes for complex components such as Field Programmable Gate Arrays (FPGA) planned to be used in this system.

- Independence of Design Teams for C & I platforms.
  To support the development of the SSLC design it is essential for the design team to be independent from teams who are developing the design of other protection and control systems. The RP has not demonstrated that independent teams are in place to deliver this expectation.

- Secondary Protection System (Hardwired).
  The Secondary Protection System (referred to as the hardwired system) is based on hardwired non-programmable technology, which is made up of a number of separate systems. In order for the RP to demonstrate that this system is adequate and resilient to systematic faults my judgement is that it should be designed as a single coordinated system. The RP has not provided sufficient information during Step 2 to describe the complete hardwired system design.

During step 3 of GDA I will be following up on the above areas and will be raising the following Regulatory Observations based on my Step 2 GDA assessment;

- Production excellence of FPGA based SSLC (primary protection).
- Independence of design teams for C & I platforms.
- Hardwired system (secondary protection).

In relation to my interactions with the RP's Subject Matter Experts (SME) in control and instrumentation, I have found the RP to be proactive in all engagements with ONR and it has made available sufficient resources to support the development of the C & I aspects of the safety case. Where necessary the RP has provided additional specialist engineering support to the C & I SME, which has given me confidence that it can develop an adequate safety case and C & I design for the UK ABWR. The RP has been open and transparent in its responses to requests for clarifications and additional technical information.

Overall, I see no reason, on control and instrumentation grounds, why the UK ABWR should not proceed to Step 3 of the GDA process.

LIST OF ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
BMS	Business Management System
BOP	Balance Of Plant
C & I	control and instrumentation
DAC	Design Acceptance Confirmation
ECCS	Emergency Core Cooling System Emergency Safety Features (ESF)
EA	Environment Agency
ESF	Emergency Safety Features
FPGA	Field Programmable Gate Array
GDA	Generic Design Assessment
HBSS	Hardwired Back-up Safety System
Hitachi-GE	Hitachi General Electric Nuclear Energy Ltd
HMI	Human Machine Interface
HVAC	Heating Ventilation & Air Conditioning
IEC	International Electro-technical Commission
IAEA	International Atomic Energy Agency
JEAC	Japan Electric Association Codes
JEAG	Japan Electric Association Guides
JPO	(Regulators') Joint Programme Office
MSIV	Main Steam Isolation Valve
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
PCS	Plant Computer System
PCoS	Plant Control System
PCSR	Pre-construction Safety Report
PSR	Preliminary Safety Report
RHWG	Reactor Harmonization Working Group (of WENRA)

LIST OF ABBREVIATIONS

RO	Regulatory Observation
RP	Requesting Party
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RQ	Regulatory Query
RRP	Resource Review Panel
SAP(s)	Safety Assessment Principle(s)
SME	Subject Matter Expert
SSC	System, Structure and Component
SSLC	Safety System Logic and Control
TAG	Technical Assessment Guide(s)
TSC	Technical Support Contractor
US NRC	United States Nuclear Regulatory Commission
V & V	Verification and Validation
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Table(s)

1 INTRODUCTION

1.1 Background

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments getting increasingly detailed as the project progresses. Hitachi General Electric Nuclear Energy Ltd's (Hitachi-GE) is the RP for the GDA of the UK Advanced Boiling Water Reactor (UK ABWR).

2. During Step 1 of GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams and made arrangements for the GDA of its ABWR design. In addition, during Step 1 the RP prepared submissions to be evaluated by ONR and the Environment Agency (EA) during Step 2.

3. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including review of key nuclear safety, nuclear security and environmental safety claims with the aim of identifying any fundamental safety or security shortfalls that could prevent the proposed design from being licensed in Great Britain.

4. This report presents the results of my assessment of the control and instrumentation (C & I) aspects of the RP's UK ABWR design as presented in the UK ABWR Preliminary Safety Report (PSR) (Ref. 1) and its supporting documentation (Refs. 2, 3, 4, 5 and 6).

1.2 Methodology

5. I undertook my assessment in accordance with the requirements of the Office for Nuclear Regulation (ONR) How2 Business Management System (BMS) procedure PI/FWD (Ref. 7). I have used ONR Safety Assessment Principles (SAPs) (Ref. 8), together with supporting Technical Assessment Guides (TAG) (Ref. 9) as the basis for this assessment.

6. My assessment has followed my GDA Step 2 Assessment Plan for C & I (Ref. 10) prepared in December 2013 and shared with the RP to maximise openness and transparency.

2 ASSESSMENT STRATEGY

7. This section presents my strategy for the GDA Step 2 assessment of the C & I of the UK ABWR (Ref. 10). It also includes the scope of the assessment and the standards and criteria that I have applied.

2.1 Scope of the Step 2 Control and Instrumentation Assessment

8. The objective of my GDA Step 2 C & I assessment for the UK ABWR was to review and judge whether the claims made by the RP related to C & I that underpin the safety, security and environmental aspects of the UK ABWR are complete and reasonable in the light of our current understanding of reactor technology.

9. For C & I "safety claim" is interpreted as being:

   - The architecture of the control and protection system can adequately perform its function.

- There are adequate C & I based safety systems to support Design Basis and Probabilistic claims.
- The design meets the high-level expectations of appropriate standards and guidance.
- The design meets the high-level expectations of the established relevant good practice for Nuclear Power Plant (NPP) design in the United Kingdom.

10. For C & I "security claim" is interpreted as being:

- The resilience of C & I based systems to withstand external threats.

11. During GDA Step 2, I have also evaluated whether the safety and security claims related to C & I are supported by a body of technical documentation sufficient to allow me to proceed with GDA work beyond Step 2.

12. Finally, during Step 2 I have undertaken the following preparatory work for my Step 3 assessment:

- Preliminary research in to the techniques for formal verification and validation of Field Programmable Gate Array (FPGA) devices used in Class 1 safety systems.
- Preliminary review of Chapter 11 (Reactor Instrumentation and Control) of the Pre-Construction Safety Report.
- A review of the draft Basis of Safety Case for the C & I architecture.
- A review of the RP's draft Step 3 C & I GDA document list.
- Preliminary planning of Step 3 assessment activities.
- Held discussions with the RP to help it develop its documentation delivery schedule.
- A review of the use of Technical Support Contractors.

2.2 Standards and Criteria

13. The goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety, security and environmental case. For this purpose, within ONR, assessment is undertaken in line with the requirements of the How2 Business Management System (BMS) document PI/FWD (Ref. 7) Appendix 1 of Ref. 7 sets down the process of assessment within ONR; Appendix 2 explains the process associated with sampling of safety case documentation.

14. In addition, the Safety Assessment Principles (SAPs) (Ref. 8) constitute the regulatory principles against which duty holders' safety cases are judged, and, therefore, they are the basis for ONR's nuclear safety assessment and therefore have been used for GDA Step 2 assessment of the UK ABWR. The SAPs 2006 Edition (Revision 1 January 2008) were benchmarked against the IAEA standards (as they existed in 2004). They are currently being reviewed.

15. Furthermore, ONR is a member of the Western European Nuclear Regulators' Association (WENRA). WENRA has developed Reference Levels, which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors.

16. The relevant SAPs, IAEA standards and WENRA reference levels are broadly embodied and enlarged on in the Technical Assessment Guides on C & I (Ref. 9). These guides provide the principal means for assessing the C & I aspects in practice.

2.2.1 Safety Assessment Principles

17. The key SAPs (Ref. 8) applied within the assessment are SAPs EKP, ECS, EQU, EDR, ERL, ECM, EMT, EAD, ELO, EHA, ESS, ESR, EES, ECV, ERC and DC (see Table 1 for further details).

2.2.2 Technical Assessment Guides

18. The following Technical Assessment Guides (TAG)s have been used as part of this assessment (Ref. 9)

- TAGs fundamental to my assessment.
  - Safety Systems, NS-TAST-GD-003
  - Computer Based Safety Systems, NS-TAST-GD-046
- Supporting TAGs which have not been used explicitly during my assessment.
  - Electromagnetic Compatibility, NS-TAST-GD-015
  - Essential Services, NS-TAST-GD-019
  - Control and instrumentation aspects of nuclear plant commissioning, NS-TAST-GD-028
  - Safety Related Instrumentation, NS-TAST-GD-031

2.2.3 National and International Standards and Guidance

19. The following national and international standards and guidance have also been used as part of this assessment:

- Relevant IAEA standards (Ref. 11):
  - Safety of Nuclear Power Plants: Design. Safety Requirements. NS-R-1
  - Software for Computer Based Systems Important to Safety In Nuclear Power Plant Safety Guide, NS-G-1.1
  - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide. NS-G-1.3
- WENRA references (Ref.12):
  - Reactor Safety Reference Levels (January 2007)
  - Safety Objectives for New Power Reactors (December 2009) and Statement on Safety Objectives for New Nuclear Power Plants (November 2010)
  - Decommissioning Safety Reference Levels (March 2012)
  - Statement on Safety Objectives for New Nuclear Power Plants (March 2013) and Safety of New NPP Designs (March 2013)
- Other international standards (Ref. 13):
  - IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems (parent standard for the design of E/E/PE safety-related systems)

- IEC 61513 - Nuclear power plants — Instrumentation and control important to safety — General requirements for systems
- IEC 61226 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

2.3 Use of Technical Support Contractors

20. During Step 2, I have not engaged Technical Support Contractors (TSC) to support my assessment of the C & I for the UK ABWR.

2.4 Integration with Other Assessment Topics

21. Early in GDA, I recognised that during the project there would be a need to consult with other assessors (including Environment Agency's assessors) as part of the C & I assessment process. Similarly, other assessors will seek input from my assessment of the C & I for the UK ABWR. I consider these interactions very important to ensure the prevention of assessment gaps and duplications, and, therefore, are key to the success of the project. Thus, from the start of the project, I made every effort to identify as many potential interactions as possible between the C & I and other technical areas, with the understanding that this position would evolve throughout the UK ABWR GDA.

22. Also, it should be noted that the interactions between the C & I and some technical areas need to be formalised since aspects of the assessment in those areas constitute formal inputs to the C & I assessment, and vice versa. These are:

- The Fault studies, probabilistic safety assessment, mechanical and human factors topic areas provide input to the assessment of the adequacy of the protection provided by the C & I systems. This formal interaction has not commenced during GDA Step 2. This work will be led by myself in coordination with the other assessment topic inspectors.
- The electrical topic area provides input to the assessment of the reliance on external sources of energy to support C & I systems. This formal interaction has not commenced during GDA Step 2. This work will be led by myself in coordination with the Electrical Inspector.
- The C & I topic area provides input to the assessment of all SMART devices and C & I systems embedded in packaged support systems in the electrical and mechanical topic areas. This formal interaction has not commenced during GDA Step 2. This work will be led by the Electrical and Mechanical Inspectors.

23. In addition to the above, during GDA Step 2 there have been interactions between C & I and the rest of the technical areas, for example, Management of Safety and Quality Assurance etc. Although these interactions, which are expected to continue thorough GDA, are mostly of an informal nature, they are essential to ensure consistency across the technical assessment areas.

3 REQUESTING PARTY'S SAFETY CASE

24. This section presents a summary of the RP's preliminary safety case in the area of C & I. It also identifies the documents submitted by the RP, which have formed the basis of my assessment of the UK ABWR C & I during GDA Step 2.

3.1 Summary of the RP's Preliminary Safety Case in the Area of Control and Instrumentation

25. The aspects covered by the UK ABWR preliminary safety case in the area of C & I can be broadly grouped under 4 headings which can be summarised as follows

3.1.1 Categorisation and Classification of C & I Systems:

26. The RP's safety case for the Categorisation and Classification of Systems, Structures and Components (SSC)s has historically been based on Japanese rules. For the UK ABWR the safety case will follow the guidance set out in the ONR SAPs in SAP ECS.1 for the Categorisation of SSCs and SAP ECS.2 for the Classification of SSCs. The RP is also applying the approach outlined in IEC 61226 for the classification of instrumentation and control systems in nuclear power plants and IEC 61513 for the general requirements for instrumentation and control systems in nuclear power plants. IEC 61513 gives further guidance on the categorisation and classification of C & I systems.

27. The RP has based the allocation of category and classification for C & I systems on the existing ABWR scheme and has committed to update the allocation following the development of the UK ABWR Fault Schedule. The development of the Fault Schedule will take into account the existing ABWR allocation, the requirements of IEC 61226 and the application of experience and engineering judgement.

28. The RP claims that the allocation of category and classification for C & I systems is adequate to allow the design of C & I systems to progress.

3.1.2 Design Codes and Standards:

29. The RP's safety case for the design codes and standards is based on the policy for the base line design of the ABWR, which uses Japan Electric Association Codes (JEAC) and Japan Electric Association Guides (JEAG). The UK ABWR design development will follow a similar approach but will include IEC nuclear sector standards, IAEA guidance and take into account ONR guidance.

30. The RP has reviewed the standards and guides identified in the previous paragraph and produced a comparison summary. In addition it has reviewed IEC nuclear standards and has listed IEC and JEAG standards, which are, either fundamental for system design, Tier 1 standards, or are standards which support these standards, Tier 2.

31. The RP has identified a number of overarching standards such as IEC 61508, IEC 61513 and IEC 61226 to be important to the design of the UK ABWR.

32. The RP intends to demonstrate that the development processes and practices it currently uses are compatible with IEC standards. It has stated that where shortfalls are found against IEC standards measures will be taken to address them.

3.1.3 Control and Instrumentation System Architecture:

33. The RP's safety case for the C & I System Architecture is based on it meeting the categorisation and classification requirements specified in the Fault Schedule. To achieve these requirements the C & I System Architecture has been design to deliver; the required safety functions, the associated reliability of these functions and the deterministic considerations.

34. The RP has stated that the system is designed to be diverse, independent and segregated to defend against common cause failure due to hazards and systematic failures. It has also stated that the C & I System Architecture is designed to limit propagation of failures and loss of function.

35. The RP's design for the C & I System Architecture for the main plant is divided into 3 systems: the Safety System Logic and Control (SSLC), the Hardwired Back-up System and the Plant Control System. The RP has stated that the platforms for these systems will use diverse technology; FPGA, Hardwired non-programmable and microprocessor (Programmable Logic Controller) based, respectively. The RP has identified each system and its function along with its category, classification and its platform technology.

36. The C & I System Architecture design prevents access from external off-site systems to it by the use of one-way communications devices ("Data Diodes").

37. The RP claims the design of the C&I architecture meets the deterministic and probabilistic requirements placed upon it.

3.1.4 Safety System Logic and Control (SSLC):

38. The RP's safety case for the Class 1 Primary Protection System, the SSLC, is based on it meeting the deterministic and probabilistic claims made upon it. The SSLC is the primary safety system for the UK ABWR providing; reactor shutdown, reactor pressure vessel isolation, maintain reactor core water cover and provide residual heat removal and other essential safety feature actuation systems.

39. To support the claims on the C & I System Architecture the SSLC platform design will be based on FPGA technology, which is diverse from the Hardwired Back-up and Control Systems.

40. The SSLC is a 4-division system operating mainly on a 2-out-of-4 (2oo4) voting logic system. The equipment for each division is physically separated by locating it in different areas of the facility.

41. The RP design of the SSLC prevents lower class systems (Class 2 & 3) adversely influencing its operation by only allowing information to be read from it. The operator interface for the SSLC is provided by a touch-screen operated Class 1 Human Machine Interface (HMI). Operator actions are confirmed by the use of hard-wired pushbuttons that do not rely on communications systems.

42. The RP claims the design of the SSLC meets the deterministic and probabilistic requirements placed upon it, particularly the claim that it uses diverse technology from the hardwired Back-up and Plant Control systems.

3.2 Basis of Assessment: RP's Documentation

43. The RP's documentation that has formed the basis for my GDA Step 2 assessment of the safety claims related to the C & I for the UK ABWR is:

- UK ABWR PSR Chapter on C & I "Preliminary Safety Report on C & I" (Ref. 1). This document presents the background of the design of C & I systems for the UK ABWR and identifies the scope of the C & I systems covered in the Generic Design Assessment process. It gives a high-level description of the major C & I systems and identifies standards, which are applicable to the UK ABWR design.
- UK ABWR C & I New Platform Development for Protection System and Decision on Protection System Platform letter (Refs. 2 and 3). These documents present the protection system platform technology choice for the UK ABWR.
- UK ABWR Topic Report "Categorisation and Classification of Structures, Systems and Components" (Ref. 4). This document describes the Categorisation and Classification system, which will be applied to the UK ABWR. It presents the international standards and guidance which has been used to develop the system and it provides a list of the indicative Classification for major systems.
- UK ABWR Topic Report "Codes and Standards" (Ref. 5). This document presents the codes and standards that will be applied to the UK ABWR design. It cross-references Japanese standards against the standards that will be applied for the UK ABWR design.
- UK ABWR GDA "C & I E Basic Plan" (Ref. 6). This document provides description on the design, implementation, qualification, and documentation of C & I systems important to safety for the UK ABWR.
- UK ABWR GDA tracking sheet (Ref. 14).
- Responses to Regulatory Queries (RQ) (RQ-ABWR-0152 to 157 and 172 (Ref. 15)) Reference 16.

44. In addition, in May 2014 the RP submitted to ONR for information an advance copy of the UK ABWR Pre-Construction Safety Report (PCSR). Chapter 11 (Ref. 17) addresses C & I. Although I have not covered this report in my GDA Step 2 formal assessment, seeing it has been useful to start planning and preparing my GDA Step 3 work. I have also seen draft versions of other documents the RP has identified it will deliver during Step 3. This has also informed my Step 3 assessment planning.

4 ONR ASSESSMENT

45. My assessment has been carried out in accordance with ONR How2 BMS document PI/FWD, “Purpose and Scope of Permissioning” (Ref. 7).

46. My GDA Step 2 C & I assessment has followed the strategy described in Section 2 of this report and has not required the assistance of Technical Support Contractors.

47. My Step 2 assessment work has involved continuous engagement with the RP’s C & I Subject Matter Experts (SME), ie Technical Exchange Workshops (in Japan and the UK) and progress meetings (mostly video conferences) have been held. I have also visited:

- Kashiwazaki Kariwa Units 6 & 7 ABWRs where I could tour the majority of the facility including the upper Drywell where the (internal) Main Steam Isolation Valves (MSIV) are located. I also viewed the Control Room from the visitors viewing area along with other plant areas.

- Omika Works where they manufacture and assemble control systems and I could see the manufacturing facility and the Japanese ABWR Control Room simulator.

- Hitachi Works, where they manufacture reactor internal components and I could see the manufacturing facility and components which were destined for other ABWRs currently under construction.

48. During my GDA Step 2 assessment, I have identified some shortfalls in documentation which have generally led to the issue of RQs; overall I have raised seven RQs. Shortfalls in the safety case have generally led to the issue of Regulatory Observations (RO)s. I have not raised any specific C & I ROs during GDA Step 2. I have contributed to two ROs raised by the Fault Studies Inspector that relate to C & I and Fault Studies matters. These are:

- RO-ABWR-0007 Spurious C & I failure as design basis initiating events

- RO-ABWR-0010 Design Basis Analysis of essential services and support services

49. My assessment sample has focused on four main technical areas within the RP’s C & I safety case, which I consider to be fundamental to the safety of the C & I systems. These areas are:

1. Classification and Categorisation of C & I Systems
2. Design Codes and Standards
3. C & I System Architecture
4. Primary Protection System

50. I judge that the technical areas I have selected for my assessment are suitable and sufficient for me to make a judgement of the adequacy and the fundamental safety of the C & I design of the UK ABWR during Step 2 of GDA.

51. Details of my GDA Step 2 assessment of the UK ABWR preliminary safety case in the area of C & I including the areas of strength that I have identified, as well as the items

that require follow-up and the conclusions reached are presented in the following sub-sections.

4.1 Classification and Categorisation of C & I Systems:

4.1.1 Assessment

52. My assessment has focused on the C & I aspects of the Classification and Categorisation of Systems. I have assessed the RP's Preliminary Safety Report on C & I" (Ref. 1) and I have reviewed the supporting "Categorisation and Classification of Structures, Systems and Components" (Ref. 4) document.

53. I have used the ONR SAPs ECS.1 (Categorisation) and ECS.2 (Classification) and international standard IEC 61226, "*Nuclear power plants Instrumentation and control important to safety classification of instrumentation and control functions*" (Ref. 13), to inform my assessment and judgements of the adequacy of the RP's safety case. IEC 61513, "*Nuclear power plants Instrumentation and control important to safety General requirements for systems*" (Ref. 13), has also been used to inform my judgements. Table 1 of this report gives additional information on the basis of the findings of my assessment.

54. The RP's approach to the categorisation of safety functions and the classification of systems has historically been based on Japanese guidance. The RP has claimed that the Japanese approach results in the categorisation of safety functions that broadly aligns with the regulatory expectations in the United Kingdom. The RP has committed to adopt the guidance set out in ONR SAPs ECS.1, ECS.2, IEC 61226 and IEC 61513 for the fully developed UK ABWR design. I judge that this approach is adequate. I will follow-up this matter during Step 3 of GDA to gain confidence that the RP has adequately interpreted the guidance and has appropriately categorised and classified the C & I safety functions and systems.

55. The RP has stated that the current categorisation and classification of safety functions and systems is based on the allocation for its existing ABWR design and engineering judgement. Tables 3.3.1-1, 3.3.1-2 and 3.3.1-3 of reference 1 identify the assumed category and classification for the UK ABWR. My sample assessment of these tables has revealed that the allocation of category and class meet my expectations.

56. The RP has committed to undertake a review of the categorisation and classification of C & I systems against the expectations set out in ECS.1, ECS.2, IEC 61226 and IEC 61513. The RP's revised approach is to categorise safety functions as either category A, B or C depending of the role the function plays in nuclear safety. Category A would identify functions which play a significant role in nuclear safety. With regard to classification, the RP's approach is to classify safety systems as either class 1, 2 or 3, with class 1 being the highest classification. This work will consist of a review of the faults identified in the Japanese ABWR fault assessment and identification of faults not included in the original Japanese work. Following this review the UK ABWR Fault Schedule will be updated and the C & I safety systems categorisation and classification will be updated.

57. I have assessed the RP's revised approach and I am satisfied that it meets the expectations set out in ONR SAP ECS.1 and ECS.2 and my expectations. I consider the RP's commitment to adopt the international standards IEC 61226 and IEC 61513 as a positive demonstration it is adopting relevant good practice.

4.1.2 Strengths

58. The RP has a systematic approach to the Categorisation and Classification of C & I systems, which is based on the relevant ONR SAPs and international standards.

59. The RP has committed to review the categorisation and classification of C & I safety systems for the UK ABWR and update it with any required changes or to address additional faults identified during its review.

4.1.3 Items that Require Follow-up

60. During my GDA Step 2 assessment of Classification and Categorisation of C & I Systems I have identified the following additional potential shortcomings that I will follow-up during Step 3:

- The current allocation of category and classification for C & I safety functions and systems is based on the current Japanese ABWR design and engineering judgement. I will follow-up the RP's review of the categorisation and classification of C & I safety function and systems along with the allocation of functional requirements to gain confidence that the RP has adequately interpreted the guidance and has appropriately categorised and classified C & I safety functions and systems in place for the UK ABWR design.

4.1.4 Conclusions

61. Based on the outcome of my assessment of Classification and Categorisation of C & I Systems, I have concluded that that the RP has an adequate process to categorise and classify C & I safety systems. I have compared its approach with the relevant ONR SAPs and international standards and I am satisfied my expectations have been met.

4.2 Design Codes and Standards:

4.2.1 Assessment

62. My assessment has focused on the design codes and standards applied to C & I Systems. I have assessed the RP's Preliminary Safety Report on C & I" (Ref. 1). I have also reviewed the supporting "Codes and Standards Report" (Ref. 5) and the C & I E Basic Plan (Ref. 6).

63. I have used the ONR SAPs ECS.3 (Standards), ESS.27 (Computer Based Safety Systems) and ESR.5 (Standards for Computer Based Equipment). To inform my assessment and judgements of the adequacy of the RP's safety case. ONR's Safety Systems (T/AST/003) and Computer Based Safety Systems (NS-TAST-GD-046) TAGs along with international standards IEC 61513, "*Nuclear power plants Instrumentation and control important to safety General requirements for systems*" (Ref. 13), and IEC 61508, "*Functional safety of electrical/electronic/programmable electronic safety-related systems*" have also been used to inform my judgements. Table 1 of this report gives additional information on the basis of the findings of my assessment.

64. Section 2.2, Design Policy for C & I Systems Important to Safety, of the PSR (Ref. 1) describes the design policy for the existing baseline design. This section states that the baseline C & I systems design is based on Japanese Safety Design and Japanese Electric Association Guides (JEAG) design codes, standards and guides. It has stated that the development of the UK ABWR C & I design will follow the existing design practice and will include IEC nuclear sector standards, the latest IAEA guidance and take cognisance of ONR guidance included in the SAPs and TAGs. In particular TAGs

003 and 046. The RP has provided a table (Table 2.2-1 in Reference 1) which correlates Japanese Safety Design Guides with IAEA guidance and ONR SAPs.

65. The RP has stated that for UK ABWR a comparison with IEC standards will be carried out to demonstrate that the development process and design practices used are, as a minimum, comparable to these standards. Where shortfalls are identified, the RP has committed to either modify its design processes or to compensate for the shortfall by introducing other activities. To facilitate the comparison the RP has reviewed IEC standards, which it believes are relevant to the design of NPPs, and produced an equivalence table against the Japanese design codes, standards and guides. This table is shown in section 2.4.1 of the PSR (Ref. 1). The RP has identified two tiers of IEC standards, Tier 1, primary standards that it considers are fundamental to system design and implementation and Tier 2, standards which support Tier 1 standards.

66. During my assessment of the C & I E Basic Plan (Ref. 6) I identified an inconsistency in the RP's identification of design standards. This related to the inconsistent application of JEAG and JEAC standards and IEC standards between the PSR (Ref. 1) and the C & I E Basic Plan (Ref. 6). An example of this inconsistency relates to the standards applied to the verification and validation of C & I systems. The PSR states that IEC 60880 and IEC 62138 will be used, whereas the C & I E Basic Plan states that JEAG 4069 will be used. I have raised a RQ (RQ-ABWR-0172 Reference 15) on this matter to clarify which standards the RP intends to use and I will follow it up during Step 3 of GDA.

67. I have reviewed the RP's correlation table (Table 2.2-1 in Reference 1) and its comparison table in (section 2.4.1 of the PSR Reference. 1) and I judge that the RP has identified the appropriate international standards which should be applied to the C & I design for NPPs.

68. I have compared the codes and standards identified in the PSR (Ref. 1) against the expectations set out in ONR TAGS 003 & 046 and concluded that the RP has identified the appropriate international standards. (IEC 61508, 61513, IEC 62138, IEC 60880, IEC 60987 and IEC 62566)

4.2.2 Strengths

69. The RP has reviewed IEC Nuclear Standards and produced a prioritised list, which is split into tier 1 and 2 standards, which it will use as the basis for its design.

70. The RP has identified appropriate international standards and guides and has committed to review its guidance against the expectations set out in these standards and guides. Where shortfalls in expectations are identified, it has committed to address them.

4.2.3 Items that Require Follow-up

71. During my GDA Step 2 assessment of Design Codes and Standards I have identified the following additional potential shortcomings that I will follow-up during Step 3:

- The RP has committed to review its design guidance against the expectations set out in international standards and guides. However, this review has not been completed. I will follow-up the RP's review of the design standards for C & I safety systems to gain confidence that the RP has adequately identified and incorporated the expectations of the these standards for the UK ABWR design.

- The inconsistency between the identification of design standards between the RP's documentation will be followed up in Step 3. This will be carried out by assessing the response to RQ - 0172.

4.2.4 Conclusions

72. Based on the outcome of my assessment of Design Codes and Standards, I have concluded that the RP has identified appropriate design codes and standards and has put in place a mechanism to review its own guidance against the expectations set out in national and international standards and guides. In addition the RP has committed to address any shortfalls it identifies during its review.

73. I judge that although I have found an inconsistency with regard to the identification of standards in different RP documents the overall approach to the selection of design standards is adequate.

4.3 Control and Instrumentation System Architecture:

4.3.1 Assessment

74. My assessment has focused on the high-level design of the C & I architecture and the main systems that are connected to form the overall C & I system. I have assessed the RP's "Preliminary Safety Report on C & I" (Ref. 1), the "C & I New Platform Development for Protection System letter" (Ref. 2) and the "Decision of Protection System Platform" report (Ref. 3).

75. I have used the ONR SAPs ESS (Safety Systems) and ESR (Control and instrumentation of safety-related systems) to inform my assessment and judgements of the adequacy of the RP's safety case. ONR's Safety Systems (T/AST/003) and Computer Based Safety Systems (NS-TAST-GD-046) TAGs along with international standards IEC 61513, "*Nuclear power plants Instrumentation and control important to safety General requirements for systems*" (Ref. 13), and IEC 61508, "*Functional safety of electrical/electronic/programmable electronic safety-related systems*" have also been used to inform my judgements. Table 1 of this report gives additional information on the basis of the findings of my assessment.

76. During my assessment, I have conducted a high-level review of the major systems, which form the C & I architecture. These are:

    1. Safety System Logic and Control
    2. Hardwired back-up safety system (HBSS)
    3. Plant Control System (PCoS)
    4. Plant Computer System (PCS)
    5. Other systems (eg Reactor and Turbine Auxiliary Control Systems)

77. The C & I architecture is described in Section 4.3 of the PSR (Ref. 1) and is diagrammatically represented in Figure 4.3-1, Overall C & I Architecture. The high-level claims made by the RP is that the C & I Architecture reflects the required safety functions, the reliability requirements and the deterministic and non-functional requirements and, that the C & I Architecture supports the reactor control systems, reactor safety systems and the back-up safety system in a manner that allows the failure rate of these systems to be claimed in combination. A number of sub-claims have been identified by the RP, which support the high-level claims. The RP has

stated that the systems, which make up the C & I Architecture, are diverse, independent and segregated to defend against common cause failures. My assessment has focused on the high-level claims relating to diversity, independence and segregation as these are fundamental to the overall adequacy of the C & I Architecture and the RP's safety case.

78. As listed in paragraph 76 the C & I Architecture consists of five main systems. My assessment has focused on the three of these systems, which are the SSLC, HBSS and the PCoS. Assessment of the Plant Computer System and the Reactor and Turbine Auxiliary Control Systems will be carried out in the following steps of GDA. In addition, I recognise that there are other C & I systems used within the UK ABWR, such as Fuel Route Control Systems, Heating Ventilation and Air Conditioning (HVAC) Control Systems and control systems embedded within packaged equipment (eg diesel generators and electrical load control systems) that I will also assess in the following steps of GDA.

79. The main claim that underpins the RP's safety case relates to the diversity, independence and segregation of the three main systems within the C & I Architecture.

4.3.1.1 Overall C & I Architecture

80. The overall C & I Architecture consist of the main systems identified in paragraph 76 connected together by a communications network. It is divided into three hierarchical levels, 1, 2 and 3. Level 1 is the Human Machine Interface and overall unit operation, Level 2 is the control and protection systems and the interfaces to levels 1 and 3, and Level 3 is the local monitoring, sensors and actuators. The Level 1 HMI includes the Main Control Room displays used by the plant operations personnel to control the plant. Within Level 2, there are a number of intermediate sub-systems, which form the control and protection systems. These subsystems include distributed equipment and communication networks.

81. I have conducted a high-level assessment of the design of the architecture and concluded that the hierarchical approach meets my expectations and aligns with relevant good practice for the design of large industrial control and protection systems.

4.3.1.2 Diversity

82. The three main systems within the C & I Architecture are the SSLC, HBSS and PCoS.

83. During the early stages of my assessment a potential shortfall in the diversity between the SSLC and other systems, was identified as a regulatory concern. The SSLC and PCoS were based on the same basic hardware and software technology (microprocessor based) and therefore did not meet expectations of diversity or protection against common cause failures as set out in ONR SAPs ESS and EDR. The RP recognised the significance of my concern and conducted a review to indentify alternative technologies to demonstrate it met my expectations. The result of the RP's review identified that an alternative technology could be used for the SSLC. The RP selected a FPGA based solution for the SSLC platform technology, which will, in its opinion address the regulatory concern. The RP has confirmed the change in the SSLC platform technology in two documents, the" C & I New Platform Development for Protection System letter" (Ref. 2) and the "Decision of Protection System Platform" report (Ref. 3).

84. The HBSS platform is based on hardwired logic non-programmable components which the RP claims is diverse from the SSLC platform technology. The PSR (Ref. 1) does not provide sufficient information for me to assess its adequacy. This system consists of a number of sub-systems, which perform both automatic and manually initiated

safety functions. The RP has stated within the PSR (Ref. 1) that it will review the manually initiated safety functions and modify the design to provide automatic initiation. I raised RQ-153 (Ref. 15) to clarify the technology the RP intends to use for the HBSS. The response to my RQ has indicated that the RP has, at the time of writing this report, not selected the technology it will use although it has confirmed it will be non-programmable.

85. The PCoS functionality is provided by two platforms and comprises class 2 and 3 systems. The platforms are the Hitachi Omika works HIACS and nu-Safe. It should be noted that both platforms use largely the same technology the main difference is in the degree of fault tolerance used in the different safety classes through enhanced internal features such as additional redundancy. Both platforms are microprocessor based programmable logic industrial control systems used in the nuclear power generation and industrial control environments. In the case of the nu-Safe system it has been qualified to be used as a safety system with an integrity of Safety Integrity Level 3 against the requirements of IEC 61508 (Ref. 13) although in this case its use is safety Class 2 which aligns to the lower integrity IEC 61508 SIL 2 .

86. During my assessment of the PSR (Ref. 1) I identified that pressure measurement was used as the fundamental parameter for a number of process measurement variables. For example, pressure measurements are used for direct pressure, differential pressure, level and flow measurements. This applied to process variables, which are inputs to the SSLC, HBSS and PCoS. As this is a potential weakness in the design as, in my opinion, it will be difficult for the RP to demonstrate diversity of measurements and equipment to support its safety claims I raised RQ-0154 (Ref. 15) to clarify the RP's approach. The RP has stated that it will review the diversity of pressure measurements. I will follow up this matter in the following steps of GDA.

87. Overall, the RP claims that the three main systems used to control and protect the UK ABWR are diverse as they are based on three different technologies, FPGA (SSLC), Hardwired Logic components (HBSS) and microprocessor (PCoS).

88. I have assessed the diversity claims the RP has made and I judge they are adequate based on the change in technology it has committed to make for the SSLC. With regard to the Secondary Hardwired Protection System, it is my opinion that the RP should review the design and where necessary modify it to provide a fully integrated system.

4.3.1.3 Independence and Segregation

89. The RP claims that the main C & I systems are independent and segregated from each other. The PSR (Ref. 1) describes the high-level requirements for systems to be independent and segregated. The RP has stated that more detailed information will be available in the C & I Architecture Basis of Safety Case document, which will be provided at the beginning of Step 3.

90. During the early stages of my assessment a potential shortfall in the independence between the SSLC and other systems, was identified as a regulatory concern. ONR SAP ECS.2 sets out the expectation that there should be appropriately designed interfaces between different classes of systems to ensure that a failure of a lower class system will not propagate to an item of a higher class. The proposed UK ABWR design, in my opinion, did not provide sufficient protection against the propagation of faults from lower to high class systems as there was direct read and write connectivity from lower class systems to the Class 1 SSLC. In addition, connection between other classes of system and to off-site systems did not adequately protect against propagation of faults. The RP has put forward a number of modifications to protect

against propagation of faults and improve the isolation of systems from each other. The method the RP has included in the design described in the PSR (Ref. 1) is the use of one-way gateway, which will prevent lower class systems affecting higher class system. This method has also been introduced for the off-site connection and the interfaces between the Plant Computer Control System and the general nuclear power station computer networks. In addition to eliminating a wide range of faults this improvement will also be of considerable benefit for the security of the systems.

91. During my review of the RP's safety case it was unclear if all the SSLC and PCoS were independent from each other from end to end. For example, from the sensing instrument, through to the logic solving event and on to the final termination equipment. To clarify the design I raised RQ-155 (Ref. 15). The response to this RQ has revealed that there are a number of sensing instruments that share common connections, particularly around the connections to the reactor pressure vessel. This matter will be followed up in the following steps of GDA. In other areas, the RQ confirmed the claim that the three systems are otherwise independent of each other.

92. The physical location and segregation of C & I equipment in particular the SSLC has been described at a high-level in the PSR (Ref. 1). Section 4.4, Location of Architecture Elements, describes the location of the equipment for each division of C & I equipment for the four division SSLC. In other sections of the PSR, the principle of segregation is stated as a design intent and no detailed information is provided.

93. I have assessed the RP's claims that the main C & I systems are independent of each other and the high-level information relating to segregation and I judge that for the independence of systems the RP has put measures in place to protect against propagation of faults. Therefore my judgement is that at the level of the safety claims I am content that the three major systems are independent from each other. With regard to segregation, the RP has stated its high-level design principles and provided some supporting design information but there is insufficient information in the PSR for me to make a judgement of the adequacy of the design. This matter will be followed up in the following steps of GDA.

4.3.2 Strengths

94. The RP has recognised that the architecture should provide systems, which are diverse, independent and segregated from each other to defend against common cause failures and to achieve the required deterministic and probabilistic requirements.

95. The RP has committed to a significant modification to the design of the SSLC to address the identified diversity shortfall. The revised design provides diversity in the three platforms by the use of [1]FPGA technology for the SSLC, non-programmable HBSS and Programmable Logic Controller based PCoS.

96. The RP has modified the C & I Architecture design to include one-way gateway to limit fault propagation between the Class 1 SSLC and the Classes 2 and 3 PCoS. As stated above this has the additional benefit of increasing the resilience from off-site influences and therefore increases the security of the overall C & I Architecture.

4.3.3 Items that Require Follow-up

97. During my GDA Step 2 assessment of Control and Instrumentation System Architecture I have identified the following shortcomings that I will follow-up during Step 3:

[1] *Many FPGA integrated circuits do contain embedded microprocessors but the RP has agreed that the type of FPGA technology it will employ will not include such complex devices.*

- The design of the HBSS is not a fully integrated system and the technology the RP will apply to its design has not been finalised.
- The HBSS has a number of manually initiated safety functions. Modifications, which the RP has committed to make, will be required to automate the operation of these functions.
- Additional fault studies may show the requirement for increased functionality of the HBSS for essential safety feature actuation and other areas.
- The PSR does not describe or justify the design of important C & I systems such as the Fuel Handling Machine control system, Heating Ventilation and Air Conditioning Control Systems and control systems embedded within packaged equipment (eg Diesel generators and electrical load control systems)
- Segregation of systems is only described at a principle level within the PSR. Although I judge that these principles meet my expectations further assessment will be required in the following steps of GDA to assess the detailed design.

98. During my GDA Step 2 assessment of Control and Instrumentation System Architecture I have identified the following additional potential shortcomings that I will follow-up during Step 3:

- The potential lack of diversity of pressure measurements, which the RP has committed to review.
- The use of common instrumentation connections around the reactor pressure vessel and the associated reduction in Independence of measurement.

4.3.4 Conclusions

99. Based on the outcome of my assessment of the Control and Instrumentation System Architecture, I have concluded that the C & I architecture addresses my high-level expectations that it is diverse and independent. With regard to segregation, there is insufficient information in the RP's submission for me to judge the overall adequacy of these claims. In addition, the introduction of the one-way gateway for off-site connections increases the security resilience of the system.

100. Although I have found a number of matters requiring follow up during Step 3 of GDA, I am satisfied that the RP recognises these matters and will review the design to identify where further review and potential modifications are required. Overall, I judge that the high-level design of the C & I architecture is adequate. It is also important to note that the RP has already committed to a number of significant design changes to the meet relevant good practice.

4.4 Safety System Logic and Control (SSLC):

4.4.1 Assessment

101. My assessment has focused on high-level design of the SSLC as this is the primary safety Class 1 protection systems. I have assessed the RP's "Preliminary Safety Report on C & I" (Ref. 1), the "C & I New Platform Development for Protection System letter" (Ref. 2) and the "Decision of Protection System Platform" report (Ref. 3).

102. I have used the ONR SAPs ESS (Safety Systems) and ESR (Control and instrumentation of safety-related systems) to inform my assessment and judgements of

the adequacy of the RP's safety case. ONR's Safety Systems (T/AST/003) and Computer Based Safety Systems (NS-TAST-GD-046) TAGs along with international standards IEC 61513, "*Nuclear power plants Instrumentation and control important to safety General requirements for systems*" (Ref. 13), and IEC 61508, "*Functional safety of electrical/electronic/programmable electronic safety-related systems*" have also been used to inform my judgements. Table 1 of this report gives additional information on the basis of the findings of my assessment.

103. My assessment is based on the revised SSLC platform technology (FPGA) which the RP committed to change (Ref. 2 & 3) from a microprocessor based system. Paragraph 83 describes the regulator concerns relating to the diversity of this system and the RP's rationale for the change in platform technology.

4.4.1.1 SSLC Design

104. As described in paragraph 83 the SSLC will use FPGA technology to deliver its function. The use of this technology will be the first time it has been used for a complete primary protection system for Nuclear Power Plant in the UK. The detailed design of the FPGA based SSLC is not included in the PSR (Ref. 1) as the decision to change from a microprocessor based system was made by the RP at the same time the PSR was being written. However, the functionality of the FPGA SSLC will be very similar to that of the microprocessor based SSLC.

105. The SSLC performs the following functions; Reactor Protection System (RPS), Main Steam Isolation Valve (MSIV) operation, Emergency Core Cooling System (ECCS) and Emergency Safety Features (ESF). It comprises of a number of modules connected together using a combination of electrical or optical communications. The main modules are; Remote Multiplexing Units, Digital Trip Modules, Trip Logic Units, Safety Logic Units and Output Logic Units. These modules are interconnected in different configurations depending on the safety function they are supporting. The description of the SSLC modules within the PSR is at a high-level and it did not give sufficient technical information for me to assess if they used diverse technology from the modules used in the PCoS. I requested clarification from the RP by raising RQ-152 (Ref. 15). In the RP's response to RQ-152 it confirmed that the technology used for the modules within the SSLC will be diverse from that used for the PCoS.

106. The SSLC is subdivided at a high-level into four divisions, which are grouped in various combinations to perform the required safety function. Table 5.2-1 of the PSR (Ref. 1) gives examples of the SSLC Controller Assignment and indicates the assignment of safety functions to each division.

107. The interface of the SSLC with other systems is described and assessed in section 4.3 of this report and is therefore not included in this section.

108. I have assessed the high-level design of the SSLC and consider it to be appropriate for the safety claims the RP is making against it in terms of its overall design concept. The description, in the PSR (Ref. 1), of the design of FPGA based SSLC is at a very high-level with statements of intent rather than detailed technical descriptions. Since the submission of the PSR, the RP has presented further technical design information during technical engagements. This information has not been included in my formal assessment, but it has given me confidence that the design of the FPGA based SSLC will fulfil the claims the RP has made on it. During these engagements I have also gained confidence in the competence of the RP's' design personnel to deliver an adequate system although they have limited experience of justifying designs in the UK regulatory environment. The RP has stated, within the PSR, that a more detailed description will be provided in the SSLC Basis of Safety Case, which will be provided

during Step 3 of GDA. The design of the FPGA SSLC will be a matter which I will follow up during Step 3 of GDA.

4.4.1.2 C & I Management System and Design Development

109. The RP's overall C & I design management system for the development process will be based on its existing practices and procedures and is based on a life-cycle approach. The RP has stated that the existing practices and procedures will be reviewed to confirm they are suitable for use during the UK ABWR project. The development of the SSLC FPGA platform will be carried out by a sub-division of the RP's parent company with the requirements specifications for the SSLC being produced by the RP. Quality Assurance activities will be managed on a lifecycle approach throughout the design process. The RP has stated in the PSR (Ref. 1) Section 9.2.2. that the Quality Assurance approach for the development of the FPGA SSLC will be described during Step 3 of GDA.

110. The RP has stated that its approach to the development of the design for C & I systems for UK ABWR will follow the requirements defined in IEC 61513 "*Nuclear power plants, Instrumentation and control important to safety, General requirements for systems"*. In addition the development of software based systems for Class 1 systems will follow the requirements of IEC 60880, "*Nuclear power plants, Instrumentation and control systems important to safety, software aspects for computer based systems performing category A functions"* and for Class 2 and 3 IEC 62138, "*Nuclear power plants, Instrumentation and control systems important to safety, software aspects for computer based systems performing category B and C functions"*. It has identified in Section 10.7 of the PSR (Ref. 1) that it's development of complex components such as FPGAs will comply with the requirements of IEC 62566 and will be also be based on the existing RP's sub-division's practices modified to comply with the requirements of IEC 61513 and IEC 62566.

111. Figure 9.3-1 of The PSR (Ref. 1), General C & I Design Flow, of the PSR depicts the high-level split of responsibility at a departmental level for the requirements capture, design development and manufacture of C & I systems. The PSR does not describe the RP's or its sub-division's design organisation in any further detail than that shown in the figure.

112. My assessment of the RP's C & I design management and development systems has revealed a number of potential shortcomings. The development of the FPGA based SSLC is new to the RP's design organisation and as such presents a number of challenges with regard to demonstrating the production excellence aspects required of a high integrity reactor protection system as set out in ONR TAG 046 (Ref. 9). In addition the PSR does not describe how the RP will demonstrate the expected independence of the design teams for each of the main C & I systems (SSLC, PCoS and HBSS) which would support its claims that common cause failures are reduced as far as is reasonably practicable during the design, verification and validation (production excellence) processes. I judge that the overall life-cycle approach described in the PSR meets the expectations of IEC 61513 and that the RP has identified the appropriate international standards for the development of the C & I systems. During Step 3 I will follow-up the RP's development of its production excellence approach and its organisational changes to demonstrate the independence of its design teams. In addition the RP may need to undertake research into the tools and techniques required to demonstrate production excellence for high integrity FPGA based protection systems.

4.4.1.3 Human Machine Interface

113. The plant operator interacts with the SSLC via a dedicated Human Machine Interface (HMI) in the Main Control Room. The HMI uses a combination of touch screen display and hardwired buttons depending on the functionality required. PSR Section 5.2.8 describes the overall approach. The HMI is not described in detail in the PSR . The RP has stated that the HMI will be connected directly to the SSLC and will be classified as a Class 1 system.

114. I have performed a high-level assessment of the HMI design and its classification. This assessment revealed that the design of the HMI did not meet my expectations with regard to the claimed classification. My particular concern was related to the requirement for bi-directional communications between the HMI and the SSLC and the use of SMART components (touch-screen HMI) within a class 1 system. The SSLC HMI uses a touch-screen display to manipulate information which is then used by the class 1 SSLC. To clarify the classification of the HMI I raised RQ-156 (Ref. 15). The response to this RQ stated that the classification of the HMI will be commensurate with the classification of the SSLC. My judgement is that the current SSLC HMI design, using touch screen based technology with input into the SSLC, does not meet the expectations of the classification the RP is claiming for it. It is my opinion that this type of HMI could only achieve at best class 2 requirements, due to the use of SMART components and the associated bi-directional communication with the class 1 SSLC, and as such does not meet the expectations set out in ONR SAP ECS.2

4.4.2 Strengths

115. The safety functions of the SSLC are based on the requirements of the previous microprocessor based Primary Protection System.

116. Appropriate international standards have been selected.

117. The design development process is based on a life-cycle approach.

118. The use of one-way gateways increases the security resilience to off-site influences.

4.4.3 Items that Require Follow-up

119. During my GDA Step 2 assessment of the SSLC I have identified the following shortcomings that I will follow-up during Step 3:

- The Production excellence aspects of the development of the FPGA SSLC have not been fully described.
- The independence of the design development teams for each main C & I system has not been described.
- The design of the Human Machine Interface to the SSLC does not meet the expectations of a class 1 system.

120. During my GDA Step 2 assessment of the SSLC I have identified the following additional potential shortcomings that I will follow-up during Step 3:

- The application of FPGA technology to all functional roles of an NPP primary protection system will be the first in the UK and as such, the development of the design will require detailed assessment.

121. During my GDA Step 2 assessment of the SSLC, I have identified the following areas that may require research to be undertaken by the RP in order to underpin the safety claims in the C & I. I will follow these matters, as appropriate, during Step 3:

- Research into the tools and techniques required to demonstrate production excellence for high integrity FPGA based protection systems.

4.4.4 Conclusions

122. Based on the outcome of my assessment of the SSLC, I have concluded that the high-level design meets my high-level expectations.

123. Further design development is required to build confidence that the design will fully meet its safety function requirements and research is required by the RP to develop its approach to the justification of the production excellence aspects of its design processes. Independence of the design team for the SSLC from personnel involved in the design of the other independent systems (Secondary Protection and Control Systems) has not been described in the PSR and I judge this is a weakness in the RP's organisation. I will record the fact however that the RP has committed to develop an independent team for the SSLC.

4.5 Out of Scope Items

124. The following items have been left outside the scope of my GDA Step 2 assessment of the UK ABWR C & I.

- Review of the C & I systems associated with the Balance Of Plant (BOP) systems. The reason for leaving this matter out of the scope of my GDA Step 2 assessment is that I will include this item along with other C & I systems such as Fuel Route Control Systems and C & I systems embedded in other equipment in my Step 3 assessment as they do not affect the fundamental design of the C & I architecture.

125. It should be noted that the above omissions do not invalidate the conclusions from my GDA Step 2 assessment. During my GDA Step 3 assessment, I will follow-up the above out-of-scope items as appropriate; I will capture this within my GDA Step 3 Assessment Plan.

4.6 Comparison with Standards, Guidance and Relevant Good Practice

126. In Section 2.2 above, I have listed the standards and criteria I have used during my GDA Step 2 assessment of the UK ABWR C & I to judge the adequacy of the preliminary safety case. My overall conclusions in this regard can be summarised as follows:

- SAPs: I have reviewed the design of the main C & I Architecture taking into account the relevant SAPs. I have concluded that the design broadly satisfies the expectations set out in each SAP. Table 1 provides further details.
- TAGs: The C & I Architecture Design broadly meets the expectations of the two fundamental TAGs I have used in my assessment. With regard to TAG 046 further supporting evidence is required to fulfil the production excellence aspects of the approach to justifying the FPGA based Primary Protection System.
- Standards: I have reviewed the design and development standards the RP has identified it will apply to the design and development of the C & I Architecture. I have concluded that they are appropriate and meet the expectations of relevant good practice in the UK.

4.7 Interactions with Other Regulators

127. I have briefly interacted with United States Nuclear Regulatory Commission (US NRC) through a telephone conference and have briefed my delivery manager on this topic for a meeting with the Japanese regulator.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

128. The RP has provided a PSR for the UK ABWR for assessment by ONR during Step 2 of GDA. The PSR together with its supporting references present the high-level claims in the area of C & I that underpin the safety of the UK ABWR.

129. During Step 2 of GDA, I have conducted an assessment of the parts of the PSR and its references that are relevant to the area of C & I against the expectations of the SAPs and TAGs. From the UK ABWR assessment done so far I conclude the following:

- Overall, I am satisfied that the high-level claims made by the RP are reasonable, sufficiently complete for Step 2, and can be adequately underpinned with sufficient arguments and robust evidence. I am also confident that the RP will be able to articulate reasonable claims in the PCSR.
- I have identified a number of shortcomings during my assessment, which are identified in section 4 of this report. I will follow up these matters during the following steps of GDA.
- The RP has been proactive in all engagements with ONR and has made available sufficient resources to support the development of the C & I aspects of the safety case. Where necessary the RP has provided additional specialist engineering support to the C & I SME, which has given confidence that it can develop an adequate safety case for the UK ABWR. The RP has been open and transparent in its responses to requests for clarifications and additional technical information.
- The RP has committed to make modifications to the Japanese ABWR design to fulfil ONR's regulatory expectations.

130. Overall, I see no reason, on C & I grounds, why the UK ABWR should not proceed to Step 3 of the GDA process.

5.2 Recommendations

131. My recommendations are as follows.

- Recommendation 1: The UK ABWR should proceed to Step 3 of the GDA process.
- Recommendation 2: All the items identified in Step 2 as important to be followed up should be included in ONR's GDA Step 3 Assessment Plan for the UK ABWR C & I.
- Recommendation 3: All the relevant out-of-scope items identified in sub-section 4.5 of this report should be included in ONR's GDA Step 3 Assessment Plan for the UK ABWR C & I.
- Recommendation 4: Based on my findings identified in section 4.2 paragraph 66 relating to the inconsistent application of design codes and standards I recommend a review of design standards and codes used for the UK ABWR design is conducted to ensure they are consistently applied and referenced in the RP's safety case.

6 REFERENCES

1 *GA91-9901-0001-00001, XE-GD-0107, Preliminary Safety Report on Control & Instrumentation, Rev B, Hitachi-GE, 13 March 2014, TRIM 2014/109383*

2 *HGNE-REG-0023N, Letter from Hitachi-GE to ONR, C & I New Platform Development for Protection System, Hitachi-GE, 31st March 2014, 7, TRIM 2014/132981*

3 *3E-GD-A0036, Decision on Protection System Platform, Hitachi-GE, Rev 0, 31st March 2014, TRIM 2014/133005*

4 *GA91-9901-0007-00001, XE-GD-0104, Categorisation and Classification of Structures, Systems and Components, Rev B, Hitachi-GE, 14 March 2014, TRIM 2014/109395*

5 *GA91-9901-0008-00001, XE-GD-0103, Codes and Standards Report, Rev B, Hitachi-GE, 14 March 2014, TRIM 2014/109462*

6 *GA32-1502-0001-00001, 3D-GD-A0003, C & I E Basic Plan, Rev 0, Hitachi-GE, 31 March 2014, TRIM 2014/132459*

7 *ONR How2 Business Management System. BMS: Permissioning – Purpose and Scope of Permissioning. PI/FWD – Issue 3. August 2011*
http://www.onr.org.uk/operational/assessment/index.htm

8 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. http://www.onr.org.uk/saps/saps2006.pdf

9 *Technical Assessment Guides*

Safety Systems. NS-TAST-GD-003. Issue 6. HSE. July 2011

Electromagnetic Compatibility, NS-TAST-GD-015 Rev 1. ONR. April 2013

Essential Services, NS-TAST-GD-019 Rev 2. ONR. May 2013

Control and instrumentation aspects of nuclear plant commissioning, NS-TAST-GD-028, Rev 3, May 2013

Safety Related Instrumentation, NS-TAST-GD-031 Rev 3. ONR. April 2013

Computer Based Safety Systems. NS-TAST-GD-046 Rev 3. ONR. April 2013

http://www.onr.org.uk/operational/tech_asst_guides/index.htm

10 *Generic Design Assessment of HGNE's Advanced Boiling Water Reactor (ABWR) Step 2 Assessment Plan for* Control and Instrumentation ONR-GDA-AP-13-002 Revision **.** ONR December 2013. TRIM Ref 2013/406683

11 *IAEA Standards and Guidance*.

Safety of Nuclear Power Plants: Design. Safety Requirements. International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-R-1. IAEA. Vienna. 2000.

Software for Computer Based Systems Important to Safety In Nuclear Power Plant Safety Guide. International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-G-1.1. IAEA. Vienna 2000

Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide. International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-G-1.3. IAEA. Vienna. 2002.

www.iaea.org.

12 *Western European Nuclear Regulators' Association.*

Reactor Safety Reference Levels (January 2007)

Safety Objectives for New Power Reactors (December 2009) and Statement on Safety Objectives for New Nuclear Power Plants (November 2010)

Decommissioning Safety Reference Levels (March 2012)

Statement on Safety Objectives for New Nuclear Power Plants (March 2013) and Safety of New NPP Designs (March 2013)

http://www.wenra.org/

13 *International Standards*

IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems (parent standard for the design of E/E/PE safety-related systems)

IEC 61513 - Nuclear power plants — Instrumentation and control important to safety — General requirements for systems

IEC 61226 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

14 *UK ABWR Document Tracking Sheets. Updated versions submitted to the Joint Programme Office (JPO) throughout GDA Step 2. TRIM Folder Ref. 5.1.3.9587.*

15 *Regulatory Queries*

RQ-ABWR-0152 – C & I Architecture – 1 (Remote Multiplexing Technology), A Poole, 1st May 2014, TRIM 2014/172256

RQ-ABWR-0154 – C & I Architecture – 2 (Diversity of Pressure Measurement Instruments), A Poole, 1st May 2014, TRIM 2014/172282

RQ-ABWR-0153 – C & I Architecture – 3 (Hardwired Backup System Technology), A Poole, 1st May 2014, TRIM 2014/172283

RQ-ABWR-0155 – C & I Architecture – 4 (Independence of detection, logic solving and termination instrumentation and equipment between all Control & Instrumentation Platforms), A Poole, 1st May 2014, TRIM 2014/172283

RQ-ABWR-0156 – C & I Architecture – 5 (Classification of SSLC Operator Terminal), A Poole, 1st May 2014, TRIM 2014/172352

RQ-ABWR-0157 – C & I Architecture – 6 (SSLC Class 1 supporting certification), A Poole, 1st May 2014, TRIM 2014/172365

RQ-ABWR-0172 – C & Safety Case Documentation – 1 (Compliance with IEC Standards), A Poole, 22nd May 2014, TRIM 2014/199007

16 *GA91-9201-003-00112, 3E-GD-A0045 – Response to RQ-ABWR-0152, -0153, -0154, - 0155, -0156 and -0157, Rev 0, 28th may 2014, TRIM 2014/205441*

17 *GA10-9101-0100-11000, 3E-GD-A0043 - Generic Pre Construction Safety Report Chapter 11 on Control and Instrumentation, Rev DR1, 30 May 2014, TRIM 2014/209788*

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No and Title	Description	Interpretation	Comment
EKP.3, 4 & 5	Engineering Principle: Key principles	EKP.3 – Defence in depth A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.	High-level safety principles are described in PSR Section 2, Safety Principles and Development Practice. The RP's safety principles for nuclear facilitates (PSR section 2.1.1) identifies 3 high-level safety principles. These are: • Unification of management responsibility • Adoption of defence in depth • Adoption of proven technical principle Table 2,1-2 Objectives and Essential means of Defence in Depth, identifies the defence in depth levels (1 to 5) the RP is adopting for the UK ABWR design. This table shows the C & I systems, which will be adopted at each level. The RP has adopted diverse technologies for each defence system. I am satisfied that the PSR adequately addresses this SAP.
		EKP.4 – Safety function The safety function(s) to be delivered within the facility should be identified by a structured analysis.	The RP's approach to the identification of safety functions is described in PSR Section 2.3, Categorisation and Classification. ABWRs in operation in Japan have followed Japanese guidance. The RP has stated that the Japanese guidance broadly aligns with the

			expectations set out in the ONR SAPs. PSR Section 3, Requirements, outlines the RP's approach to capturing the safety function requirements. It has stated that a combination of the production of a fault schedule and deterministic and probabilistic analysis will be used to identify each safety function. I am satisfied that the PSR adequately addresses this SAP.
		EKP.5 – Safety measures Safety measures should be identified to deliver the required safety function(s). Specific C & I interpretation and guidance Computer Based Safety Systems Technical Assessment Guide. NS-TAST-GD-046	PSR Section 3, Requirements, identifies the source of safety function requirements for each safety system, The RP has acknowledged that functional requirements for each C & I safety function has evolved with the design of the ABWR since it was originally designed and therefore does not meet with the recommended practices in the UK. However, it has stated that it will review all functions to ensure they are appropriate to protect against all existing and any new faults identified as part of its review. A Fault Schedule will be created to capture all events that may lead to a fault and the safety functions required to protect against them. I am satisfied that the PSR adequately addresses this SAP. However, follow up will be required in the following steps.

ECS.1 - 3	Engineering Principle: Safety classification and standards	ECS.1 – Safety Categorisation The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.	The RP's approach to the categorisation of safety functions is described in PSR Section 2.3, Categorisation and Classification. ABWRs in operation in Japan have followed Japanese guidance. The RP has stated that the Japanese guidance broadly aligns with the expectations set out in the ONR SAPs. For UK ABWR the RP has stated that it will follow the guidance for categorisation of safety functions set out in ONR SAP ECS.1. I am satisfied that the PSR adequately addresses this SAP.
		ECS.2 – Safety classification of structures, systems and components Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.	The RP's approach to the classification of safety functions is described in PSR Section 2.3, Categorisation and Classification. For UK ABWR the RP has stated that it will follow the guidance for classification of safety functions set out in ONR SAP ECS.2 and the international standards IEC 61226 and IEC 61513. I am satisfied that the PSR adequately addresses this SAP.
		ECS.3 - Standards Structures, systems and components that are	PSR Section 2.2 Design Policy for C & I Systems Important To Safety, and section 2.4, Codes and Standards, describe the standards

		important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards. Specific C & I interpretation and guidance Safety Systems Technical Assessment Guide T/AST/003 Computer Based Safety Systems Technical Assessment Guide. NS-TAST-GD-046	that the RP will apply to the design of the UK ABWR. ABWRs in operation in Japan have followed Japanese design guides and codes. For the UK ABWR the RP has stated that it will compare the current design processes with the requirements of the equivalent IEC standards and where shortfalls are identified, they will be addressed. I am satisfied that the PSR adequately addresses this SAP although it has not completed its review of Japanese and IEC design standards. This will require further follow up during Step 3 of GDA.
EQU.1	Engineering Principle: Equipment qualification	EQU.1 – Qualification Procedures Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.	PSR Section 2.5, Qualification, sets out the RP's approach to the qualification of C & I systems. Qualification requirements for the major systems are described at a high-level and in some cases, the PSR states that Qualification requirements will be developed in the following stages of GDA. Where C & I equipment has been used in the Japanese ABWR design, the qualification has been carried out in line with Japanese JEAG and JEAC guides. I am satisfied that the RP has suitable procedures in place for the qualification of C & I equipment and where further development of qualification requirements are to be developed in the following stages I am confident that the RP will develop adequate arrangements.

EDR.1, 2, 3, 4	Engineering Principle: Design for reliability	EDR.1 Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate. EDR. 2 Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.	See EKP.4 for assessment of the RP's approach to the analysis of faults and the identification of safety functions PSR Section 2.1.6, C & I Platform Defence in Depth and Diversity Approach for Safety Function, describes the RP's high-level defence in depth principles for safety functions. PSR Table 2.1-2, Objective and Essential means for Defence in Depth, sets out the levels of defence in depth and the associated C & I systems for each level. PSR Section 4.2, Rationale, describes the high-level design principles for redundancy, segregation and diversity. PSR Section 4.5.2 Segregation PSR Section 4.5.4 Diversity and common Cause Failure Redundancy is described at a systems level through out the PSR I am satisfied the RP has adequately addressed the high-level principles of redundancy, diversity and segregation in the C & I Design.

		EDR. 3 Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability. EDR. 4 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. Specific C & I interpretation and guidance Safety Systems Technical Assessment Guide T/AST/003 Computer Based Safety Systems Technical Assessment Guide. NS-TAST-GD-046	See EDR.2 for the assessment of the of the RP's approach to Common Cause Failures PSR Section 4, Architecture, describes the overall C & I Architecture and includes claims against the failure of systems. The approach the RP has adopted in the overall C & I design is to have divisions within systems to protect against spurious operation and prevent single random failures preventing the operation of the safety functions. I am satisfied the RP has adequately addressed the high-level principles of protection against single random failures effecting the performance of the safety system in the C & I Design.
ERL.3	Engineering Principle: Reliability claims	ERL.3 The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.	PSR Section 3, Requirements, set out the RP's approach to identifying the reliability requirements of safety systems. Its approach is to develop a fault schedule, which will identify the Classification of each system and therefore its reliability requirement. The provisional reliability claims for each of the main systems, control, primary and back-up safety systems are set out in section 4.2.1. These are:

		Specific C & I interpretation and guidance Computer Based Safety Systems Technical Assessment Guide. NS-TAST-GD-046	• PCoS 1 x 10^{-2} spurious failures per year • SSLC 1 x 10^{-4} pfd • HBSS 1 x 10^{-2} pfd I am satisfied the RP has a structured methodology for the identification of reliability requirements and that the provisional reliability claims are appropriate and achievable.
ECM.1	Engineering Principle: Commissioning	ECM.1 Before operating any facility or process that may affect safety it should be subject to commissioning tests to demonstrate that, as built, the design intent claimed in the safety case has been achieved. Specific C & I interpretation and guidance Computer Based Safety Systems Technical Assessment Guide. NS-TAST-GD-046	PSR Section 9.3, Safety Lifecycle, identifies commissioning as an activity. PSR Section 9.5.6.1, Commissioning, describes at a high-level the activities included during commissioning. Other sections within the PSR identify commissioning as an activity that is required to be carried out. The PSR does not describe the Commissioning activities in detail and states that this information will be developed during Step 3 and 4 of GDA. Overall, I am satisfied the RP has identified Commissioning as a Safety Lifecycle activity and described at a high-level the activities that will be carried out. I will follow up during the following steps of GDA the development of the RP's approach to commissioning.
EMT. 7	Engineering Principle: Maintenance, inspection and testing	EMT.7 In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component.	The PSR does not specifically address In-service functional testing. However, in the RP's review of Review of IEC Nuclear Standards (Section 2.4.1) it has identified IEC 60671 as the standard it will use to address this requirement. I am satisfied the RP has identified the

			appropriate international standard (IEC 60671) for surveillance testing and I will follow up how the RP incorporates In-service testing in its design during the following steps of GDA.
EAD.1	Engineering Principle: Ageing and degradation	EAD.1 The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.	The safe working life of SSCs has not specifically been addressed in the PSR. PSR Sections 9.5.6.3, Ageing and Obsolescence Managements, and 9.5.6.4, System Replacement Lifecycles, state that information will be provided in the PCSR. It is my opinion that there is insufficient information within the PSR for me to assess if the RP has adequate processes in place to assess the safe-working life of SSCs during the design phase. In addition, the PSR does not describe state what the working life is for C & I equipment. I will follow up this matter during my review of the PCSR and during the following steps of GDA.
ELO.1	Engineering Principle: Layout	ELO.1 The design and layout should facilitate access for necessary activities and minimise adverse interactions during such activities.	PSR Section 4.4, Location of Architecture Elements, describes the physical layout of the equipment associated with the four divisions of the SSLC. For this system, the RP has stated that each division is located in separate sections of the reactor building. For other systems there is no information relating to the physical location. In Section 4.5.2 of the PSR, Segregation, the high-level principle of segregation is described. It is my opinion that there is insufficient information within the PSR for me to assess if the physical layout of C & I systems within the

			ABWR design. I will follow up this matter during the following steps of GDA.
EHA.1	Engineering Principle: External and internal hazards	EHA.1 External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.	The PSR does not describe the RP's approach to protecting C & I systems form External Hazards. Section 4.4 of the PSR, Location of Architecture Elements, states that the physical layout of the four divisions of the SSLC has considered Internal Hazards. PSR Section 2.5, Qualification, states that the qualification process for C & I systems will demonstrate that they are resilient to hazards such as seismic, electromagnetic interference and the environment. It is my opinion that there is insufficient information within the PSR for me to assess if the RP has adequately considered the affect of external and internal hazards have on C & I systems. I will follow up this matter during the following steps of GDA and I will coordinate with the Internal and External Hazards Specialist assessors.
ESS.1, 2, 3, 7, 8, 18, 21, 23, 27	Engineering Principle: Safety systems	ESS.1 - Requirement for safety systems All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.	See EKP.4 for assessment of the RP's approach to the analysis of faults and the identification of safety functions.

		ESS.2 - Determination of safety system requirements The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.	See EKP.4, ECS.2 and EDR.2 for assessment of the RP's approach to the determination of safety systems requirements.
		ESS.3 - Monitoring of plant safety Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions.	PSR figure 4.3-1, Overall C & I Architecture, indicated that Human Machine Interfaces will be available for monitoring the plant status. PSR Section, 8 Human Machine Interface, describes the design and location of the human machine interfaces in the ABWR design. Table 8.1-2, HMIS framework, identified the function and location of each HMI and its safety category and classification. It is my opinion that the HMI design meets the high-level expectations of this SAP. I recognise the design of HMIs requires assessment by C & I and Human Factors Specialist Assessors and I will coordinate my step 3 and 4 assessment with the appropriate ONR Inspector.
		ESS.7 - Diversity in the detection of fault sequences The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.	Diversity in fault detection has not been considered in detail in the C & I PSR. The PSR states that diversity in the sensing instrumentation between the SSLC and other safety systems will be required for the UK ABWR design. It is my opinion that there is insufficient information in the PSR to assess if this SAP has been adequately addressed in the design of the UK ABWR, although I have identified a

		ESS.8 - Automatic initiation A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action. ESS.18 - Failure independence No fault, internal or external hazard should disable a safety system.	potential concern with regard to the use of pressure measurements as a common safety system initiator. I will follow up this matter during the following steps of GDA. PSR Section 4.3, Overall C & I Architecture, states that it is the RP's intention to modify the design of C & I safety system to meet the expectations of ESS.8. I am satisfied that the RP has identified the requirements of this SAP in the PSR. I will follow up the RP's commitment to review the automatic operation of safety systems in the following steps of GDA. The PSR has limited information of how failure independence will be achieved. It states that non-functional requirements of independence, redundancy and diversity will be applied to the design of the C & I architecture but does not give enough information for me to judge the adequacy for each C & I systems. Segregation of systems is a design principle that has been stated for each C & I system. Figure 4.4.3-1 depicts the instrumentation connections to the reactor pressure vessel. This figure shows that the instrumentation for three independent systems share a common connection point. It is my opinion that the PSR adequately sets out the high-level design principles the RP intends to apply to the UK ABWR design. However, there is insufficient information for me to assess the adequacy of the failure independence of each C & I system. My

			assessment has revealed that the instrumentation connections to the reactor pressure vessel are shared which does not meet the expectations of this SAP. I will follow up this matter during the following steps of GDA.
		ESS.21 – Reliability The design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.	This SAP has not been specifically addressed in the PSR. The design of the C & I Architecture has three clearly identifiable systems, which avoid complexity in their interconnections. There is insufficient information in the PSR to assess if there are means to reveal internal C & I system faults. This matter will be followed up in Steps 3 and 4 of GDA. I am satisfied that this SAP is sufficiently addressed within the PSR for my Step 2 assessment although the SAP is not fully met. Further follow up assessment will be required during Steps 3 and 4.
		ESS.23 - Allowance for unavailability of equipment In determining the safety system provisions, allowance should be made for the unavailability of equipment.	There is insufficient information in the PSR to assess if allowances for the unavailability of equipment have been addressed in the UK ABWR design. I will follow up on this matter in the following steps of GDA.

		ESS.27 - Computer-based safety systems Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures. Specific C & I interpretation and guidance Safety Systems Technical Assessment Guide T/AST/003	PSR Section 2.4.1, Review of IEC Nuclear Standards, identifies two tiers of standard the RP will consider during the design of the UK ABWR. It has identified the following standards as fundamental to the design of the C & I systems; • IEC 61226 • IEC 51513 • IEC 60880 • IEC 62138 • IEC 60978 • IEC 62556 Other supporting standards are identified within the PSR. Production Excellence and Independent Confidence Building measure have been identified at a high-level in section 10, Hardware and Software Development & System Justification, of the PSR. In addition section 9, Management Systems for C & I design, describes the overall approach to managing the design and development of C & I systems. Overall, I am satisfied that the RP has addressed the high-level expectations of this SAP and identified the appropriate IEC standards for the design and development of computer based safety systems. Additional information will be required during the following steps of GDA to support the claims the RP has made. I will follow up this matter during the following steps of GDA.

ESR.1, 3, 5, 7	Engineering Principle: Control and instrumentation of safety-related systems	ESR.1 - Provision in control rooms and other locations Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility.	See ESS.3 for the assessment of the provision of control rooms and other locations.
		ESR.3 - Provision of controls Adequate and reliable controls should be provided to maintain variables within specified ranges.	See ESS.3 for the assessment of the adequacy of controls to maintain variables within specified ranges.
		ESR.5 - Standards for computer based equipment Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.	See ESS.27 for the assessment of the standards applied for computer based equipment.

		ESR.7 - Communications systems Adequate communications systems should be provided to enable information and instructions to be transmitted between locations and to provide external communications with auxiliary services and such other organisations as may be required. Specific C & I interpretation and guidance Safety Related Instrumentation Technical Assessment Guide	Figure 4.3-1, Overall C & I Architecture, shows connections to off-site systems. These are from the Emergency Response Facility and the PCS. The purpose of these connections is to allow information to be transmitted off-site in the case of a severe accident (PSR section 6.5.2). The off-site connection to the PCS is not described in the PSR. To prevent adverse effects on the C & I systems from external systems the RP has introduced into the UK ABWR a one-way gateway to isolate the C & I systems. I am satisfied the RP has adequately addressed the expectations of this SAP. There is insufficient information in the PSR for me to assess the design of the one-way gateway and I will follow up on this matter during the following stages of GDA.
EES	Engineering Principle: Essential services	EES.1 - Provision Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and fault conditions.	Section 7, Support Services, of the PSR describes the services that are required to support C & I safety systems. The PSR identifies; • Electrical supplies • Air Supplies • Water Cooling System • HVAC • Fire Protection for C & I Systems The PSR states that the Classification of support systems will be the same as for the systems they support. I am satisfied that the PSR adequately

			identifies essential services that support C & I systems which in turn maintain a safe plant state as required by this SAP.
ECV	Engineering principles: containment and ventilation: containment monitoring	ECV.6 – Monitoring devices Suitable monitoring devices with alarms and provisions for sampling should be provided to detect and assess changes in the stored radioactive substances or changes in the radioactivity of the materials within the containment. ECV.7 – Leakage monitoring Appropriate sampling and monitoring systems and other provisions should be provided outside the containment to detect, locate, quantify and monitor leakages of nuclear matter from the containment boundaries under normal and accident conditions.	PSR Section 6.3.8, Radiation monitoring System, identifies a number of systems that will be provided. These are; • Radiation Monitoring Systems • Main steam line radiation monitor • Reactor building HVAC radiation monitor • Fuel handling area radiation monitor I am satisfied that the RP has identified C & I systems to monitor leakage. However, I will coordinate with the Specialist Radiation Protection assessor to assess the overall adequacy of these systems during the following steps of GDA. See ECV.6 for the assessment of the provision of leakage detection systems.
ERC.2	Engineering Principle: Reactor core	ERC.2 - Shutdown systems At least two diverse systems should be provided for shutting down a civil reactor.	PSR Table 3.3.1-1 Category and Classification for Class A (assumptions for the UK ABWR development) identifies the category A safety functions for the UK ABWR. It indicates for

			reactor shutdown two diverse systems will be used. These systems will be initiated by the FPGA based SSLC and the Hardwired Back-up system. I am satisfied that this SAP has been addressed. However as the PSR only indicates the design assumption for the UK ABWR I will coordinate with the ONR Fault Studies Specialist Assessor to ensure these assumptions are followed through into the design. I will follow up this matter during the following stages of GDA.
DC.1	Engineering Principle: Decommissioning	DC.1 - Design and operation Facilities should be designed and operated so that they can be safely decommissioned.	Decommissioning has been recognised as a lifecycle activity in sections 9.3, Safety Lifecycle and 9.5, Overall Lifecycle of the PSR. The PSR does not give a description of how decommissioning of C & I will be considered in the design. I am satisfied that decommissioning has been recognised by the RP as a Safety Lifecycle activity, which I consider to be sufficient for my Step 2 assessment although the SAP is not fully met. Further follow up assessment will be required during Steps 3 and 4.